Defence Research and Development Canada
Recherche et développement pour la défense Canada

Detecting wormholes in mobile ad hoc networks through hop count analysis

J. David Brown

Defence R&D Canada – Ottawa

Technical Memorandum
DRDC Ottawa TM 2012-118
December 2012

Canada

Detecting wormholes in mobile ad hoc networks through hop count analysis

J. David Brown
Defence R&D Canada – Ottawa

Defence R&D Canada – Ottawa
Technical Memorandum
DRDC Ottawa TM 2012-118
December 2012

Principal Author

Original signed by J. David Brown

J. David Brown

Approved by

Original signed by Julie Lefebvre

Julie Lefebvre
Head/Cyber Operations Section

Approved for release by

Original signed by Chris McMillan

Chris McMillan
Head/Document Review Panel

Abstract

This report proposes a new method to reliably detect wormhole attacks in mobile ad hoc networks (MANETs) by carefully observing the propagation of standard routing control packets through the network. The method is compatible with standard routing techniques and does not require additional hardware or sophisticated processing. The detection scheme is introduced and motivated using an intuitive argument, following which a mathematical analysis is performed that supports the heuristics. A simulation of the scheme demonstrates its effectiveness in dense MANETs and confirms the theory. Suggestions for future development are proposed to further enhance detection accuracy.

Résumé

Dans le présent rapport, on propose une nouvelle méthode de détection fiable des attaques du trou noir contre des réseaux mobiles ad hoc (Mobile Ad Hoc Network - MANET) reposant sur l'observation attentive de la propagation de paquets de contrôle de routage communs dans ces réseaux. Cette méthode est compatible avec les techniques de routage courantes et ne nécessite aucun matériel supplémentaire ou traitement de pointe. On présente et soutient l'algorithme de détection au moyen d'une argumentation intuitive suivie d'une analyse mathématique qui appuie la méthode de l'heuristique. Le rapport comporte les résultats de simulations montrant l'efficacité de l'algorithme au sein de MANET denses et confirmant la théorie énoncée. On y propose également de futurs développements visant à améliorer davantage l'exactitude de la détection.

This page intentionally left blank.

Executive summary

Detecting wormholes in mobile ad hoc networks through hop count analysis

J. David Brown; DRDC Ottawa TM 2012-118; Defence R&D Canada – Ottawa; December 2012.

Background: While mobile ad hoc networks (MANETs) offer the promise of rapidly deployable and flexible communications, adopting them for use in practice requires that they be robust against attack. How best to secure MANETs against information loss and denial of service is an active area of research in both academia and industry. The wormhole attack is one of the most serious attacks that can be mounted against a MANET and is also one of the most difficult to defend against. By tunneling legitimate control packets between two malicious nodes, a wormhole distorts the perceived topology of the network and breaks standard routing protocols. Although a number of algorithms have been proposed to detect and avoid wormholes, many of these rely on changes to standard protocols or mandate that mobile devices be equipped with special hardware.

Principal results: This paper introduces a method to detect wormholes that can be implemented by making use of standard MANET routing protocols and without any special hardware. To detect whether it is under attack by a wormhole, a node initiates a network flood and analyzes flood propagation statistics collected by its neighbours; to simplify implementation, the network flood can be implemented using standard route request messages from the popular ad hoc on demand distance vector (AODV) routing protocol. The detection algorithm is mathematically analyzed, providing further insight into its operation; its correctness and effectiveness are demonstrated by simulation.

Significance of results: The results of this report demonstrate a non-invasive method for wormhole detection that does not consume significant additional bandwidth or require additional resources. Such detection techniques are important because they allow for the securing of MANETs by observing naturally occurring parameters that exist as a consequence of the network's standard operation. Through simulation, the detection scheme is shown to be effective in dense MANETs, successfully detecting more than 90% of wormholes with a false positive rate of less than 10%.

Future work: The detection mechanism proposed here computes a simple statistic based on the propagation of flood packets among a node's immediate neighbours. By considering the propagation of such flood packets to more distant neighbours,

the detection mechanism may prove more robust and could further improve accuracy. Additionally, incorporating realistic mobility models and node distributions may lend additional weight to these results.

Sommaire

Detecting wormholes in mobile ad hoc networks through hop count analysis

J. David Brown ; DRDC Ottawa TM 2012-118 ; R & D pour la défense Canada – Ottawa ; décembre 2012.

Contexte : Les réseaux mobiles ad hoc (Mobile Ad Hoc Network - MANET) offrent la perspective de communications adaptatives déployables rapidement. Toutefois, leur intégration à des systèmes pratiques nécessite qu'ils soient résistants aux attaques. On cherche activement les meilleurs moyens de protéger les MANET contre la perte de données et de service demeure un domaine de recherche actif. L'une des attaques la plus dommageable et difficile à éviter est celle du trou noir. Cette dernière déforme la topologie perçue d'un MANET et détruit les protocoles de routage standard en effectuant une tunnellisation de paquets de contrôle valides entre deux nœuds malveillants. Bien qu'un certain nombre d'algorithmes aient été proposés pour détecter et éviter cette attaque, un grand nombre d'entre eux nécessitent la modification de protocoles standard ou l'ajout de matériel spécial à des appareils mobiles.

Résultats : Dans le rapport, on présente une méthode de détection des attaques du trou noir pouvant être mise en œuvre au moyen de protocoles de routage de MANET standard sans matériel particulier. Pour détecter si une attaque provient d'un trou noir, un nœud déclenche une inondation de réseau dont il analyse les statistiques de propagation recueillies par les nœuds avoisinants. On peut simplifier le déclenchement de l'inondation à l'aide de messages de demande de route standard reposant sur le populaire protocole de routage à vecteur de distance à la demande pour réseaux ad hoc (Ad-hoc On Demand Distance Vector - AODV). On présente également une analyse mathématique de l'algorithme de détection, afin d'expliquer son fonctionnement de façon plus approfondie, puis on démontre son exactitude et son efficacité grâce à des simulations.

Portée : Le présent rapport porte sur une méthode non invasive de détection des attaques du trou noir qui n'exige par une importante largeur de bande supplémentaire ou de ressource additionnelle. L'élaboration d'une telle méthode est importante, car elle permet de protéger un MANET par l'observation de paramètres découlant du fonctionnement normal du réseau. Des simulations ont montré que l'algorithme de détection est efficace dans le cas de MANET denses ; il a détecté plus de 90 % des attaques du trou noir avec un taux de fausses alarmes inférieur à 10 %.

Recherches futures : Le mécanisme de détection proposé effectue des calculs statistiques simples fondés sur la propagation de paquets d'inondation parmi les nœuds avoisinants du nœud d'inondation. En évaluant cette propagation vers des nœuds voisins plus éloignés, on pourrait rendre le mécanisme de détection encore plus robuste et exacte. De plus, l'ajout de modèles de mobilité pourrait appuyer les résultats obtenus.

