A Packet Traversal Time per Hop based Adaptive Wormhole Detection Algorithm for MANETs

Jonny Karlsson and Göran Pulkkis
Dept. of Business Management and Analytics
Arcada University of Applied Sciences
Helsinki, Finland
e-mail: jonny.karlsson@arcada.fi

Laurence S. Dooley
School of Computing and Communications
The Open University
Milton Keynes, United Kingdom
e-mail: laurence.dooley@open.ac.uk

***Abstract*— Routing security challenges significantly impact the wide-scale adoption of *mobile ad hoc networks* (MANET), with wormholes constituting an especially severe threat. Wormhole detection algorithms like *traversal time and hop count analysis* (TTHCA) and *modified transmission time-based mechanism* (M-TTM) combine effective detection with low traffic overheads. TTHCA measures *packet traversal time* (PTT) per route *hop count* (HC), while M-TTM compares an *expected round trip time* (RTT) with a *measured* RTT. However, using only fixed thresholds for the permissible PTT/HC and *measured* RTT deviations respectively, both algorithms are compromised so *participation mode* (PM), *out-of-band* (O-B) wormholes are inadequately detected in MANETs with large radio range fluctuations. This paper presents an extended variant of the TTHCA algorithm called *traversal time per hop analysis* (TTpHA) that dynamically adapts the PTT per hop threshold to both different node radio coverages and prevailing MANET conditions. Experimental results confirm TTpHA provides superior PM O-B detection performance compared to TTHCA and M-TTM, with commensurately low false positive rates and traffic overheads.**

Keywords—Mobile networks; MANET; MANET security; routing security; hop count; packet traversal time; variable radio range; TTHCA.

I. INTRODUCTION

A *mobile ad hoc network* (MANET) is a self-configuring arrangement of wireless nodes where multi-hop communication is feasible without requiring core infrastructure like routers and base stations. Potential MANET applications include military communications, vehicular and sensor networks, as well as Internet access mechanisms in scenarios where nodes are out-of-radio range.

Their open nature and the absence of dedicated routers mean that MANETs are especially vulnerable to routing attacks [1][2]. The *wormhole attack* [3] is one of the most severe MANET routing threats since it is relatively easy to launch, difficult to detect, and yet can cause significant communications disruption. Two collaborating malicious nodes create a fictive shortcut link in the network by forwarding routing packets to each other with the intention to attract more data packets to traverse the wormhole link. Once the wormhole has been successfully established, the malicious nodes can disrupt network operation by either dropping packets or launching more pernicious attacks, such as eavesdropping and packet sniffing.

A wormhole attack can be launched in either *hidden mode* (HM) or *participation mode* (PM) [4]. In the former, malicious nodes capture and forward routing packets to each other without modifying the actual packets, so the wormhole nodes never appear in routing tables. In contrast, PM nodes process routing packets as any pair of legitimate nodes and therefore appear in a wormhole infected route as two contiguous nodes.

The malicious nodes can forward routing packets to each other using either an *in-band* (I-B) or *out-of-band* (O-B) wormhole link. An I-B link tunnels packets between the malicious nodes via genuine network nodes, while an O-B link is more complex because it requires an external communication channel, i.e. network cable or directional antenna, to establish a direct link between the wormhole nodes.

Designing effective robust wormhole detection schemes means considering all four modes with each mandating different requirements upon the detection mechanism. While various detection strategies have been proposed in [3][5-13], most solutions have some recurring limitations including the inability to detect all wormhole types, the requirement for dedicated hardware, reliance on particular MANET environments, and imposing high computational overheads and/or bandwidth loads upon the network.

Several wormhole attack detection schemes are based on analysing *round trip time* (RTT) per hop, including *delay per hop indication* (DelPHI) [6], *wormhole attack prevention* (WAP) [7], and *transmission time based mechanism* (TTM) [8]. A route with an unrealistically high RTT per *hop count* (HC) or between any two successive hops is suspected to be wormhole infected. RTT-based approaches offer low overhead solutions in terms of hardware, computation, and throughput, but have the limitation that variations in a node's packet processing time must be small. In a real MANET, nodes can exhibit high packet processing time variations resulting in low wormhole detection rates and high *false positive* (FP) rates for RTT-based solutions, as is theoretically proven in [9] and in [10].

Alternative approaches like *wormhole attack detection using hop latency and adjoining* (WAD-HLA) node analysis [11] and *neighbor probe acknowledge* (NPA) [12] improve the detection performance of RTT-based methods by measuring the RTT between two nodes multiple times and using statistics to determine the RTT value. This correlates better with the route

distance between two hops, though such strategies tend to lead to increased network traffic loads.

Another approach [9, 10, 13] for improving the distance estimation accuracy between nodes is to subtract the packet processing times from RTT measurements, resulting in the air *packet traversal time* (PTT). The PTT of a route reflects better than RTT the route distance between two nodes. In [9], a modified version of TTM (M-TTM) was proposed where every node on a route measures the RTT between itself and the next hop. The *measured* RTT is then compared with the *expected* RTT, which is estimated by measuring the packet processing times of the *route request* (RREQ) and *route reply* (RREP) packets at the next hop and thereafter adding the maximum PTT (PTT_{MAX}). If the *measured* RTT between two nodes is significantly higher than the *expected* RTT, then a wormhole is suspected.

