Matam and Tripathy *EURASIP Journal on Wireless Communications and Networking* 2013, **2013**:180
http://jwcn.eurasipjournals.com/content/2013/1/180

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

WRSR: wormhole-resistant secure routing for wireless mesh networks

Rakesh Matam* and Somanath Tripathy

Abstract

Wormhole attack is one of the most severe security threats in wireless mesh network that can disrupt majority of routing communications, when strategically placed. At the same time, most of the existing wormhole defence mechanisms are not secure against wormhole attacks that are launched in participation mode. In this paper, we propose WRSR, a wormhole-resistant secure routing algorithm that detects the presence of wormhole during route discovery process and quarantines it. Unlike other existing schemes that initiate wormhole detection process after observing packet loss, WRSR identifies route requests traversing a wormhole and prevents such routes from being established. WRSR uses unit disk graph model to determine the necessary and sufficient condition for identifying a wormhole-free path. The most attractive features of the WRSR include its ability to defend against all forms of wormhole (hidden and Byzantine) attacks without relying on any extra hardware like global positioning system, synchronized clocks or timing information, and computational intensive traditional cryptographic mechanisms.

Keywords: Wormhole attack; Secure routing; Unit disk graph; Wireless mesh network

1 Introduction

Wireless mesh networks (WMNs) have emerged as a promising technology to provide low-cost, high-bandwidth, wireless access services in a variety of application scenarios [1]. A typical WMN as shown in Figure 1 is comprised of a set of stationary mesh routers (MRs) that form the mesh backbone and a set of mesh clients that communicate via mesh routers. Security is a critical component that contributes to the performance of WMN. The major challenges that need to be dealt with in addressing security issues mainly arise due to open nature of the wireless medium and multi-hop cooperative communication environment. These factors make network services more vulnerable, specifically due to attacks coming from within the network.

Routing protocols in WMN are susceptible to various security attacks. A detailed survey of such attacks can be found in [2]. In this paper, we focus on a particularly devastating form of attack called wormhole attack [3], on hybrid wireless mesh protocol (HWMP), the default path-selection protocol for IEEE 802.11-based WMN [4].

*Correspondence: m.rakesh@iitp.ac.in
Dept. of Computer Science and Engineering, Indian Institute of Technology Patna, Patna, Bihar 800013, India

Wormhole attacks can be broadly categorized into two types depending on the type of adversary involved. Wormhole attack launched by colluding external adversaries is called as hidden wormhole attack. Similarly, a wormhole attack launched by malicious colluding internal nodes is called as an exposed/Byzantine wormhole attack. Wormhole attacks (both hidden and exposed) in general are challenging to defend against [3]. However, Byzantine wormhole attack is relatively much difficult to detect than a hidden wormhole, as the nodes involved in the former form legitimate part of the network, and can bypass existing security mechanisms [5]. To launch a wormhole attack, the colluded malicious nodes establish a direct communication channel between themselves and thereby bypass several intermediate nodes. The established channel can be an out-of-band high-speed communication link or an in-band logical tunnel. The wormhole link is usually established between nodes that are located far away from each other. Once established, the wormhole link attracts most of the traffic as the control packets traversing through a wormhole link advertise much better link metric. Selection of such links results in denial of service (DoS), affecting the performance of the network severely.

It has been shown that a strategic placement of the wormhole can disrupt on average 32% of all

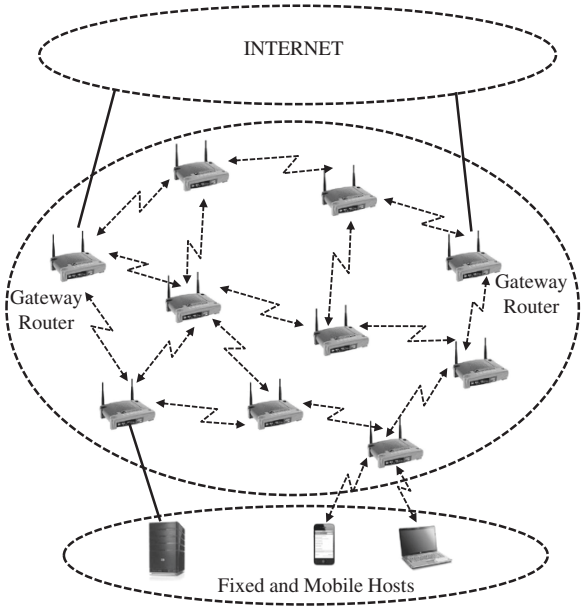

Figure 1 A typical wireless mesh network.

communication across the network [6]. In this work, we consider both hidden and exposed wormhole attacks. Hereinafter whenever we refer to wormhole attack, it means both hidden and exposed wormhole attack, unless specified explicitly.