Table of contents

Acknowledgements

Thank you to Mazda Salmanian, Stephane Lemieux, and Peter Mason for many interesting discussions and valuable suggestions regarding the development and presentation of this work.

1 Introduction

Mobile ad hoc networks (MANETs) are self-organizing and self-configuring networks of mobile wireless nodes that operate without any centralized control. MANETs make possible the rapid deployment of communication infrastructures where none exists and facilitate the creation of low-power, low-cost sensor networks. Because nodes in a MANET can operate as store-and-forward routers, high bandwidth point-to-point communication links in the MANET can extend their reach across multiple nodes by "multi-hopping" data through intermediate nodes in the network. The ability to set up high bandwidth wireless networks on-the-fly and independent of existing infrastructure is a valuable capability that facilitates rapid collaboration, information sharing, and crisis management.

Although MANETs offer a number of advantages, securing MANETs against attack has proven difficult. Wireless communications make eavesdropping very simple, wireless signals can be jammed, MANETs have no centralized authority to enforce a network security policy or analyze traffic flows, and the dynamic nature of a MANET means that network topology is always in flux. One of the most severe attacks against a MANET is the wormhole attack, whereby a malicious node in one part of the network tunnels traffic to a remote partner who rebroadcasts the traffic in another section of the network. This attack is very difficult to detect and fundamentally disrupts effective route discovery.

This report presents a novel technique to detect wormholes in a MANET. The solution requires no special hardware and is relatively simple to implement. The detection scheme relies on a node in the network initiating a network flood and subsequently analyzing the statistics from neighbouring nodes regarding the propagation of the flood packets. An explanation of the technique is presented, followed by a mathematical analysis that demonstrates its effectiveness under a reasonable set of assumptions. The results of extensive simulations are provided as well, validating the mathematical analysis.

The remainder of this report is organized as follows. Section 2 discusses the wormhole attack in some detail and provides a summary of current state-of-the-art wormhole detection techniques. In Section 3, the detection algorithm is presented and analyzed; its performance is evaluated through simulation. Real-world implementation details are considered in Section 4, leading to recommended future research in Section 5. Finally, Section 6 presents a summary and conclusion.

2 Background: MANETs and wormhole attacks

This section presents the background information necessary to appreciate the proposed defence against wormholes. After a few words about MANETs, the wormhole attack is explained in detail, followed by a discussion of currently known defences against wormholes.

2.1 Mobile ad hoc networks

Mobile ad hoc networks are self-organizing, self-configuring networks of mobile devices that communicate over limited-range wireless links and without any central coordinating authority. In a MANET, every node can act as a router, such that a source node can communicate with a destination node by forwarding traffic along a route consisting of several intermediate nodes. A number of routing protocols have been developed to enable this multi-hop forwarding among nodes in a MANET. Two popular routing protocols—both published as IETF Internet standards—are the ad hoc on-demand distance vector (AODV) routing protocol (defined in RFC 3561 [1]) and the optimized link state routing (OLSR) protocol (defined in RFC 3626 [2]).

AODV is a so-called reactive routing protocol, since it initiates the process to find a route between a source and destination only when the source has information to transmit. In a MANET using AODV, a source node finds a route to a destination node by broadcasting a route request (RREQ) message to all nodes within range. The RREQ is rebroadcast by recipient nodes until it reaches the intended destination, which then responds to the source node with a route reply (RREP) message indicating the shortest observed path between source and destination. The RREQ broadcast process is essentially a "source flood" since the source node floods the network with messages to find the destination.

In contrast to AODV, OLSR is a proactive routing protocol, since nodes in an OLSR network send out periodic control messages whether or not they have data to transmit. In a MANET using OLSR, each node identifies itself to its neighbours by periodically sending out so-called HELLO messages. The HELLO messages allow nodes in the MANET to construct local two-hop topologies; complete routing tables are constructed with the help of multipoint relay nodes, whose identification is specified by OLSR.

2.2 The wormhole attack

The wormhole attack is one of the most studied attacks against MANETs partly because it is one of the most severe. It is notoriously difficult to detect and can be mounted relatively easily and inexpensively. In one manifestation of the attack, a malicious node in one area of the MANET listens to all packets within range and forwards the packets to a colluding partner using an out of band link. This is depicted in Figure 1, where w and $w*$ are the two colluding partners.

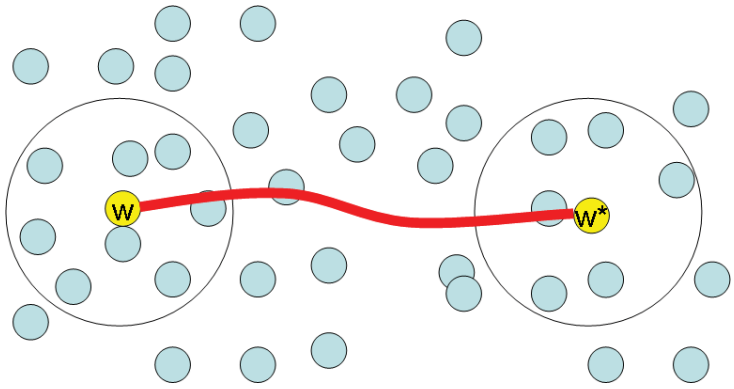


Figure 1: *A wormhole exists between w and $w*$. In this attack, all nodes within range of w believe themselves to be one-hop neighbours of nodes within range of $w*$.*

By forwarding all packets, the wormhole makes it appear to nodes within range of w that they are neighbours of the nodes within range of $w*$. This leads to the situation where the wormhole link appears to be the "fastest" or "shortest" route between many nodes in the network. Nodes will forward their traffic through the wormhole, placing the attacker in a position of extreme advantage. Not only does the wormhole distort the perceived topology of the network, it means that the attacker can record all traffic, selectively drop control packets to disrupt quality of service, or launch a denial-of-service attack by dropping all data packets. It was shown in [3] that a single strategically placed wormhole can disrupt on average one third of the traffic traversing the MANET (i.e., one third of all routes between nodes will flow through the wormhole), making this a formidable attack. Furthermore, encrypting data and control packets offers little defence against wormholes, as the malicious nodes can easily tunnel the information without decrypting it.

A wormhole attack is effective against both of the two widely-used MANET routing protocols: OLSR and AODV. In the case of OLSR, since a wormhole tunnels all HELLO messages, nodes are led to believe they are one-hop neighbours with distant non-neighbouring nodes. Similary, in AODV a wormhole between the source and destination would tunnel the RREQ messages, leading the destination to believe that the shortest path includes the wormhole. In both cases, tunneling the control

messages distorts the perceived topology of the network and leads the wormhole to assume control of traffic between source and destination nodes.

2.3 Current defences against wormholes

A significant amount of research has been devoted to detecting and avoiding wormhole attacks. A myriad of solutions have been proposed; many of these solutions require specialized hardware or changes to routing protocols, although some of them are less invasive and detect wormholes under specific network assumptions. A summary of popular detection techniques is provided below, along with a brief description of their limitations.