While M-TTM provides good detection performance under certain conditions, it has a number of limitations. Firstly, each node along a route must add four different timestamps to every routing packet to reflect the specific times incurred in receiving and forwarding RREQ and RREP packets. The assumptions underpinning how the *expected* RTT is determined are also unrealistic since in [9] PTT_{MAX} is presumed to be $1\mu s$ which corresponds to a distance of about *300m*. In a real network, the PTT_{MAX} of a node will be dependent on both its hardware and surroundings, since in a *line-of-sight* (LOS) link PTT_{MAX} will be much higher than when there are obstacles between nodes. Furthermore, applying a set *2ms* threshold for the maximum difference between the *measured* and *expected* RTT values means that it cannot detect all wormhole types. For instance, if the MANET has a PM O-B wormhole, then the PTT between the malicious nodes is short and is the only extra delay incurred.

Traversal time and hop count analysis (TTHCA) [10] is a recent wormhole detection technique designed as a security extension to the *ad hoc on demand distance vector* (AODV) [14] routing protocol and is lightweight in terms of both network overheads and computational complexity. It combines the benefits of RTT-based approaches and HC analysis [15] to provide improved detection for all wormhole types under a multiplicity of network scenarios. TTHCA applies a fixed threshold R/S, where R is the maximum radio range per node and S is signal propagation speed (i.e. $3 \cdot 10^8$ *m/s*), for the maximum permissible PTT/HC. In a homogeneous MANET where all nodes are in LOS, TTHCA is able to detect PM O-B wormholes. However, in real MANETs nodes usually have different hardware and encounter obstacles like walls and buildings. This causes fluctuations in the radio coverage of nodes. For both PM I-B and HM O-B/I-B wormholes, radio coverage variations do not affect wormhole detection performance of TTHCA, because such wormhole links incur long delays. However, for a fast-link PM O-B wormhole TTHCA detection rate is dependent on both radio coverage variation and wormhole length. See [10] for a critical evaluation of TTHCA.

The main limitation of TTHCA is its use of a rigid threshold in the PTT/HC analysis, so to relax this constraint, this paper introduces an extended flexible detection technique called *traversal time per hop analysis* (TTpHA). This uses TTHCA as its kernel and by using a dynamic threshold for the maximum permissible PTT value for each hop, TTpHA can readily adapt to prevailing network conditions and can handle variable node radio ranges and different environments, while affording superior detection accuracy.

A key factor in detecting PM O-B wormholes with PTT-based detection techniques, including TTpHA, TTHCA and M-TTM, is the accuracy of the timestamps generated for incoming and outgoing routing packets. For I-B and/or HM wormholes this is though not an issue due to their long link delays. This paper includes an analysis of the requirements on the *timestamp resolution* (TR) for TTpHA and provides comparative simulation results between TTpHA and M-TTM for PM O-B wormhole attack detection performance for different TR values and network conditions. The impact of node mobility during the route discovery procedure on TTpHA and M-TTM wormhole attack detection performance is also evaluated.

As it in [10] was shown that I-B and HM wormholes can be successfully detected by both TTHCA and TTpHA (since it is an extension of TTHCA) and since TR and radio covarage variabilities are not critical for such wormholes, the focus of this paper turns to the challenging PM O-B wormhole detection. The remainder of the paper is organized as follows: The TTpHA algorithm is introduced in Section II. Simulation experiments and a comparative results analysis of TTpHA with the original TTHCA algorithm and M-TTM is then presented in Section III, with some concluding comments being given in Section IV.

II. THE PACKET TRAVERSAL TIME PER HOP ANALYSIS ALGORITHM

TTpHA is a significant extension to the TTHCA algorithm [10], embracing two new features. TTpHA measures and analyses PTT for each successive hop ($PTT_{i,i+1}$) rather than PTT/HC to provide more accurate wormhole attack detection, and uses a dynamic threshold for the maximum permissible $PTT_{i,i+1}$ to automatically adapt to variable radio ranges and network environments. In this section, the TTpHA route discovery procedure to obtain $PTT_{i,i+1}$ calculations is presented before describing and critically analyzing the dynamic threshold mechanism.

A. TTpHA Extended AODV Route Discovery Procedure

TTpHA extends the AODV route discovery procedure analogously to TTHCA [10] with routing packet processing time (ΔT_i) measurements at all destination and intermediate nodes where ΔT_i is the sum of the AODV RREQ and RREP packet ($RREQ_{AODV}$ and $RREP_{AODV}$) processing times at node i ($\Delta T_i = \{\Delta T_{RREQ}\}_i + \{\Delta T_{RREP}\}_i$). To render $PTT_{i,i+1}$ calculations, TTpHA measures PTT between each intermediate and the destination node (PTT_i) in a similar way as route PTT measurements are performed in TTHCA. Each PTT_i is delivered to the source node as a separate parameter of a new RREP packet ($RREP_{TTpHA}$) together with the sum of all ΔT_i values (ΔT_{TOT}). To achieve high resolution timestamps, the ΔT_i measurements must be performed at the physical layer while routing packets are processed at the network layer. For this reason, the ΔT_{TOT} parameter and the PTT_i values cannot be simply added to $RREP_{AODV}$ as is proposed in [10]. The complete TTpHA extended AODV route discovery procedure is illustrated in Fig. 1, where node 1, 2 and 3 are the source, intermediate, and

destination nodes respectively, $\{T_{RREQr}\}_i$ and $\{T_{RREQs}\}_i$ are the timestamps generated when receiving and sending the first bit of $RREQ_{AODV}$ at node i, while $\{T_{RREPr}\}_i$ and $\{T_{RREPs}\}_i$ are the corresponding $RREP_{AODV}$ timestamps.