There are several potential ways of defending against a wormhole attack, each of which exploits a different unique feature exhibited by a wormhole node/link. For example, schemes like [3,7-13] exploit the abnormal length of a wormhole. As previously stated, a wormhole link is usually established between nodes that are physically separated by large distance, thereby bypass several intermediate nodes. Therefore, the simplest way to defend a wormhole attack is by preventing nodes from being tricked into forming a wormhole link by equipping nodes with location systems (GPS) and verifying the relative position of a transmitter during peer-link establishment. Location-based schemes can successfully defend hidden wormhole attacks but cannot prevent Byzantine wormholes from being established as the colluded nodes involved in the attack are legitimate part of the network. Clock-based mechanisms can restrict the distance travelled by packets but are constrained by clock synchronization issues. Even though alternate mechanisms exist that overcome the synchronization issue, they cannot prevent malicious nodes from forming a Byzantine wormhole for the aforementioned reason.

The other unique characteristic of a wormhole link is that it abnormally increases the node's neighbourhood, and this feature is being exploited in [8,14-16] to detect hidden wormhole. Let W_1 be a wormhole node that shares an out-of-band channel with another wormhole node W_2. Now, W_1 can relay its neighbourhood information to W_2 and trick W_2's neighbours into believing that they share direct neighbourhood with W_1's neighbours. This abnormally increases the neighbour count of a node-sharing neighbourhood with a wormhole node. Unfortunately, such schemes fail to detect Byzantine wormholes as Byzantine wormhole link (established between colluded internal nodes) does not alter the neighbourhood information of their respective neighbours. On similar lines, protocols exist that exploit abnormal path attractions of wormhole nodes [17].

In this paper, we present a novel routing protocol (*WRSR*) that addresses both hidden and exposed wormhole attacks in WMN. It depends on neighbourhood connectivity information and relies on existence of shorter alternate sub-paths. To the best of our knowledge, this is the first of such kind that prevents Byzantine wormhole attacks using neighbourhood connectivity information. A part of this work is published in [18].

The rest of the paper is organized as follows. The related work is presented in Section 2. Network assumptions and adversarial model are presented in Section 3. Section 4 presents the proposed wormhole resistant secure routing (WRSR) protocol. The proof of concept supporting WRSR is presented in Section 5. The performance of WRSR is analysed in Section 6. Section 7 presents a brief discussion on WRSR and other existing approaches addressing wormhole attacks. Finally, Section 8 concludes the paper.

2 Related work

Most of the existing approaches that address wormhole attacks rely on specialized hardware like GPS, synchronized clocks or directional antennas. These protocols have been specifically designed to address hidden wormhole attacks. The very first countermeasure developed by Hu et al. in [3] requires GPS and tightly synchronized clocks. To overcome the clock synchronization issues, alternate schemes [9-12] have been proposed based on the message round trip time (RTT). Wormhole attack prevention algorithm (WAP) presented in [7] is based on timing information that requires each node to maintain a Wormhole Prevention Timer and overhear its neighbour's retransmission. WAP assumes that wormhole nodes only use wormhole link (in-band-tunnel/ out-of-band channel) and do not re-broadcast control messages in their local neighbourhood. Recently, Zhou et al. proposed a wormhole detection mechanism called neighbour-probe-acknowledge (NPA) that is based on standard deviation of RTT (stdev(RTT)) [19]. NPA is triggered when node detects change in network topology. To obtain RTTs, each node sends probe messages locally for T times to all its neighbours and gets T acknowledge messages from each neighbour. A wormhole is detected by identifying large deviations in stdev(RTT).

The end-to-end wormhole detection algorithm presented in [8] is based on euclidean distance estimation technique that requires GPS. The source estimates the minimum hop count of the shortest path between source to destination and compares it with shortest route received. If it is much smaller than the estimated value, the source node raises an alert of wormhole attack and initiates a wormhole *TRACING* procedure to identify the end points of a wormhole.

The protocol presented in [16] uses local neighbourhood information to detect wormholes. It is based on the observation that formation of a wormhole link changes the network topology. It assumes that, in a sufficiently dense network, for every given pair of neighbours, there exists at least one common neighbour. Nodes sharing neighbourhood with wormhole node (w_1) can detect a wormhole if it cannot reach the subsequent wormhole node (w_2) through any other node except (w_1). Thaier et al. proposed DeWorm [20] that uses routing discrepancies between neighbours along a path from the source to destination to detect a wormhole. It is based on the observation that, to have a successful impact on the network, the wormhole must attract significant amount of traffic and the length of the wormhole must be significantly large.

Few protocols exist that specifically address Byzantine wormhole attacks. On-demand secure Byzantine resilient routing protocol (ODSBR) [5] is one such protocol based on DSR [21] that addresses Byzantine attacks. ODSBR relies on explicit network layer acknowledgement on the received data and on a binary search-based probing mechanism to detect malicious dropping of packets. The detection mechanism is instantiated by a source node after observing $log\ n$ number of faults, where n is the length of the path. The source node probes intermediate nodes in a binary search fashion to determine the faulty link.

SPROUT [22] is another source-routed, link-state, multipath probabilistic routing protocol that operates in two stages: route generation and route selection. In the route generation stage, a large number of routes are probabilistically generated without taking any routing metric to account. The reliability and round-trip time of each active route are then analysed to choose an optimal route. In this scheme, the route performance feedback is used to select an optimal route which leads to high route establishment latency.