Location-based solutions

One of the most cited examples of wormhole defence is the packet leash, discussed in [4]. The authors propose a so-called geographic leash, whereby source nodes embed geographic location information (e.g., GPS data) in transmitted packets and receiving nodes accept packets only from source nodes within some bounded distance. Also proposed are temporal leashes, which do not require location information but instead place strict limits on the length of time a packet may take to move from one node to another. Both types of leashes require specialized hardware: positioning hardware or tightly synchronized clocks.

In [5], the authors present a detection scheme called End-to-End Detection of Wormhole Attack (EDWA). In the EDWA scheme, a source node in an AODV MANET sends an RREQ message and waits for the RREP. The authors modify AODV such that the destination node includes its location in the RREP. Based on the physical distance between source and destination, the source can compute the expected number of hops for a route to the destination—paths with fewer than this number are suspected to contain wormholes. While this method may be effective, it presumes all nodes are equipped with positioning hardware and desire their positions to be known; furthermore it requires a modification to AODV.

Route and hop count analysis solutions

A statistical approach dubbed Statistical Analysis of Multi-path (SAM) is proposed in [6]; the authors observe that since a wormhole presents an attractive path for network traffic, it is likely that a wormhole link will occur with very high frequency in routing tables. The detection approach is to search for anomalies in route frequency, declaring a wormhole to be present if a particular link has much higher frequency of occurrence than all others. This method is intuitively satisfying, however it leaves unanswered

the question of what is an appropriate link occurrence frequency for a general case (e.g., it is possible there is a favourable link that connects many nodes).

A proactive approach called multipath hop-count analysis (MHA) is proposed in [7], where a source node selects among multiple available paths to a destination. These paths are obtained using a modified AODV protocol and their lengths are computed (with length measured in terms of number of hops). The authors suggest that routes with too small a hop count are unhealthy as they may be indicative of a wormhole; the MHA technique requires that nodes avoid these routes. While this technique may prove effective in avoiding wormholes, it can result in a high false positive rate if there is little discrepancy between valid route lengths and wormhole route lengths.

Round trip timing solutions

The Wormhole Attack Prevention (WAP) algorithm presented in [8] proposes to detect wormholes by having each node maintain a table of its neighbours and identify anomalous behaviour. Assuming the MANET uses AODV, WAP requires that when a node sends an RREQ message it will start a timer and record how long it takes to hear its neighbours rebroadcasting the message. If the wait time for a neighbour to rebroadcast exceeds some threshold, the neighbour is declared to be affected by the wormhole. Difficulties with this approach involve generating a reasonable estimate of wait time; if packet processing times are unpredictable then this method breaks down.

In [9], a protocol similar to AODV is proposed that allows a destination node to identify a set of disjoint paths between itself and the source. The source computes the round trip travel time for messages sent along each of these paths and thereby determines an average "delay per hop" value for the MANET. If a particular route exhibits a higher than expected delay per hop, this is indicative of a wormhole. The authors call this technique DelPHI: Delay Per Hop Indication Wormhole Detection. Like the WAP scheme, DelPHI is loses its effectiveness if packet processing times are less predictable.

Graph-based solutions

A clever approach for detection that is valid for both AODV and OLSR MANETs is presented in [10]. The idea relies on identifying so-called "forbidden structures" in the connectivity graph of the MANET. For instance, if two non-neighbouring nodes share several independent neighbours, it can be shown that this violates certain assumptions about node connectivity in the MANET (e.g., all nodes have equal range, unit-disk model) and could only be caused by a wormhole. This algorithm tends to work best in dense MANETs with known topologies.

OLSR protocol analysis solutions

An approach for wormhole detection in OLSR MANETs is presented in [11, 12] and relies on detecting anomalies in the arrival time of HELLO messages. It is observed that HELLO messages tunneled through a wormhole are subject to an increased variability in arrival time. By computing the power spectral density of the arrival time sequence, it is possible to observe the signature of the delay function added by the wormhole. This detection approach has proven to be effective and non-invasive, but operates only on OLSR networks. Further research in [13] has extended this technique to work for any network (i.e., not just MANETs using OLSR) by sending probe messages that enable the detection of timing anomalies.

3 A hop-count algorithm for detecting wormholes: analysis and results

Section 2 described the wormhole attack on a MANET and listed some of the defences available against this attack. In this section, we present a defence against wormhole attacks that relies on sending out probe packets using a simple network flooding algorithm. Our solution requires no special hardware and proposes a simple yet effective detection metric. We begin by describing the algorithm itself, along with an explanation for why it works. Next we present a mathematical analysis of the algorithm that supports the heuristic explanation, and finally we demonstrate its efficacy through simulation.

3.1 Detecting wormholes by counting packet hops

We propose that any node in the MANET can initiate a simple network flood procedure and its neighbouring nodes can compute statistics based on the propagation of flood packets throughout the network. Using the observed statistics, we show that it is possible to determine whether or not the MANET is under attack.

For our purposes, a flood packet is a control message[1] that contains at a minimum the following information: a node identifier and a value *hop_count*, which indicates how many "hops" or nodes a particular flood packet has traversed. For a node X_i broadcasting a flood packet with a hop count of j, we adopt the notation $< i, hop\_count = j >$ to denote its flood packet. We assume also that each node X_i maintains a Boolean internal variable, tx_yet_i, which indicates whether or not X_i has broadcast a flood packet.

In simple terms, the flooding procedure requires that every node receiving a flood packet must increment the value of *hop_count* and rebroadcast the flood packet, assuming the node has not already sent this flood packet. The details of the flooding algorithm are as follows:

Figure 2(a) shows how a flood propagates through a MANET under normal, non-compromised conditions. Node X_S initiates a flood, broadcasting a message with $hop\_count = 1$; nodes within range of X_S re-broadcast this message with $hop\_count = 2$, and so on. Not shown in the figure is that X_S also observes the broadcast messages $< a, hop\_count = 2 >$ and $< b, hop\_count = 2 >$ from nodes X_a and X_b respectively; X_S takes no action upon receipt of these messages since $tx\_yet_S = true$. Likewise,

[1] While we assume a general control message in this section, in Section 4 we discuss how AODV could be used for this purpose.

Algorithm 1 Network flood initiated by node X_S

1. All nodes in the network begin with their tx_yet flags set to *false*.

2. Node X_S initiates a flood procedure by broadcasting $< S, hop\_count = 1 >$ and setting $tx\_yet_S = true$.

3. If any node X_n receives a flood packet $< m, hop\_count = j >$ and $tx\_yet_n = false$, X_n will broadcast $< n, hop\_count = j + 1 >$ and will set $tx\_yet_n = true$.