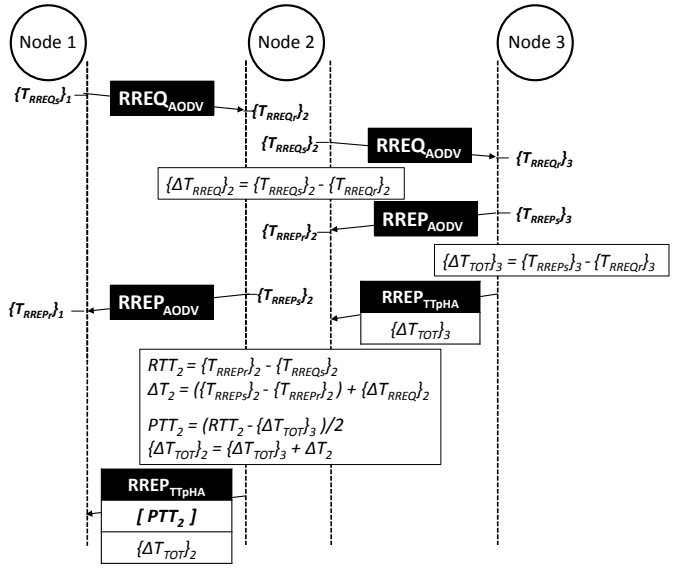

Fig. 1. The TTpHA extended AODV route discovery procedure.

Upon receiving $RREP_{AODV}$ and $RREP_{TTpHA}$ at the end of a route discovery procedure, the source node calculates each $PTT_{i,i+1}$ from

$$PTT_{i,i+1} = PTT_i \tag{1}$$

if node $i+1$ is the destination node, otherwise

$$PTT_{i,i+1} = PTT_i - PTT_{i+1} \tag{2}$$

Each $PTT_{i,i+1}$ is then inserted as an element of a vector V which is ranked in ascending order. V is used to determine a *dynamic threshold* Θ for the maximum permissible $PTT_{i,i+1}$ of the route. If nodes i and $i+1$ form a PM wormhole, then $PTT_{i,i+1}$ at node i will be larger than any healthy $PTT_{i,i+1}$. Thus, the wormhole link is detected if $V_{HC} > \Theta$. The complete TTpHA algorithm at the source node is shown in Fig. 2, where it is assumed there is only one wormhole link per route. To detect multiple wormhole links, all elements of V ($1 \le n \le HC$) must be separately evaluated.

B. Dynamic Threshold Θ

To successfully identify the $PTT_{i,i+1}$ of a wormhole link it must be compared with a threshold value that is considered to be the upper bound for healthy $PTT_{i,i+1}$ values. Automatic adaption to variable network environments and diverse node hardware requires dynamic calculation of Θ. To achieve this, an outlier detection technique, such as Grubb's test [16], the box plot method [17], or Dixon's Q-test [18] is usable to identify the wormhole link $PTT_{i,i+1}$, which is typically significantly higher than any healthy $PTT_{i,i+1}$. To determine Θ, the Q-test was chosen because it is specifically designed for small sample numbers n, typically $3 \le n \le 10$, while in analyzing all $PTT_{i,i+1}$ values of a route $n = HC$. Considering larger sample numbers [19], it is a pragmatic design assumption that $n \le 30$, since at higher values communicating nodes will be located unrealistically long distances apart and a route will incur high delays. The threshold Θ is calculated from the ranked V values as

$$\theta = \frac{V_{n-1} - Q_C V_1}{1 - Q_C} \tag{3}$$

where V_{n-1} is the second largest $PTT_{i,i+1}$ value, V_1 is the smallest value, and Q_C is the critical Q value for a chosen confidence level α defined in [20].

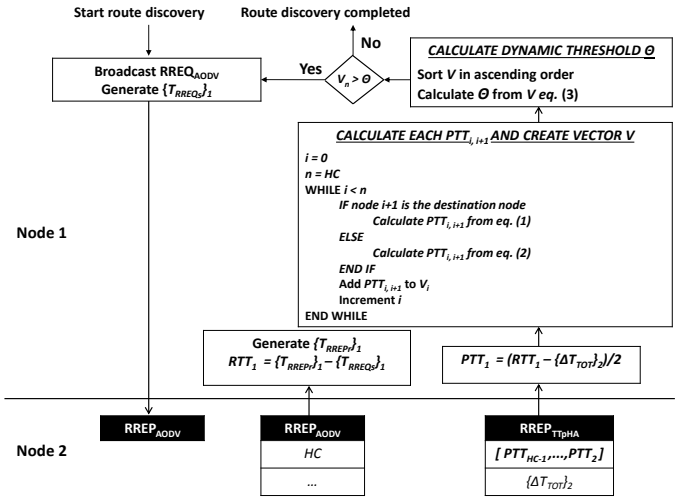

Fig. 2. Flowchart of the TTpHA algorithm at the source node (node 1).

If the route $HC < 3$, then (3) cannot be used. However, since the minimum HC of a PM wormhole infected route is 3, it is reasonable to apply the TTHCA [10] fixed threshold by defining $\Theta = \frac{R}{S}$. A wormhole is then suspected if

$$V_n > \Theta \tag{4}$$

where V_n is the largest $PTT_{i,i+1}$ value.