WARP [17] is a wormhole-avoidance routing protocol based on *ad hoc* on-demand routing protocol (AODV) [23], which avoids wormhole attacks by anomaly detection. It is based on the fact that wormhole nodes have abnormal path attractions. WARP considers link-disjoint multiple paths during path discovery but eventually selects only one path to transmit data. Each node in WARP maintains the anomaly values of its neighbours in its routing table. It computes the percentage of routing decisions in which a particular neighbour is involved. That is, it determines the anomaly value by computing the ratio of number of actual routes established through that neighbour to the number of route replies transmitted by that neighbour. If its above a certain threshold, routes replies transmitted by such a node are ignored and thus wormhole nodes are isolated.

A key point to note is that in most of the above existing work, the discussed approaches are restricted to hidden wormhole attacks. Works specifically addressing Byzantine wormhole attacks like ODSBR [5], SPROUT [22] and WARP [17] depend upon the existence of multiple disjoint paths between source S and destination D. In this paper, we propose a wormhole-resistant secure routing protocol (WRSR) that detects and prevents the selection of wormhole paths based on neighbourhood connectivity information and alternate shorter paths.

3 Network assumptions and adversary model

3.1 Network assumptions

We consider a typical WMN architecture as shown in Figure 1, where a set of MRs forms the backbone of WMN. Few of the MRs are equipped with access point functionality to provide access services to its clients. In addition to that, a few of the MRs are designated as gateways and are connected to the Internet. MRs are more or less static and communicate in a multi-hop fashion to provide access services to its clients. MCs are typical wireless clients connected to specific MRs with access point functionality.

3.2 Adversary model

We assume that an adversary is capable of launching various kinds of wormhole attacks. To begin with, an adversary is assumed to be capable of establishing a high-speed low-latency communication link, required to launch a hidden wormhole attack. Further, an adversary can compromise a few MRs in the mesh backbone to launch a wormhole attack in participation mode. These compromised MRs exhibit Byzantine behaviour and can manipulate routing metric to influence route selection decisions. We mainly focus on wormhole attacks launched by MRs, since route discovery is carried out by MRs on behalf of mesh clients.

An attacker launches a hidden wormhole attack by recording packets at one location, relays them to another location through a wormhole link and retransmits them there into the network [3]. In a WMN, where nodes establish secure peer links and process packets only from peer stations, an adversary needs to target the Authenticated Mesh Peer-link Exchange (AMPE) protocol to successfully launch a wormhole attack [24]. In such a case, the attacker tries to convince two far-away nodes as peers by relaying AMPE protocol messages. On successfully establishing

falsified non-existent peer links, an adversary can launch various kinds of active DoS attacks and passive attacks like traffic analysis. Various kinds of defence mechanisms have been proposed, out of which, some of them depend upon extra hardware such as GPS, synchronized clocks or directional antennas, while a few others exploit the features exhibited by wormhole (like neighbourhood information, large discrepancies in path metric, etc.).

A Byzantine wormhole attack is launched by colluding malicious nodes that are legitimate part of the network and can participate in normal network operations. Therefore, securing AMPE protocol cannot prevent colluding nodes from launching a Byzantine wormhole attack. Moreover, the colluded nodes do not alter neighbourhood information of their respective neighbours, therefore detection schemes based on neighbourhood information fail to detect such a wormhole. The major challenge lies in dealing with nodes that are part of the network that can bypass the existing security mechanisms.

4 WRSR: the proposed secure routing

WRSR, the proposed wormhole-resistant secure routing protocol prevents the selection of route requests traversing the wormhole link. WRSR is based on HWMP and therefore inherits majority of its characteristics. The operation of HWMP can be found in the 'Appendix' section.

The operating principle of WRSR is to allow nodes to monitor the two-hop sub-path on a received route request (RREQ) and identify a RREQ that traverses a wormhole. A route request that traverses via a wormhole link would not satisfy the necessary wormhole-free path criterion, which can be detected at the neighbours of a wormhole node and can easily be quarantined.

A path is said to be free from wormhole links if and only if for each sub-path of length $2R$ there exists an alternate sub-path of maximum length $4R$, where R is the transmission range of a node. WRSR thrives on the fact that the probability of finding alternate routes between nodes separated by a distance $d(R < d \leq 2R)$ is high. This proof of concept is presented in Section 5.

Since, nodes in WRSR need to monitor two-hop sub-paths on a received RREQ, they need to maintain neighbourhood relations with all the nodes in their two-hop range. To facilitate this, the IEEE 802.11s beacon frame can be extended, as shown in Figure 2, to obtain necessary neighbourhood information. The extended beacon frame includes two additional fields, a flag bit and a variable length neighbour address field. The neighbour address field accommodates addresses of varying number of neighbours, and the flag bit is used to indicate presence/absence of neighbourhood information. WRSR employs an extended RREQ element and a modified routing entry as shown in Figure 3 to accommodate additional addresses for discovering wormhole-free routes. The notations used in this paper are depicted in Table 1. WRSR operates in following three processes discussed subsequently.