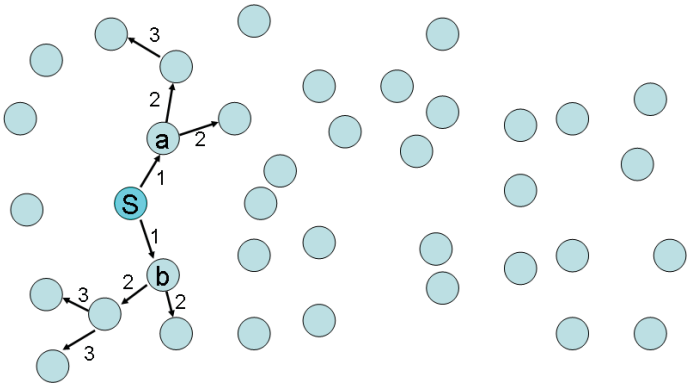
X_a and X_b observe the responses from their neighbours with $hop\_count = 3$, and so on.

Now, consider how a flood propagates through a network when X_S is under a wormhole attack, as depicted in Figure 2(b). In this case, when X_S broadcasts $< S, hop\_count = 1 >$ to initiate the flood, this message will be seen by nodes X_a and X_b (since they are neighbours of X_S) and will also be seen by nodes X_c and X_d by virtue of the wormhole between malicious nodes w and $w*$. At this point nodes X_a, X_b, X_c, and X_d will all broadcast flood packets with $hop\_count = 2$. In this simple example, X_S observes twice as many $hop\_count = 2$ messages under a wormhole attack since it will see the broadcasts of X_a, X_b, X_c, and X_d. In fact, with a little thought, it becomes clear that *all* nodes within range of the wormhole nodes w or $w*$ will observe more $hop\_count = 2$ messages under wormhole conditions than under normal conditions. This occurs because the wormhole has the effect of artificially increasing the number of neighbours seen by the nodes in its broadcast range. Note that although a node may observe additional hop count messages, the node will take no additional action if $tx\_yet = true$.

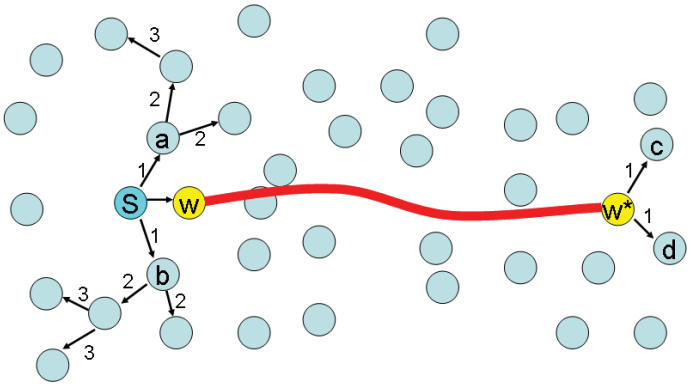
Unfortunately, simply examining the number of $hop\_count = 2$ messages seen by each node in the MANET does not provide enough information to detect a wormhole since we have no baseline to say what a "normal" number of $hop\_count = 2$ messages should be. However, once all the nodes surrounding wormhole node $w*$ have sent their respective $hop\_count = 2$ packets, they will all have $tx\_yet = true$. These nodes form a buffer around node $w*$ such that no $hop\_count = 3$ messages will reach the wormhole to be tunneled across. The result is that the wormhole does not increase the number of $hop\_count = 3$ messages to the same extent as the $hop\_count = 2$ messages.

Suppose that a monitoring system exists whereby it is possible to to determine the the number of $hop\_count = n$ messages observed by every node in the network. We define H_n to be the total number of $hop\_count = n$ messages seen by all nodes in the MANET that received the flood initialization packet $< S, hop\_count = 1 >$.

Based on the discussion above, we suggest that H_2 should be proportionally larger



(a)



(b)

Figure 2: *(a) In non-compromised network a source node, X_S, initiates a flood by broadcasting a flood packet with hop_count = 1. Nodes that receive the flood packet increment the hop_count number and rebroadcast the packet. The value of hop-count is shown next to the arrows depicting the propagation of the packets.*
(b) In network compromised by a wormhole, the flood packets initiated by source node, X_S, are tunneled through the wormhole.

than H_3 when X_S is attacked by a wormhole. Our detection system measures the ratio $H_{2/3} = \frac{H_2}{H_3}$, compares it to a threshold τ, and declares that X_S is under a wormhole attack if $H_{2/3} > \tau$. In the following section, we analyze this detection metric and describe how to select an appropriate value for τ.

3.2 Analysis of the hop count algorithm

In order to verify our hypothesis, we wish to analytically compute typical values of H_2 and H_3 for a general MANET. To begin, consider a MANET with nodes randomly distributed in a given area according to a uniform distribution with density δ nodes per unit area. Assume further that each node has a range R, such that any two nodes

separated by distance less than or equal to R are considered "neighbours" and can directly overhear one another's transmissions.

Analysis for the non-wormhole case

Under the simple assumptions above, consider the case where a node X_S initiates a network flood by transmitting $< S, hop\_count = 1 >$. For a node X_z within range of X_S, we would expect that X_z would observe all $hop\_count = 2$ messages from any nodes located in the areas where the ranges of X_S and X_z overlap, as depicted in Figure 3. The intuition for this is the fact that only those nodes within range of X_S will generate a message with $hop\_count = 2$, and X_z hears only those nodes within its own range—thus we are interested in the intersection of these two areas.

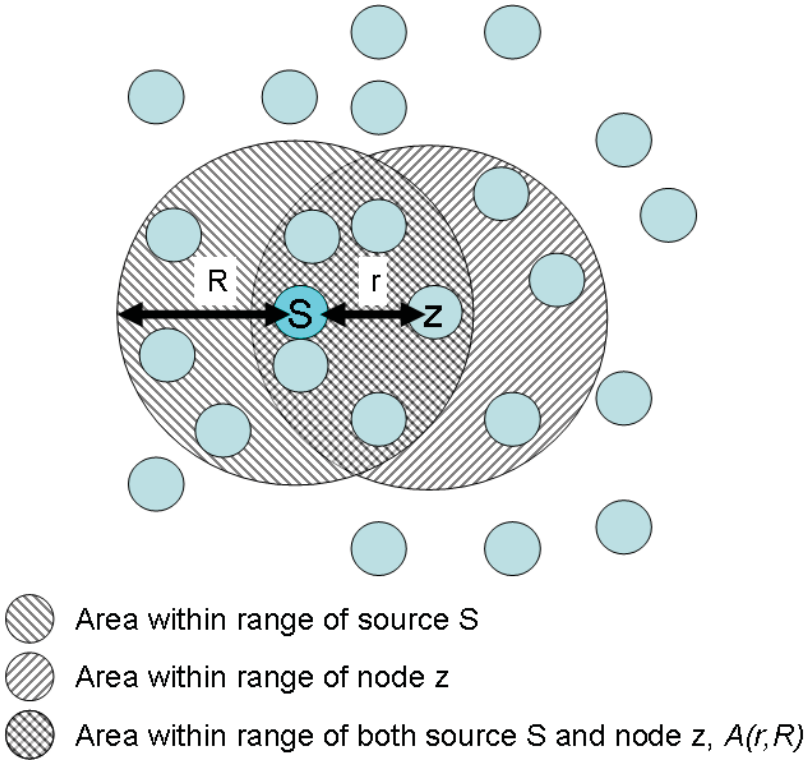


Figure 3: *Node X_z observes flood packets with with $hop\_count = 2$ from all nodes in range of both X_S and X_z. X_z observes flood packets with $hop\_count = 3$ from nodes within range of X_z but out of range of X_S.*

We denote by $A(r, R)$ the area of overlap depicted in Figure 3, where r is the distance between X_S and X_z. Thus, the expected value for the number of $hop\_count = 2$ messages seen by X_z is $h_z(2) = \delta \cdot A(r, R)$, where we adopt the notation $h_i(n)$ to be the number of $hop\_count = n$ messages seen by node X_i.