The choice of parameter α affords a useful design trade-off mechanism between wormhole detection and FP rates. A high α means low FP rates, but a concomitantly lower wormhole detection probability. Conversely, a low α increases the probability of detecting a wormhole, but with a higher FP rate. A confidence level $\alpha = 0.9$ was empirically determined for all the ensuing simulations as it represents the best design choice from a detection perspective.

A critical analysis of how key TTpHA factors including radio range variability, TR, node mobility, and time measurement tampering influence the wormhole detection capability of Θ will now be presented.

1) Radio Range Variability

If the route $HC \ge 3$, then (3) is applied to calculate Θ. As Θ is automatically determined from $PTT_{i,i+1}$ values in V, the TTpHA wormhole detection performance is dependent not only on the $PTT_{i,i+1}$ of the wormhole link but also on the variability of

$V_{i...n-1}$. The maximum permissible variability of $V_{i...n-1}$ which can still guarantee 100% detection of PM O-B wormholes is defined in Lemma 1.

Lemma 1: If $V_n = PTT_{i,i+1}$ of a wormhole link, then it will always be detected provided all $V_{i...n-1}$ are within the bounds:

$$\frac{xr_{wh}}{S} \leq V_i \leq \frac{R}{S} \quad (5)$$

where x defines the smallest permissible distance between two successive nodes ($r_{i,i+1}$) in relation to the length of the wormhole link (r_{wh}). The x value is calculated from:

$$x = \frac{r_{wh}(1 - Q_C) - R}{R(-Q_C)} \quad (6)$$

for the worst case scenario $V_{n-1}=\frac{R}{S}$, i.e. largest $r_{i,i+1}=R$.

Proof: If $V_{n-1} = \frac{R}{S}$ and $V_1 \geq \frac{xr_{wh}}{S}$ then from (3) $\Theta \leq \frac{r_{wh}}{S}$ and thus the wormhole is detected. Correspondingly, if $V_1 < \frac{xr_{wh}}{S}$ then $\Theta > \frac{r_{wh}}{S}$ and the wormhole will not be detected. ■

In a homogeneous LOS MANET environment $r_{i,i+1}$ can lie within the range [*0, R*]. This means that there is a risk that a PM O-B wormhole goes undetected if both the wormhole link and the route are short. The average $r_{i,i+1}$ is though in such environments in practice close to R while in non-LOS environments physical obstacles and differences in antenna capabilities lead to a higher variability in $r_{i,i+1}$ since the momentary radio range (R_i) at many nodes is less than R. If the maximum radio coverage of a specific node in a non-LOS environment is R_i, then $r_{i,i+1}$ is bounded by

$$r_{i,i+1} + r_{i+1,i+2} > \min\{R_i, R_{i+1}\} \quad (7)$$

(7) cannot be false, since then the 2-hop neighbor of node i would still lie within radio range and become a direct 1-hop neighbor. The condition in (7) means, that a short route infected by a short PM O-B wormhole will have a greater likelihood of going undetected than in a homogenous LOS environment.

2) Timestamp Resolution (TR)

To calculate ΔT_i in TTpHA, each intermediate node creates four timestamps ($\{T_{RREQr}\}_i$, $\{T_{RREQs}\}_i$, $\{T_{RREPr}\}_i$, *and* $\{T_{RREPs}\}_i$) and the destination node two ($\{T_{RREQr}\}_i$ and $\{T_{RREPs}\}_i$). The source node creates two timestamps to calculate route *RTT* ($\{T_{RREQs}\}_i$ and $\{T_{RREPr}\}_i$). *TR* causes for each created timestamp a measurement error E_{TR}, $0 \leq E_{TR} < TR$. The value of each generated timestamp can therefore be expressed as $T_A + E_{TR}$ where T_A is the actual time.

Each $PTT_{i,i+1}$ is calculated as

$$PTT_{i,i+1} = \frac{\{T_{RREPr} - T_{RREQs}\}_i - \{T_{RREPs} - T_{RREQr}\}_{i+1}}{2} \quad (8)$$

$PTT_{i,i+1}$ is minimized for

- $lim(E_{TR}) = TR$ when generating $\{T_{RREQs}\}_i$ and $\{T_{RREPs}\}_{i+1}$
- $E_{TR} = 0$ when generating the other timestamps

and maximized for

- $lim(E_{TR}) = TR$ when generating $\{T_{RREPs}\}_i$ and $\{T_{RREQr}\}_{i+1}$
- $E_{TR} = 0$ when generating the other timestamps.

So each calculated $PTT_{i,i+1}$ value lies between:

$$\frac{r_i}{S} - (lim(E_{TR}) = TR) \leq PTT_{i,i+1} \leq \frac{r_i}{S} + (lim(E_{TR}) = TR) \quad (9)$$

Using (8) and (9), it can be concluded that a PM O-B wormhole will always be detected provided the following condition is upheld:

$$\frac{r_{wh}}{S} - lim(E_{TR}) > \frac{\left(\frac{\max(r_i)}{S} + lim(E_{TR})\right) - Q_C\left(\frac{\min(r_i)}{S} - lim(E_{TR})\right)}{1 - Q_C} \quad (10)$$

which for $lim(E_{TR}) = TR$ is equivalent to

$$TR < \frac{Q_C(min(r_i) - r_{wh}) + r_{wh} - max(r_i)}{2S} \quad (11)$$

3) Mobility

Node mobility during the route discovery procedure will impact on a measured $PTT_{i,i+1}$ value in the sense, that it will not correspond exactly to the $r_{i,i+1}$ value when node i sends a RREQ or receives the RREP, unless nodes i and $i+1$ are moving in the same direction with exactly the same speed. $PTT_{i,i+1}$ will still represent a valid $r_{i,i+1}$ within the bound specified by (7), because even though two successive nodes on a route are moving they cannot communicate if $r_{i,i+1} > R_i$. For this reason wormhole attack detection performance will not be affected.