4.1 Route discovery process

Route discovery process employed by WRSR is almost similar to that of HWMP. The source node S initiates route discovery process for establishing a path to the destination D by broadcasting an RREQ. The RREQ processing rules of WRSR are similar to that of HWMP apart from an additional verification required to validate an RREQ. Any intermediate node that receives a broadcasted RREQ verifies the validity of two-hop address present in the RREQ (i.e. node I checks whether the two-hop address received in RREQ is present in its neighbourhood information) along with the usual validation process of HWMP. On validating the RREQ, node I creates a routing entry for the corresponding RREQ-ID, sets its state as transient and rebroadcasts it. Otherwise, it drops the RREQ.

4.2 Route selection process

The primary goal of WRSR route selection process is to select wormhole-free paths. Nodes monitor the received RREQ's for a necessary and sufficient condition to classify a path to be free from wormholes. Once an RREQ is verified to be wormhole free, the corresponding routing entry is elevated to stable state from transient state. The route selection process is shown in Algorithm 1.

Consequent upon receiving a new RREQ ($RREQ_N$), the intermediate node I processes it to take an appropriate action. Initially, the intermediate node I verifies if a transient routing entry corresponding to the RREQ-ID and sequence number received in $RREQ_N$ exists. Multiple transient routing entries may exist for the same RREQ-ID that are received through a unique two-hop node. Node I then compares the two-hop address present in $RREQ_N$ with the two-hop addresses of a set of existing routing entries represented by $\{RREQ_O\}$. If it matches with any of the existing routing entries $RREQ_O$, it is updated with $RREQ_N$ provided that it offers better metric. In case of

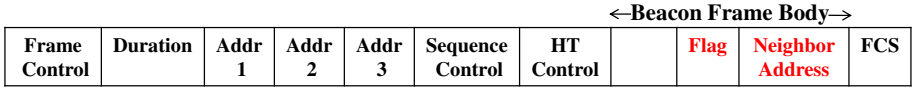

Figure 2 Extended beacon frame format.

Algorithm 1 WRSR: route selection process. On receiving $RREQ_N$ by an intermediate node I

if no routing entry exists for **S** ***then***
if(2Hop is valid) ***then***
create corresponding *RENTRY*
state ← transient
broadcast $RREQ_N$
else
drop $RREQ_N$
end if
else
if($RREQ_{ID}$, SEQ_No, $2Hop$ are valid) **then**
for(all routing table entries)
if($RREQ_{N\_2Hop}$==$RENTRY_{2Hop}$) **then**
if($RREQ_{N\_Metric} < RENTRY_{Metric}$) **then**
update($RENTRY \leftarrow RREQ_N$)
else
drop $RREQ_N$
end if
else
if($RREQ_{N\_2Hop}$ ==($RENTRY_{3Hop}$ | $RENTRY_{4Hop}$)) **then**
update($RENTRY \leftarrow RREQ_N$)
state ← stable
else
update($RENTRY \leftarrow$ better($RREQ_N$, $RENTRY$))
state ← stable
end if
else
create routing entry for $RREQ_N$
state ← transient
broadcast $RREQ_N$
end if
else
drop $RREQ_N$
end if
end if

no matching address, node I further compares the three and four-hop addresses present in $RREQ_N$ with the two-hop addresses of routing entries represented by $RREQ_O$ or vice versa. If any one of the two addresses match(two-hop address in $RREQ_N$ with three-/four-hop addresses of $RREQ_O$ or vice versa), provided the 2HA of $RREQ_N$ does not match with transmitter address of $RREQ_O$ or vice versa, an optimal of the two RREQ's ($RREQ_O$ or $RREQ_N$) is selected and state of the routing entry is set to stable. If none of the comparisons match, a new transient routing entry is created for the corresponding RREQ-ID.

This matching of addresses is carried out to select an optimal wormhole-free path. The necessary and sufficient condition for detecting a wormhole-free path is presented in Section 5. Finally, if an intermediate node I receives an $RREQ_N$ when it already has a stable routing entry to a destination D, I processes the $RREQ_N$ only if the new route request offers a better metric than the existing route. WRSR creates a separate routing entry for $RREQ_N$ and updates the existing stable entry with $RREQ_N$, only after it has been verified to be free from wormholes. This process assures the selection of a wormhole free path.

4.3 Route reply process

Like any intermediate node I, the destination node D processes multiple RREQs before selecting an optimal wormhole-free path, satisfying the route selection criteria. It unicasts an RREP through which a stable the RREQ has

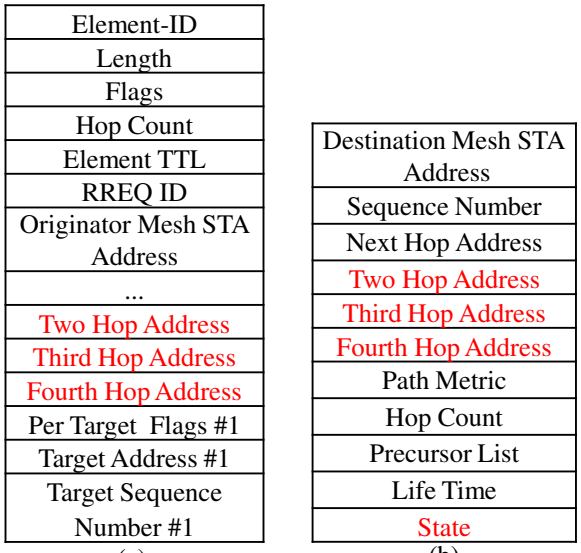

Figure 3 Route request (a) and routing entry (b) in WRSR.

been received. Subsequently, intermediate nodes propagate the RREP through wormhole-free routes.