To determine the expected number of *hop_count* = 2 messages observed by all nodes within range of X_S (as opposed to by the single node X_z) we consider a differential area *da* located at a distance r from X_S, where $r \leq R$.

The area *da* contains an expected $\delta \cdot da$ nodes, and each of these nodes will observe $\delta \cdot A(r, R)$ messages with *hop_count* = 2. Thus, the total number of *hop_count* = 2 messages is given by the integral of the product $(\delta \cdot da)(\delta \cdot A(r, R))$ over the circular area surrounding X_S. Converting *da* to polar coordinates, $da = r\ drd\theta$ and we can write

$$\overline{H_{2,NWH}} = \int_0^{2\pi} \int_0^R A(r, R)\delta^2 r dr d\theta, \tag{1}$$

where $\overline{H_{2,NWH}}$ denotes the expected number of *hop_count* = 2 messages observed in the network by nodes within range of X_S[2], assuming there is no wormhole present.

The area of the intersection of two circles separated by distance r, where the circles have equal radius, R, is given by

$$A(r, R) = 2R^2 \arccos\left(\frac{r}{2R}\right) - \frac{r}{2}\sqrt{4R^2 - r^2}. \tag{2}$$

Thus, we can evaluate $\overline{H_{2,NWH}}$ as

$$\begin{aligned}
\overline{H_{2,NWH}} &= \delta^2 \int_0^{2\pi} \int_0^R \left[2R^2 r \arccos\left(\frac{r}{2R}\right) - \frac{r^2}{2}\sqrt{4R^2 - r^2}\right] dr d\theta & (3)\\
&= (\delta^2 R^4)(2\pi)\left[\pi - \frac{3\sqrt{3}}{8} - \arccos\left(\frac{1}{2}\right) - \arcsin\left(\frac{1}{2}\right)\right] & (4)\\
&= (\delta^2 R^4)(2\pi)\left[\pi/2 - \frac{3\sqrt{3}}{8}\right], & (5)
\end{aligned}$$

where a table of integrals in [14] was used to obtain the closed form solution of the integral and the final line uses the fact that $\arccos(\frac{1}{2}) + \arcsin(\frac{1}{2}) = \pi/2$.

We now repeat this analysis to determine the expected number of *hop_count* = 3 messages observed by nodes within range of X_S. Once again, we consider a node X_z within range of X_S, as depicted in Figure 3. Node X_z will hear messages with *hop_count* = 3 from all nodes in the range of X_z[3] excluding the area where X_z and X_S overlap. The overlap is excluded since nodes in this range will have *tx_yet* = *true*

[2] i.e., nodes that receive message $< S, hop\_count = 1 >$

[3] All nodes within this range will have heard the message $< z, hop\_count = 2 >$ and will thus need to send a *hop_count* = 3 message.

since they sent *hop_count* = 2 messages already. Thus, we can write $h_z(3) = \delta \cdot (\pi R^2 - A(r,R))$, with $A(r,R)$ given by (2).

Proceeding as we did for $\overline{H_{2,NWH}}$, the total number of *hop_count* = 3 messages is found by integrating $h_z(3) \cdot (\delta \cdot da)$ over the range of X_S giving:

$$\begin{aligned}
\overline{H_{3,NWH}} &= \delta^2 \int_0^{2\pi} \int_0^R \left[\pi R^2 r - 2R^2 r \arccos\left(\frac{r}{2R}\right) + \frac{r^2}{2}\sqrt{4R^2 - r^2} \right] dr d\theta \quad (6) \\
&= (\delta^2 R^4)(2\pi) \left[\pi/2 - \left[\pi/2 - \frac{3\sqrt{3}}{8} \right] \right] \quad (7) \\
&= (\delta^2 R^4)(2\pi) \left[\frac{3\sqrt{3}}{8} \right]. \quad (8)
\end{aligned}$$

Computing the ratio of the two measures of expected hop count we obtain

$$\begin{aligned}
H_{2/3,NWH} &= \frac{\overline{H_{2,NWH}}}{\overline{H_{3,NWH}}} \quad (9) \\
&= \frac{(\delta^2 R^4)(2\pi) \left[\pi/2 - \frac{3\sqrt{3}}{8} \right]}{(\delta^2 R^4)(2\pi) \left[\frac{3\sqrt{3}}{8} \right]} \quad (10) \\
&= \frac{4\pi\sqrt{3}}{9} - 1 \quad (11) \\
&\approx 1.42. \quad (12)
\end{aligned}$$

We observe that the ratio of expected total observed *hop_count* = 2 messages to expected total observed *hop_count* = 3 messages for nodes within range of the source node X_S is independent of the network density, δ, and node range, R, and forms a constant for the MANET, with $H_{2/3,NWH} \approx 1.42$.

Analysis for the wormhole case

We repeat the previous analysis—this time for a MANET in which a wormhole attack is mounted against node X_S (and nodes in its immediate environment). Suppose that a wormhole is created between two malicious nodes: one close to X_S and another distant malicious node X_{S*} as shown[4] in Figure 4. The wireless range of each malicious node is R, just as it is for friendly nodes. Using the standard assumptions of the operation of wormholes, it is assumed that the wormhole forwards all traffic—i.e.,

[4]Note that for the purposes of our analysis we presume that the wormhole near X_S is co-located with X_S to make the computations more tractable.

all flood packets are forwarded by the wormhole. Note that if the wormhole did not forward the flood packets, this would provide an easy way to detect its presence since it would immediately reveal the true neighbours of node X_S.