4) Time Measurement Tampering

Wormhole nodes can potentially tamper with PTT_i and ΔT_i values in order to prevent the $PTT_{i,i+1}$ of a wormhole link from being $> \theta$. A successful time measurement tampering attack is though challenging to realize in practice since the malicious nodes must be aware of the exact delay of the wormhole link, otherwise the attack may easily result in either $PTT_{i,i+1} < 0$ or a $PTT_{i,i+1}$ still being $> \theta$. The prevailing conditions for a time measurement tampering attack on TTHCA to succeed has been formally analyzed and an extension for time measurement tampering detection for PM I-B wormholes has been proposed in [21]. While this extension can be applied in TTpHA, time measurement tampering attacks for PM O-B wormholes can be detected for instance by permitting third party neighboring nodes to collaborate promiscuously to validate time measurements. A future research proposal is thus to investigate a distributed time measurement tampering detection strategy.

III. SIMULATION EXPERIMENTS

The wormhole and FP detection performance for different wormhole lengths, R_i variations, and TR values was analyzed in a series of simulation experiments. The MANET simulation environments in these experiments were created in *ns-2* [22] for

packet propagation speed $S=3\cdot10^8$ *m/s* and the *TwoRayGround* [23] propagation model. All network nodes except the wormhole nodes were assigned new random positions for each simulation run. For wormhole detection evaluation two wormhole nodes were strategically placed in the center of the simulation environment, a specific distance r_{wh} from each other, to disrupt as much network traffic as possible from all network nodes. The shortest wormhole length tested was $r_{wh} = 3R$, i.e. 3 hops, since in the simulation environment the amount of network traffic attracted in shorter wormholes is minimal. The wormhole link delay for an O-B link was defined as S/r_{wh}, which corresponds to the use of a directional antenna. During the FP detection evaluations the simulation environment was wormhole free. TTHCA [10] and M-TTM [9] were used as comparators since TTpHA is based on TTHCA and uses a similar packet delay per hop analysis scheme to that employed in M-TTM. The *2ms* fixed threshold for the maximum permissible difference between the *measured* and *expected* RTT values defined in [9] was omitted due to its impropriety for PM O-B wormhole detection. Hence, a wormhole is detected if any *measured* RTT > *expected* RTT.

In the experiments, two MANET scenarios are considered, i.e. an indoor and an outdoor environment, for which the respective parameter settings are shown in Table 1. In both environments it is assumed that all network nodes use *IEEE 802.11n compliant* wireless hardware, which determines the approximate R values in Table 1. The outdoor environment size and number of nodes N are defined as in [15] while the indoor environment dimensions reflect a large building. In a real MANET, the momentary radio range R_i will also be dependent on the antenna used and node surroundings, e.g. in an indoor environment containing obstructions like walls R_i is smaller than in a LOS environment. A random R_i distance value in the range $min(R_i) \leq R_i \leq R$ is introduced. The results from these simulation experiments are presented in the following subsections.

TABLE I. SPECIFIC PARAMETERS USED FOR INDOOR AND OUTDOOR SIMULATION ENVIRONMENTS

Parameter	Outdoor settings	Indoor settings
Number of nodes (*N*)	300	300
Network width (*W*)	1000m	100m
Network length (*L*)	4000m	400m
Maximal radio range / node *(R)*	250m	70m
Number of infected (N_{IR}) and healthy (N_{HR}) route samples	200	200

A. *Variable Radio Range*

In the first set of experiments, the comparative wormhole detection performance of TTpHA, TTHCA, and M-TTM was evaluated for different R_i variability levels and wormhole lengths. The results, shown in Fig. 3, reveal that for TTpHA, radio range variability does not significantly impact on the wormhole detection performance since > 90% of the wormhole infected routes were detected outdoors and > 80% indoors for all tested R_i variations. This contrasts to TTHCA, where the combination of a short wormhole and high radio range variability substantially decreased the detection rate.

In the outdoor environment, TTpHA wormhole detection rate tended to slightly drop with increased R_i variability. For example, the detection rate of the 3-hop wormhole was approximately 95% for $min(R_i)=R$ and 90% for $min(R_i)=0.2R$. The opposite trend was observed for the indoor environment, with 82% detection rate for the 3-hop wormhole case when $min(R_i)=R$ and 100% when $min(R_i)=0.2R$. The reason is that the route HC indoors was often <5 when $min(R_i)=R$ which according to *Lemma 1* means there is a risk that the condition in (5) is not upheld. The (5) condition has a significantly higher probability of being upheld when $min(R_i)=0.2R$, for which the average route HC is significantly higher. Outdoors the average route HC was higher than indoors and therefore (5) was mostly upheld even for $min(R_i)=R$.