4.4 Route maintenance

Route maintenance in WRSR is similar to that of HWMP. Whenever a node I discovers a link failure, it initiates the route maintenance process by transmitting a RERR message addressed to the source. Node I can optionally initiate route discovery process on behalf of the source to reduce the route selection latency. Intermediary nodes on receiving a RERR message mark the corresponding routing entry and propagate the RERR message towards the source S. The source S on receiving the RERR message can re-initiate the route discovery process by broadcasting an RREQ.

Table 1 Notations and their meaning in WRSR

Notation	Meaning
RREQ	Route request
$RREQ_{ID}$	Route request identity
SEQ_No	Route request sequence number
$RREQ_N$	Newly received route request
$RREQ_O$	Existing routing table entry
2Hop	Two-hop address in route request
$RREQ_{N\_iHop}$	*i*th hop address in $RREQ_N$
RENTRY	Entry in routing table
$RENTRY_{iHop}$	*i*th hop address of routing entry
$RREQ_{N\_Metric}$	Routing metric in $RREQ_N$
$RENTRY_{Metric}$	Routing metric of a particular routing entry

5 Proof of concept

In this section, we show that the route selection process employed by WRSR avoids the wormhole path by verifying the necessary and sufficient condition for wormhole-free path. For simplicity reason, let us assume that each node is equipped with an omnidirectional antenna with unit transmission range. This can be easily fitted into the unit disk graph (UDG) model.

5.1 Unit disk graph

UDGs have been extensively employed to create an idealized communication model for a multi-hop wireless network [14,20,25]. In UDGs, each node can be modelled as a disk of unit radius in a plane. Each node is a neighbour of all nodes located within its disk. We assume that the network consists of a large number of nodes distributed uniformly with density ρ (number of nodes in a circle) inside a disk of radius R (considered to be unity in our model). Two nodes can directly communicate with each other if the distance between them is less than or equal to R.

5.2 Problem formulation

Hop count is an important field in the routing process. Therefore, many popular routing protocols including HWMP, DSDV-ETX [26], MR-LQSR [27], etc., use hop-count as an important field in the RREQ element, even though the metric employed to select an optimal route is different. Essentially, a wormhole bypasses the multiple intermediary hops to cover a distance of W_d between two wormhole nodes W_1 and W_2 that are usually separated by a large distance $d_{W_{1,2}}$ ($d_{W_{1,2}} > 2R$) in a single hop. A typical wormhole path in a network is shown in Figure 4. The length of a wormhole sub-path which connects two distant nodes u and v that are neighbours of wormhole nodes w_1 and w_2, respectively, is three hops apart from each other; that is, a node v can be effectively reached from w_1 in two hops through wormhole link. It has been observed that, in an uniformly distributed network, alternate paths exist between nodes separated by a distance d ($> R$). Therefore, in a genuine case (absence of a wormhole), it is possible to reach v that is two-hop away from w_1 in at most four hops with a high probability. This characteristic can be exploited by node v to differentiate a wormhole link from a genuine link. The following lemma tries to prove the existence of an alternate shortest path between nodes separated by a maximum distance of $2R$.

Lemma 1. *Lemma 1 A path is said to be free from wormhole links if the following condition is satisfied: 'for each sub-path of length 2R, there exists an alternate sub-path of*

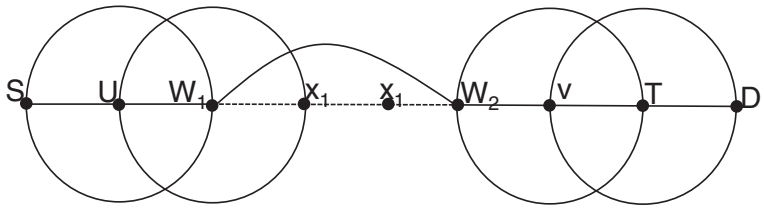

Figure 4 A typical path passing through a wormhole.

maximum length 4R with a probability of $(1-e^{-\rho(\pi(\frac{R}{4})^2)})^t$ *where "t" is the number of disks on a selected path.'*

Proof. Consider a network where large number of nodes are uniformly and independently distributed with density ρ, inside a disk of radius R. In such a network, the number of nodes in a region $\Re$ with area $\Delta_{\Re}$ follows Poisson distribution that can be realised as follows.

$$Pr(\Re \text{ contains } n \text{ nodes}) = e^{-\rho\Delta_{\Re}}\frac{(\rho\Delta_{\Re})^n}{n!}. \quad (1)$$