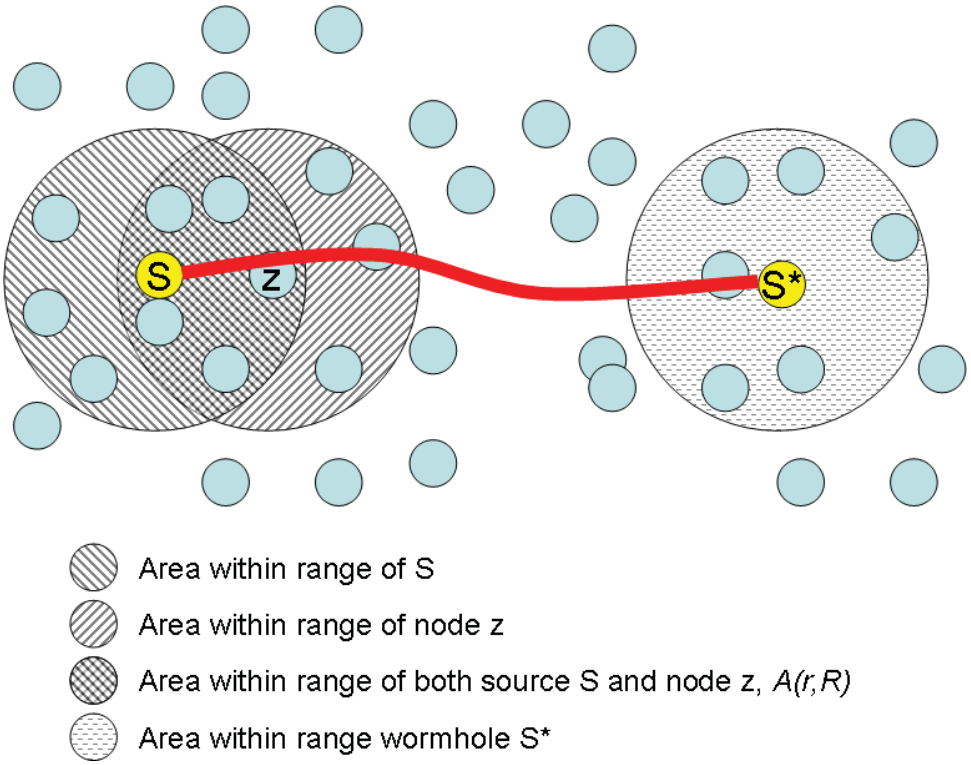


Figure 4: *Node X_z observes flood packets with with hop_count = 2 from all nodes in range of both X_z and X_S* and also *from nodes within range of X_{S*}. X_z observes flood packets with hop_count = 3 from nodes within range of X_z but out of range of X_S.*

To compute the expected number of *hop_count* = 2 messages observed by neighbours of X_S[5], we consider the messages observed by node X_z in Figure 4. As before, X_z will see *hop_count* = 2 messages from all nodes in the overlapping area of the ranges of X_S and X_z. In addition, under wormhole attack, X_z will observe *hop_count* = 2 messages from all nodes in the range of X_{S*}; this occurs since X_{S*} rebroadcasts the packet $< S, hop\_count = 1 >$ and all neighbours of X_{S*} respond with *hop_count* = 2 packets which are tunneled back to the origin of the wormhole and rebroadcast near X_S. Thus, $h_z(2) = A(r, R) \cdot \delta + \pi R^2 \cdot \delta$, where $A(r, R)$ is given in (2).

It is possible to reframe the argument made for a node X_z near X_S for a different node,

[5]Once again, we consider neighbours of X_S to be any node that observes $< S, hop\_count = 1 >$. In the wormhole case, nodes within range of X_{S*} will also observe $< S, hop\_count = 1 >$ and thus will count as "neighbours" of X_S.

X_{z*}, on the other side of the wormhole in the range of X_{S*}. Thus, the total number of *hop_count* = 2 messages observed by recipients of the packet $< S, hop\_count = 1 >$ is *twice* the integral of $h_z(2) \cdot (\delta \cdot da)$ over the range X_S[6], giving

$$\overline{H_{2,WH}} = 2\delta^2 \int_0^{2\pi} \int_0^R \left[\pi R^2 r + 2R^2 r \arccos\left(\frac{r}{2R}\right) + \frac{r^2}{2}\sqrt{4R^2 - r^2} \right] dr d\theta \quad (13)$$

$$= (\delta^2 R^4)(4\pi) \left[\pi/2 + \left[\pi/2 - \frac{3\sqrt{3}}{8} \right] \right] \quad (14)$$

$$= (\delta^2 R^4)(4\pi) \left[\pi - \frac{3\sqrt{3}}{8} \right]. \quad (15)$$

To compute the number of *hop_count* = 3 messages observed in the wormhole case, we note that none of the *hop_count* = 3 messages will reach the wormhole nodes since all nodes in the range of the wormhole nodes will have $tx\_yet = true$ after responding to the $< S, hop\_count = 1 >$ flood message. Thus, for our node X_z, the analysis is precisely the same as in the non-wormhole case. The total number of *hop_count* = 3 messages is double, however, since once again any argument we make for node X_z could be equally made for a node in the range of X_{S*}. Thus, $\overline{H_{3,WH}} = 2\overline{H_{3,NWH}}$, producing

$$\overline{H_{3,WH}} = (\delta^2 R^4)(4\pi) \left[\frac{3\sqrt{3}}{8} \right]. \quad (16)$$

Taking the ratio of $\overline{H_{2,WH}}$ and $\overline{H_{2,WH}}$ yields

$$H_{2/3,WH} = \frac{(\delta^2 R^4)(4\pi) \left[\pi - \frac{3\sqrt{3}}{8} \right]}{(\delta^2 R^4)(4\pi) \left[\frac{3\sqrt{3}}{8} \right]} \quad (17)$$

$$= \frac{8\pi\sqrt{3}}{9} - 1 \quad (18)$$

$$\approx 3.84. \quad (19)$$

As suggested by our heuristic argument in Section 3.1, we have proven that the ratio of the expected number of *hop_count* = 2 messages to *hop_count* = 3 messages seen by nodes in range of the source is larger under wormhole attack. The ratios of these expected values are constants, independent of network density and node range under our connectivity assumptions. In the following section, we simulate the performance of our detection scheme to evaluate its effectiveness.

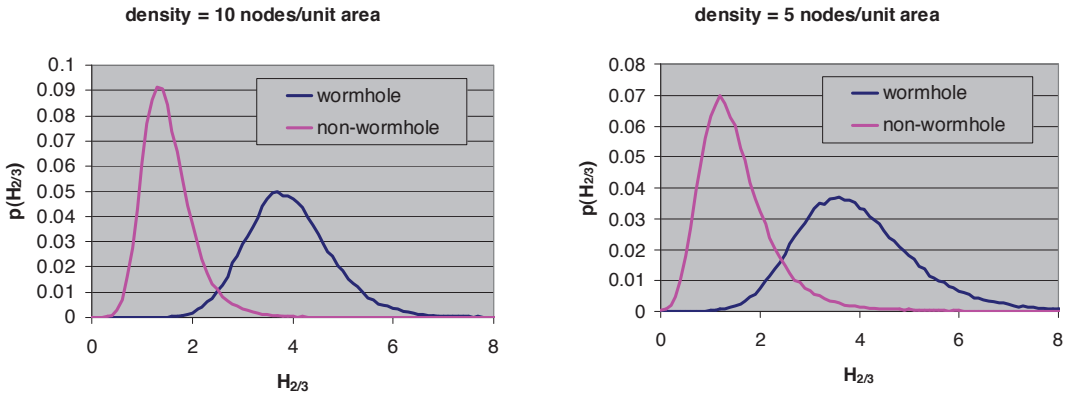
[6]it is twice the integral since we integrate once over the range of X_S and once over the equal range of X_{S*}

3.3 Simulated performance

To evaluate the proposed detection scheme, we ran simulations in MATLAB whereby a 12 unit by 12 unit area was populated with nodes randomly distributed according to a uniform distribution. All nodes were assumed to have a transmission range of $R = 1$ unit. We simulated a wormhole by introducing a node near the "source node" that was connected to another malicious node a distance of at least 5 units away. All traffic seen at one end of the wormhole was rebroadcast at the other end. Finally, we varied the density of the nodes to evaluate its effect on our scheme. We considered densities of $\delta = 2$, 3, 4, 5, and 10 nodes/unit^2.