Wormhole detection performance of TTHCA fails dramatically for $min(R_i)<R$ because it is based on the average PTT/HC. For $R_i < R$ the average $r_{i,i+1}$ is low compared to R and the condition $PTT/HC > R/S$ [10] is not upheld. M-TTM, on the other hand, provided 100% detection of all wormholes outdoors and of all 5-hop wormholes indoors. However, no wormholes shorter than 5 hops were detected indoors. The reason is that M-TTM assumes $PTT_{MAX}=1\mu s$ for the *expected* $RTT_{i,i+1}$ and a wormhole is suspected if a *measured* $RTT_{i,i+1}$ > *expected* $RTT_{i,i+1}$. A wormhole link is therefore only detected if $r_{wh} > \frac{1\mu s}{s}$. A cursory review of the results reveals that TTpHA is much more flexible, since it automatically adjusts its threshold to the prevailing environment, while M-TTM and TTHCA are only appropriate to outdoor environments.

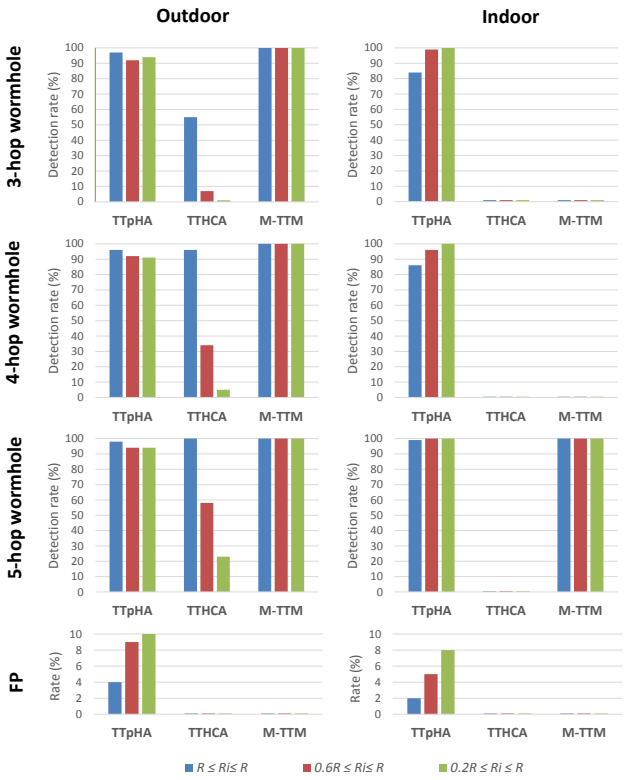

Fig. 3. Comparative TTpHA and M-TTM wormhole detection and FP performance for different wormhole lengths and radio range variations.

In terms of the corresponding FP rates, it was observed that the R_i variability level impacts on the performance of TTpHA since outdoors, the FP rate was just 4% when $R \leq R_i \leq R$, but 10% when $0.2R \leq R_i \leq R$. The corresponding FP rates indoors were marginally lower, at 2% and 8% respectively. These results can

be reduced by choosing a higher confidence value α for the threshold. However, this will decrease wormhole detection rates. From a wormhole detection perspective, a FP rate of up to 10% is still a laudable outcome considering the significant detection improvement achieved by TTpHA compared to both TTHCA and M-TTM. Furthermore, a higher FP rate does not prevent communication with a destination node, but the shortest route might be disabled.

It needs to be stressed that the fixed threshold used in TTHCA and PTT_{MAX} in M-TTM could be manually adjusted to the indoor environment to provide similar detection performance to that achieved for the outdoor environment. However, since this would involve decreasing these values, there would be a significantly higher FP detection rate outdoors. This highlights a key advantage of TTpHA in its ability to automatically adjust to its environment and move seamlessly between different situations without the need for any manual parameter adjustment.

These results are based on the assumption that each timestamp used in all three detection techniques can be generated with a *1ns* measurement accuracy. This is not a wholly realistic assumption for all constituent MANET hardware even if *TR* values as good as *1 ns* can be achieved with currently available timestamping hardware [24][25]. Therefore, the next section presents a performance insight into relaxing this assumption.

B. Time Measurement Accuracy

The next series of experiments analyzed the requirements imposed upon wireless interface hardware regarding the tolerances to TR required to monitor and process in-coming and out-going routing packets. Again different wormhole lengths were used and the performance of TTpHA and M-TTM was tested across a TR range from *1ns* to *1μs*. For example, *TR=10ns* means that every node is capable of both detecting and timestamping reception or transmission of a routing packet every *10ns*. In these experiments, a radio range variability of $0.2R \leq R_i \leq R$ was used to reflect a realistic mixture of node hardware and obstacles. Due its overall poor wormhole detection performance in highly variable radio range scenarios, TTHCA was not included as a comparator in this particular results analysis.

The results in Fig. 4 show that the TTpHA wormhole detection performance is not significantly decreased even when *TR* at each node is only *100ns*, as more than 90% of all tested wormholes were detected. The reason for this is obvious in the outdoor scenario, because the maximum allowable TR value in (11) $>100ns$ when the route $HC \geq 5$ and $r_{wh}=750m$ and the majority of the obtained wormhole infected routes had more than 5 hops. The corresponding maximum tolerable TR for the indoor environment does not exceed *100ns* before the route $HC \geq 9$. However, each $PTT_{i,i+1}$ value can vary within the bounds in (9), and since these can only be compromised in exceptional circumstances, wormhole detection performance is not significantly lowered despite a large proportion of infected routes being shorter than 9 hops. Even for $TR=1\mu s$, TTpHA still provides good performance in the outdoor environment scenario with a detection rate of ≈90% for all wormholes. For the indoor environment, the wormhole detection rate becomes heavily degraded when $TR=1\mu s$ with a detection rate of only 30…50%. The reason is that *TR* is in fact larger than any $\frac{r_{i,i+1}}{s}$ and $\frac{r_{wh}}{s}$. It is thus in practice impossible to discern a healthy link from a wormhole infected link, as is also indicated by the corresponding FP rate (~32%) being akin to the detection rate.