□

Let $N_{u,v}$ be the number of hops on the shortest path between u and v. Then, clearly we have

$$N_{u,v} \geq \frac{d_{u,v}}{R}. \quad (2)$$

In a network where density of nodes ρ is high, with high probability we should obtain

$$N_{u,v} \leq 2\frac{d_{u,v}}{R}. \quad (3)$$

If $d_{u,v} \geq \frac{R}{2}$, then there are $t = \lfloor 2\frac{d_{u,v}}{R} \rfloor - 1$ disks with radius $\frac{R}{4}$ and origins at distances $d_i = \frac{R}{2}i + \frac{R}{4}$, $1 \leq i \leq t$, from u on a line going through u to v, as shown in Figure 5. Clearly, the distance between two nodes in adjacent disks is at most R. Using Equation (1) we obtain,

$$\begin{aligned} &Pr(\text{at least one node in each disk}) \\ &= (1 - P(\text{no node in a disk}))^t \\ &= (1 - e^{-\rho\pi((\frac{R}{4})^2)})^t. \end{aligned} \quad (4)$$

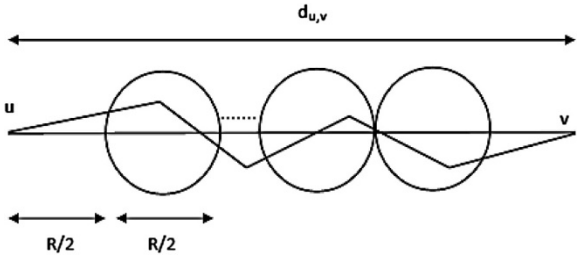

Figure 5 Finding a path between *u* and *v*.

Therefore, there is a path of length $t+1 = \lfloor 2\frac{d_{u,v}}{R} \rfloor$ with probability at least $(1 - e^{-\rho\pi((\frac{R}{4})^2)})^t$. Thus, obtaining such a path is possible with high probability if $(e^{-\rho\pi((\frac{R}{4})^2)})^t \ll 1$ that implies

$$\rho \gg \frac{\ln(\lfloor 2\frac{d_{u,v}}{R} \rfloor - 1)}{\pi(\frac{R}{4}^2)}. \quad (5)$$

In Figure 4, $d_{w_1,v} \leq 2R$, i.e. the minimum number of hops required to cover a distance of $2R$ between w_1 and v is 2 (if traversed through a wormhole). Therefore, the nodes w_1 and v, separated by a distance $2R$, can reach each other with the help of a common neighbour w_2 traversing through a shortest path $w_1 \rightarrow w_2 \rightarrow v$. Based on the above observations, if one can obtain a necessary condition that there exists a sub-path of maximum length $4R$ with probability $(1-e^{-\rho\pi((\frac{R}{4})^2)})^t$, which is computed to be high, is sufficient to identify a wormhole-free path.

6 Simulation results

In this section, we present the simulation results to showcase the effectiveness of proposed wormhole-resistant secure routing protocol. The experiments were carried out on OMNeT++4.2.1, a discrete event network simulator [28]. The performance of WRSR is compared with WARP [17] and ODSBR [5]. To carry out the following experiments, we set up a network of 400 MRs over an area of 2,000 m^2, forming the mesh backbone. The transmission range of each MR is set to 100 m. The IEEE 802.11 MAC protocol is employed with a channel data rate of 54 Mbps.

To begin with, we analyse the effect of wormhole attack on the performance of WRSR, WARP and ODSBR on a network, where nodes are independently and uniformly distributed based on Poisson distribution. To maximize the impact of wormhole attack, the wormhole link is centrally placed, as a centrally placed wormhole link can attract higher number of route selection decisions [6]. The wormhole link is simulated as a high-speed low-latency communication link between two malicious nodes. The comparison results are based on percentage of packets (PDR) delivered in presence of multiple wormholes. Source and destination nodes are chosen randomly, and

the total simulation time was set to 3,000 s. The experiment was designed in such a way that each source transmits 0.5 MB of video traffic to a corresponding destination in presence of wormhole links. Initially, the length of wormhole was set to *4R*, where *R* is the transmission range of a node. The packet length was set to 1,024 bytes. The same experiment was repeated by increasing the number of wormhole links. For any given combination of simulation parameters, we ran 150 different simulations and finally averaged over all 150 different topologies.

Figure 6 shows the performance comparison of different protocols. We mainly focus on the result of WARP and ODSBR, as HWMP is devoid of any defence mechanism. The lower percentage of packets delivered by WARP and ODSBR is due to the latency in detecting the wormhole link. Since, WARP is an anomaly based wormhole detection scheme, it initially suffers from packet loss due to the possible selection of wormhole nodes in the initial route discovery process. Its performance is enhanced once a wormhole node is detected and isolated. Similarly, ODSBR enters into a probing state only when there is a violation in packet loss threshold. Therefore, both WARP and ODSBR suffer from initial packet losses as conformed in Figure 6. The results depict cumulative packet loss registered in the network at the end of simulation time. The lower packet loss percentage of WRSR is attributed to the zero latency in detecting a wormhole link and therefore registers consistent performance over rest of the protocols.