For each density, we ran our simulation 100,000 times. In each run of the simulation, the flooding scheme was run on a network without a wormhole and then repeated on an identical network (i.e., all nodes in the same locations) where X_S was attacked by a wormhole. Measured values for the ratio $H_{2/3}$ were recorded for the wormhole and non-wormhole cases for every run.

Figure 5 shows the probability density function (pdf) for the observed values of $H_{2/3}$ in both wormhole and non-wormhole cases—i.e., the pdf for $H_{2/3,WH}$ and $H_{2/3,NWH}$. For a density of $\delta = 10$ nodes/unit^2 in Figure 5(a) we observe that *the pdf for the non-wormhole case peaks with a mean near* 1.4, as predicted by (12). Likewise, *the pdf for the wormhole case peaks with a mean near* 3.8, as predicted by (19). The means of the pdfs in Figure 5(b) for densities of $\delta = 5$ nodes/unit^2 have similar values.



(a) (b)

Figure 5: *The pdf of the ratio $H_{2/3}$ is plotted for both wormhole and non-wormhole cases. The peak of the non-wormhole pdf is very close to 1.4 and the peak of the wormhole pdf is very close to 3.8.*

While the pdfs in Figure 5 (a) and (b) show similar means, we note that the pdfs for $\delta = 5$ nodes/unit^2 are wider than those for $\delta = 10$ nodes/unit^2. Thus, although the means are invariant to node density—as discovered in Section 3.2—the distributions

are not. Thus, the success rate of our wormhole detector for randomly distributed nodes following a uniform distribution depends upon the node density and the selected threshold, τ, where a wormhole is declared if $H_{2/3} > \tau$.

Table 1: *Correct detection and false detection rates as a function of the threshold* τ.

		correct detection	false detection
$\tau = 2$	$\delta = 5$	97.9%	22.5%
	$\delta = 10$	99.8%	16.9%
$\tau = 2.5$	$\delta = 5$	92.1%	10.3%
	$\delta = 10$	97.2%	5.4%
$\tau = 3$	$\delta = 5$	80.1%	4.9%
	$\delta = 10$	88.9%	2.0%

The rate of *correct detection* of wormholes (i.e., the percentage of time the detector will identify a wormhole when one is present) is found by integrating the wormhole pdf from τ to infinity. The rate of *false detection* of wormholes (i.e., the percentage of time the detector declares a wormhole when there is none present) is found by integrating the non-wormhole pdf from τ to infinity. Table 1 summarizes the correct detection and false detection rates for $\delta = 5$ and $\delta = 10$ for a few choices of τ.

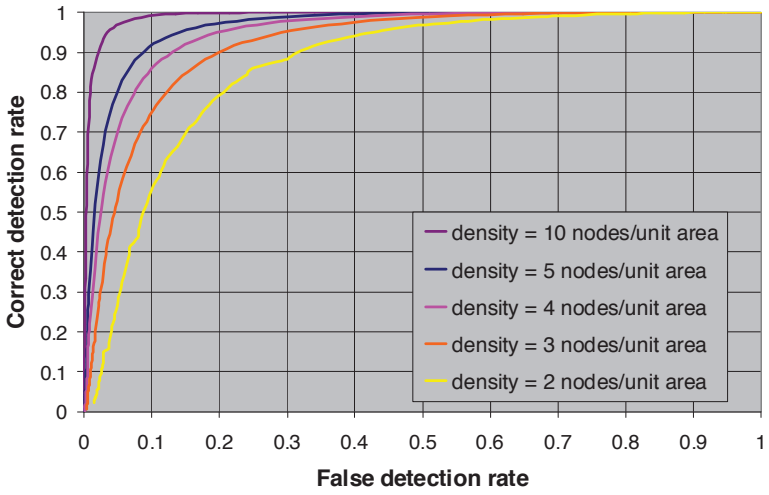


Figure 6: *Operating characteristic for the wormhole detection scheme demonstrating the tradeoff between true positives (correct detection of a wormhole) and false positives (detecting a wormhole when there is none present). Decreasing the detection threshold,* τ*, moves one further to the right along any curve (i.e., better detection rate but higher false positive rate).*

A quick glance at Table 1 shows that increasing τ yields a smaller false detection

rate at the expense of a lower correct detection rate. Also noted is the improved performance of the detection scheme in the higher density environment.

To completely characterize the detection scheme for all simulated densities, Figure 6 shows the operating characteristic of the detector, plotting correct detection rate versus false detection rate for densities of $\delta = 2$, 3, 4, 5, and 10 nodes/unit^2. The operating characteristic curves clearly show the effect of density on the detection scheme. For a desired correct detection rate, higher density environments yield a lower false positive rate. However, even with a density of $\delta = 2$ nodes/unit^2, the scheme is still usable with a correct detection rate of 80% for a false detection rate of 20%.

Having simulated the detection capabilities of the scheme, in the next section we consider some of the practical details of implementing this detection mechanism in a MANET.

4 Practical implementation details

The detection scheme described in Section 3 relies on a simple flooding procedure, the only requirements of which are that each flood message contains an identifier of the source and a record of the hop count. This flooding procedure is very general and is not tied to any particular implementation of a MANET. However, MANETs supporting the AODV protocol already implement a network flooding procedure every time nodes send out route request (RREQ) messages. Among other data, each RREQ message contains a record of the hop count and identifies the node transmitting the current message. Thus, by carefully observing the hop count of RREQ messages propagating throughout the network, it is possible to implement our detection scheme in a MANET using AODV without any changes to the standard routing protocol.

To implement this system in a practical network, each node within range of X_S must keep track of how many $hop\_count = 2$ and $hop\_count = 3$ messages it observes and must then relay this information back to X_S, which can then compute H_2 and H_3. Only those nodes within range of X_S need be concerned with keeping track of hop counts—thus, if a node does not observe the message $< S, hop\_count = 1 >$ (or does not see a hop count of 1 in an RREQ message) it need not count additional hop count messages. We have not discussed how the nodes within range of X_S will relay their information to back to X_S, but it is not hard to imagine any number of schemes to do this. All nodes that must communicate hop count information back to X_S are nearest neighbours of X_S, meaning that relaying this information will not unduly tax the MANET.