When the $TR=1\mu s$, M-TTM interestingly detected nearly 30% of the 3-hop wormholes and up to 50% of the 4-hop wormholes in the indoor environment even though for both wormhole lengths $\frac{r_{wh}}{s} < PTT_{MAX}$. The reason for this is that $(PTT_{MAX} - \frac{r_{wh}}{s}) < TR$ and as a result E_{TR} often causes a measured wormhole link $PTT_{i,i+1}$ to be $> PTT_{MAX}$. While these are still poor results, the detection rate of the 5 HC wormhole was satisfactory as more than 70% of the wormholes were detected compared to 50% for TTpHA. However, when cognizance is taken of the overall wormhole detection performance, TTpHA is noticeably superior, since it detects all wormholes types with greater flexibility than M-TTM at a consistently high rate both indoors and outdoors even when *TR=100ns*, while M-TTM was unable to detect indoor 3-hop and 4-hop wormholes at all.

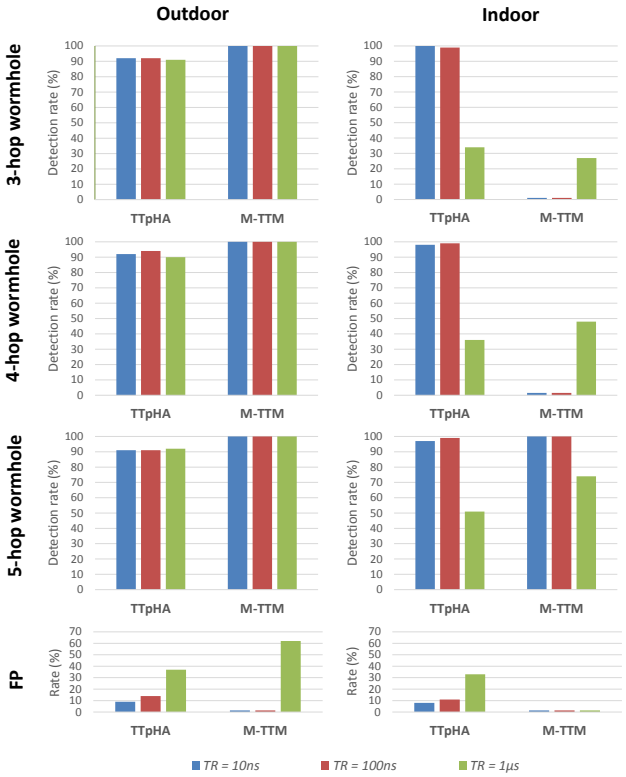

Fig. 4. Comparative TTpHA and M-TTM wormhole detection performance and FP detections for different wormhole lengths and TR values.

While the FP rate tends to increase for TTpHA with increasing TR values, the rate never exceeds 13% when $TR \leq 100ns$ in either of the tested environments. This is a satisfactory outcome since there still exists an 87% probability of finding the shortest route between the source and destination nodes. When $TR=1\mu s$ the FP rates for the outdoor and the indoor environments are 37% and 32% respectively, which although high is still acceptable since on average < 2 healthy routes need to be requested and checked to find a useful route. Hence, this

confirms that TTpHA functions outdoors with existing off-the-shelf *IEEE 802.11n compliant* wireless hardware. The wormhole detection rate of M-TTM was indoors, as for TTpHA, unchanged for all tested TR values. However, for $TR=1\mu s$, M-TTM generated a FP rate of 62% which is high since this means in less than 40% of cases, the shortest route is available for communication. The high FP rate for M-TTM outdoors is caused by $\frac{PTT_{MAX}-R}{S}=166ns$ which is $<<TR=1\mu s$, so it is very likely that a healthy *measured* $RTT_{i,i+1}$ > *expected* $RTT_{i,i+1}$.

C. Computational and Network Traffic Overheads

The only additional processing costs incurred by TTpHA in comparison with TTHCA and M-TTM, are at the source node related to the Q-test outlier technique used to calculate Θ in (3). This involves determining and ranking $PTT_{i,i+1}$ values with complexities $O(HC)$ and $O(HC^2)$ respectively. The additional overhead is negligible since HC is a very small value. At each intermediate node, PTT_i has to be computed and inserted to a new RREP packet parameter which is not required in TTHCA. This involves one operation and a $32 \cdot HC_i$ *bits* larger RREP than in TTHCA, where HC_i refers to the HC from the intermediate node i to the destination. While all these operations except ranking are also required in M-TTM, the PTT_i values are calculated at the source and the corresponding RREP packets are $3 \cdot 32 \cdot HC_i$ *bits* longer than those in TTpHA. To summarize, as well as being a more flexible wormhole detection solution, TTpHA consistently offers significantly superior wormhole detection performance in comparison with TTHCA and M-TTM, with minimal additional computation and network traffic costs being incurred.