Our second experiment, carried out on the same network topology, analyses the performance of different protocols by varying the length of the wormhole link. Similar to the first experiment, the wormhole link is centrally placed to increase its effectiveness. The results shown in Figure 7 clearly indicate that the length of the wormhole

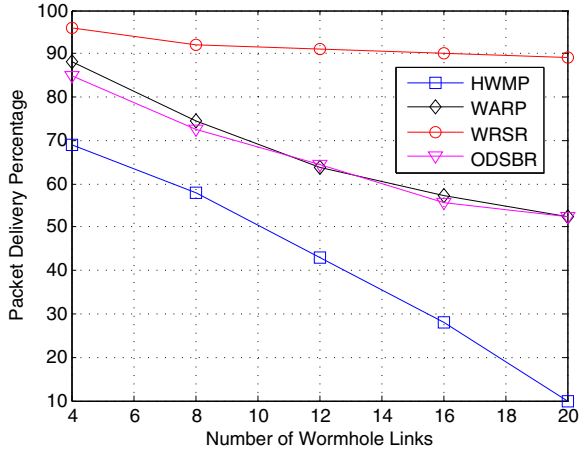

Figure 6 Performance comparison of WRSR with WARP, ODSBR and HWMP.

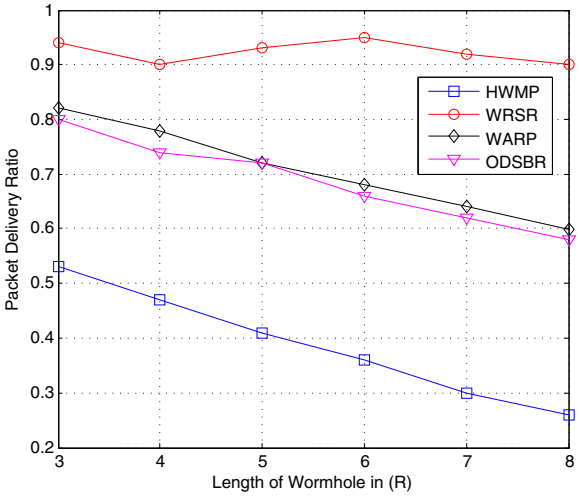

Figure 7 Performance comparison of WRSR with WARP, ODSBR and HWMP.

has no impact on the performance of WRSR, whereas performance of WARP and ODSBR falls consistently with increase in wormhole length. This characteristic is attributed to the fact that large wormholes can influence more route selection decisions.

In both the cases (varying percentage of wormhole links and varying length of wormhole link), WRSR clearly performs better in comparison to WARP and ODSBR. WRSR avoids route requests traversing a wormhole link at all times whereas WARP and ODSBR selects route requests traversing a wormhole node, until the route-building rate is higher than the allowed threshold or the packet loss threshold falls below the allowed limit, respectively. Therefore, choosing a threshold value plays a vital role in detection of wormhole node in both the protocols. The threshold values of ODSBR and WARP are obtained from the experiments conducted in [5] and [17], respectively. The loss threshold of ODSBR is considered to be $log\ n$ faults, where n is the hop-count of the selected path, whereas a threshold value of 0.51 is considered for WARP.

The above experiments were carried out for network topologies formed using Poisson distribution. On the other hand, to analyse the performance of WRSR on randomly distributed network topologies, we carry out similar kind of experiments as above with an only difference that the nodes are randomly distributed. The other network parameters are unaltered. Figures 7 and 8 show the performance comparison of different protocols in a network under wormhole attack. It can be observed that the random distribution of nodes does not have any impact on the percentage of packets delivered by WRSR. The rationale behind this is the fact that WRSR selects routes only if the RREQs meet the necessary wormhole-free path criterion. Failing to meet the same results in dropping of an

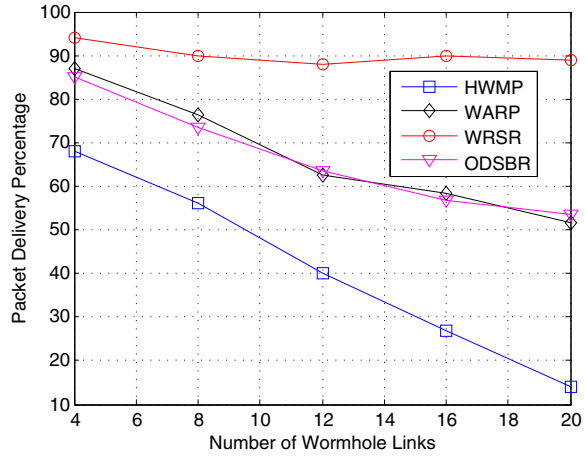

Figure 8 Performance comparison of WRSR with WARP, ODSBR and HWMP.

RREQ that may be genuine. However, existence of alternate paths due to higher node density allows WRSR to select alternate routes thereby not effecting the packet delivery ratio. At the same time, it can be observed that there is no variation in performance of WARP and ODSBR when compared to their performance in uniformly distributed network, as the protocols are not dependent on underlying network topology.

Finally, Figure 9 shows the impact of wormhole length on the packet delivery ratio of different protocols. The results clearly show that the length of wormhole link has no impact on PDR of WRSR. However, PDR of WARP and ODSBR falls with increase in length of wormhole link.