The proposed scheme detects wormholes in the vicinity of X_S only. This is advantageous since it allows the network to pinpoint which nodes are under attack—however, it does mean that in order to check for wormholes at every node in the network, every node must initiate a flood. It is clearly undesirable for every node in the network to simultaneously begin flooding the MANET as this could consume significant resources. In a MANET using AODV, one sensible implementation of the detection scheme is to simply perform detection for those nodes that are looking for new routes (i.e., nodes that initiate a RREQ procedure). In this fashion, when a node searches for a new route, it can implement the detection algorithm and can achieve some degree of certainly as to whether or not the discovered route contains a wormhole.

5 Future Work

The detection scheme proposed in this report provides an intuitively satisfying and provably effective method to detect wormholes for a specific set of assumptions. We propose further research that would extend the metrics considered by the detector and would examine its performance under a less stringent set of assumptions:

1. The detector in Section 3 examined the ratio of H_2 to H_3 in order to determine if a wormhole exists. It is possible that "higher order" ratios may yield additional insight into the presence or absence of a wormhole. For example, do the ratios H_3/H_4 or H_4/H_5 from indirect neighbours of the source impart any additional information that might help improve our detection accuracy? Importantly, these higher order ratios may help in cases where the network is less dense, as they allow us to examine more nodes and to not restrict ourselves to immediate one-hop neighbours.

2. This report explored a scheme that assumed nodes were distributed randomly according to a uniform density. It is also important to explore other node distribution scenarios that may be important in practical use cases. For instance, of possible interest is a clustered scenario where nodes assemble in distinct dense groups with each group connected by only a small subset of the nodes. Does the proposed detection scheme work equally well in these scenarios? Can the scheme be tailored in any way to improve performance?

3. The proposed scheme detects wormholes in the vicinity of a source node. Ideally, every node could use the scheme to detect whether or not it is under attack. Another approach might be to divide the MANET into "sectors" where each sector relies on a single node to execute the detection scheme and pass the result to its neighbours. What is the best way to partition the network into sectors? How effective is a sector-based technique compared to having each node perform its own wormhole detection?

6 Conclusion

This paper introduced a method to detect wormhole attacks in mobile ad hoc networks. Because the detection scheme relies on observing the propagation statistics of a network flood, it is possible to implement the scheme with minimal overhead on MANETs that employ AODV routing, making use of the AODV route discovery flooding mechanism. It is also possible to implement in any MANET (i.e., MANETs not using AODV) using the flood mechanism described, with the caveat that the flood packets would consume bandwidth. An explanation of the detection scheme was presented and a mathematical analysis was performed to prove its validity. Through simulation, it was determined that the scheme functions best in dense MANETs, correctly identifying wormholes with a high degree of certainty, while minimizing false positives. Although the precise operation of the detection technique is fully developed in this report, additional research avenues were proposed that may lead to further performance improvements in practical real-world scenarios.

References

[1] NWG, N. W. G. (2003), Ad hoc On-Demand Distance Vector (AODV) Routing, (Technical Report RFC 3561) IETF.

[2] NWG, N. W. G. (2003), Optimized Link State Routing Protocol, (Technical Report RFC 3626) IETF.

[3] Khabbazian, M., Mercier, H., and Bhargava, V. (2009), Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks, *IEEE Transactions on Wireless Communications*, 8(2), 736–745.

[4] Hu, Y., Perrig, A., and Johnson, D. (2006), Wormhole attacks in wireless networks, *IEEE Journal on Selected Areas in Communications*, 24(2), 370–380.

[5] Wang, X. and Wong, J. (2007), An end-to-end detection of wormhole attack in wireless ad-hoc networks, In *Proc. of 31st Annual International Computer Software and Applications Conference*.

[6] Song, N., Qian, L., and Li, X. (2005), Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach, In *Proc. of the 19th IEEE International Parallel and Distributed Processing Symposium*.

[7] Jen, S., Laih, C., and Kuo, W. (2009), A hop-count analysis scheme for avoiding wormhole attacks, *Sensors*, Vol. 9.

[8] Choi, S., Kim, D., Lee, D., and Jung, J. (2008), WAP: wormhole attack prevention algorithm in mobile ad hoc networks, In *Proc. of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*.

[9] Chiu, H. and Lui, K. (2006), DelPHI: wormhole detection mechanism for ad hoc wireless networks, In *Proc. of the 1st International Symposium on Wireless Pervasive Computing*.

[10] Maheshwari, R., Gao, J., and Das, S. (2007), Detecting wormhole attacks in wireless networks using connectivity information, In *Proc. of 26th IEEE International Conference on Computer Communications*.

[11] Gorlatova, M., Mason, P., Wang, M., Lamont, L., and Liscano, R. (2006), Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis, In *Proc. of IEEE MILCOM 2006*.

[12] Lynch, D., Knight, S., Gorlatova, M., Lamont, L., Liscano, R., and Mason, P. (2008), Providing effective security in mobile ad hoc networks without affecting bandwidth or interoperability, In *Proc. of 26th Army Science Conference*.

[13] Song, R. and Mason, P. (2011), Enhancement of frequency-based wormhole attack detection, In *Proc. of MILCOM 2011*.

[14] Gradshteyn, I., Ryzhik, I., and Jeffrey, A. (2000), Table of integrals, series and products, 6th ed, San Diego: Academic Press.

Acronyms and abbreviations

AODV	ad hoc on-demand distance vector
C4I	Command, Control, Communications, Computers and Intelligence
DelPHI	delay per hop indiciation
DRDKIM	Director Research & Development Knowledge and Information Management
EDWA	end-to-end detection of wormhole attack
GPS	global positioning system
IETF	Internet Engineering Task Force
MANET	mobile ad hoc network
MHA	multipath hop-count analysis
OLSR	optimized link state routing
pdf	probability density function
RFC	request for comment
RREQ	route request
RREP	route reply
SAM	statistical analysis of multi-path
SMN	secure mobile networks

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue, Ottawa ON K1A 0Z4, Canada

2a. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Detecting wormholes in mobile ad hoc networks through hop count analysis

4. AUTHORS (Last name, followed by initials – ranks, titles, etc. not to be used.)

Brown, J. D.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2012	38	14

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue, Ottawa ON K1A 0Z4, Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
15by01	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC Ottawa TM 2012-118	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

(X) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11)) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report proposes a new method to reliably detect wormhole attacks in mobile ad hoc networks (MANETs) by carefully observing the propagation of standard routing control packets through the network. The method is compatible with standard routing techniques and does not require additional hardware or sophisticated processing. The detection scheme is introduced and motivated using an intuitive argument, following which a mathematical analysis is performed that supports the heuristics. A simulation of the scheme demonstrates its effectiveness in dense MANETs and confirms the theory. Suggestions for future development are proposed to further enhance detection accuracy.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

MANET // wormhole detection // AODV // route request messages // hop count

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

DEFENCE DÉFENSE

www.drdc-rddc.gc.ca