IV. CONCLUSION

This paper has presented a *packet traversal time per hop analysis* (TTpHA) wormhole attack detection algorithm based on *traversal time and hop count analysis* (TTHCA) offering superior wormhole detection accuracy by analyzing *packet traversal time* (PTT) for each hop rather than PTT per hop count. TTpHA is significantly more flexible than related PTT-based solutions, including TTHCA and M-TTM, since it employs a dynamic threshold for the maximum permissible PTT between two legitimate nodes for adaption to prevailing MANET conditions and variable radio ranges. Critical simulation results evaluations showed that TTpHA provided accurate wormhole detection performance in both indoor and outdoor environments while the comparators, TTHCA and M-TTM, were only applicable in the outdoor environment without manual adjustments of their fixed thresholds. The results also indicated that in outdoor environments with long radio ranges, TTpHA can be implemented using low timestamp resolution *off-the-shelf* wireless hardware, while providing consistently high wormhole detection rates. Concomitantly, the costs in terms of false positive rates and the corresponding computational and network overheads remain pragmatically low.

REFERENCES

[1] S. Agrawal, S. Jain, and S. Sharma, "A survey of routing attacks and security measures in mobile ad-hoc networks," *Journal of Computing*, vol. 3, pp. 41-48, 2011.

[2] J. Karlsson, L. S. Dooley and G. Pulkkis, "Routing security in mobile ad-hoc networks," *Issues in Informing Science & Information*, vol. 9, pp. 369-383, 2012.

[3] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *IEEE INFOCOM*, Apr. 2003.

[4] M. Khabbazian, H. Mercier and V. K. Bhargava, "NIS02-1: Wormhole attack in wireless ad hoc networks: Analysis and countermeasure," in *IEEE GLOBECOM, Nov. 2006.*

[5] M. Khabbazian, H. Mercier and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Trans. on Wirel. Commun.,* vol. 8, pp. 736-745, 2009.

[6] H. S. Chiu and K.-S. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," in *ISWPC*, Jan. 2006.

[7] S- Choi, D.-Y. Kim, D.-H. Lee and J.-I. Jung, "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks," in *IEEE SUTC*, Jun. 2008.

[8] P. V. Tran, L. X. Hung, Y. Lee, S. Lee and H. Lee, "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks," in *IEEE CCNC*, Jan. 2007.

[9] S. Qazi, R. Raad, Y. Mu and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," *Journal of Network and Computer Applications,* vol. 36, pp. 582-592, 2013.

[10] J. Karlsson, L. S. Dooley and G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," *Sensors*, vol. 11, pp. 11122-11140, 2011.

[11] C. P. Vandana and F. S. Devaraj, "WAD-HLA: Wormhole Attack Detection Using Hop Latency And Adjoining Node Analysis in MANET," *International Journal of Engineering Research & Technology*, vol. 2, 2013.

[12] [J. Zhou, J. Cao, J. Zhang, C. Zhang and Y. Yu, "Analysis and countermeasure for wormhole attacks in wireless mesh networks on a real testbed," in *IEEE AINA*, Mar. 2012.

[13] V. Mahajan, M. Natu and A. Sethi, "Analysis of wormhole intrusion attacks in MANETS," in *IEEE MILCOM*, Nov. 2008.

[14] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *IEEE WMCSA*, Feb. 1999.

[15] S. Jen, C. Laih and W. Kuo, "A hop-count analysis scheme for avoiding wormhole attacks in MANET," *Sensors,* vol. 9, pp. 5022-5039, 2009.

[16] F. E. Grubbs, "Procedures for Detecting Outlying Observations in Samples," *Technometrics*, vol. 11, no. 1, pp. 1-21, 1969

[17] J. W. Tukey, Exploratory Data Analysis, Reading, Addison-Wesley, 1977.

[18] R. B. Dean and W. J. Dixon, "Simplified Statistics for Small Numbers of Observations," *Anal. Chem.,* vol. 23, pp. 636-638, 1951.

[19] D. B. Rorabacher, "Statistical treatment for rejection of deviant values: critical values of Dixon's Q parameter and related subrange ratios at the 95% confidence level," *Anal. Chem.,* vol. 63, pp. 139-146, 1991.

[20] S. P. Verma and A. Quiroz-Ruiz, "Critical Values for Six Dixon Tests for Outliers in Normal Samples up to Sizes 100, and Applications in Science and Engineering," *Revista Mexicana de Ciencias Geológicas*, vol. 23, no. 2, pp. 133-161, 2006.

[21] J. Karlsson, L. S. Dooley and G. Pulkkis, "Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm," *Sensors,* vol. 13, pp. 6651-6668, 2013.

[22] ns, "The Network Simulator - ns-2," [Online]. Available: http://www.isi.edu/nsnam/ns/. [Retrieved 7 June 2016].

[23] A. Goldsmith, Wireless Communications, Cambridge, Cambridge University Press, 2005

[24] XILINX, "LogiCORE IP AXI 10-Gigabit Ethernet v1.1 Product Guide for Vivado Design Suite," 18 December 2013. [Online]. Available: http://www.xilinx.com/support/documentation/ip_documentation/axi_10g_ethernet/v1_1/pg157-axi-10g-ethernet.pdf. [Retrieved 7 June 2016].

[25] Microsemi, "MAX24288 IEEE 1588 Packet Timestamper and Clock and 1 Gbps Parallel to Serial MII Converter," January 2013. [Online]. Available: http://www.microsemi.com/document-portal/doc_view/126640-max24288-data-sheet-2013-01. [Retrieved 7 June 2016].