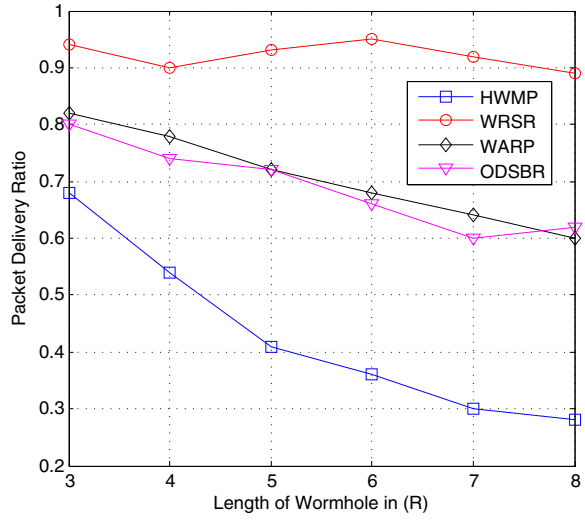

Figure 9 Performance comparison of WRSR with WARP, ODSBR and HWMP.

6.1 Detection rate of WRSR

The success achieved by a wormhole detection algorithm is measured in terms of percentage of wormholes detected. Every successful detection of a wormhole link contributes to the success rate of WRSR. To compute the detection rate, we set up a network of 400 MRs that are uniformly distributed over an area of 2,000 m^2 using Poisson distribution function. Wormhole nodes are randomly selected, and the density of nodes ρ (number of nodes in a disk) is varied between 4 to 7. A successful wormhole detection event comprises of an RREQ traversing a wormhole that fails to meet the required wormhole-free path criterion, which is then appropriately identified and quarantined. To achieve this, each node in WMN monitors the two-hop sub-path traversed by an RREQ, for existence of an alternate sub-path connecting the two-hop node. Table 2 summarizes the detection rate of WRSR. WRSR reports higher detection rate with increasing value of ρ. This is due to the fact that, for higher values of ρ, the probability of finding an alternate path is high.

6.2 False positives in WRSR

The amount of false positives reported by WRSR is computed in a similar fashion as the computation of the detection rate. A false positive in WRSR is a situation where an RREQ traversing a genuine link is dropped for failing to meet the necessary wormhole-free path criterion. This situation arises when no alternate path exists within a maximum of four hops connecting a two-hop node traversed by the RREQ.

However, the existence of an alternate path only depends on the density (ρ) of nodes in the network. Therefore, the impact of false positives reported by WRSR is studied by varying the density of nodes in the network. The simulation set up is such that for varying configurations of the network, the performance of WRSR is evaluated for various node densities(number of nodes in a disk). We specifically monitor for scenarios where a genuine link is falsely considered as a wormhole and such an RREQ is dropped. Table 3 summarizes the percentage of false positives reported by WRSR. The amount of false positives reported is relatively high for a lower density values. But, as shown in the Table 3, negligible false positives occur for higher values of ρ. The values represented are rounded off to the nearest ceiling value.

6.3 Impact of wormhole length

The length of a wormhole link has negligible impact on the performance of WRSR. Wormholes greater than *2R*

Table 2 Wormhole detection rate of WRSR

Density (ρ)	4	5	6	7
Detection rate (%)	94.67	99.33	100	100

Table 3 False positives reported by WRSR

Density (ρ)	4	5	6	7
False positive (%)	6	3	0	0

have almost 100% detection rate. We evaluated the performance of WRSR by varying the length of wormhole link for a constant node density ρ(=4). Table 4 summarizes the impact of wormhole length on WRSR. Results clarify that WRSR reports almost 100% detection rate for wormhole links greater than *2R*.

6.4 Impact of node degree

Node degree plays an important role in the detection rate achieved by WRSR. It requires a minimum average node degree (number of neighbours) of *3*. However, the percentage of false positives is high for a node degree of *3*, as shown in Table 3. This is due to non-availability of alternate links between nodes of interest. WRSR reports 100% detection rate for an average node degree of *4* and above. A node degree of *4* is justified in a network like WMN, where nodes are strategically placed to provide access services to its clients.

7 Discussion

Routes traversing through a wormhole link are relatively much shorter and offer better metric when compared to genuine routes. The wormhole link essentially bypasses intermediary nodes to create non-existent routes in the network. WRSR successfully identifies a wormhole link during route discovery due to the existence of alternate paths between nodes separated by a distance d ($R < d \leq 2R$). In a uniformly distributed network with density ρ, we have analytically and experimentally shown that the probability of finding at least one alternate path is very high (98%). The static nature of mesh topology in mesh backbone contributes to the higher detection probability as links are more stable.

Existing protocols like SPROUT [22] and WARP [17] that address Byzantine wormhole attacks rely on existence of link-disjoint multiple paths between source and destination. SPROUT probabilistically generates multiple routes to destination and monitors the performance of each active route by means of signed end-to-end acknowledgements. It computes the reliability and round-trip time of an active route using the fraction of packets sent over it. SPROUT allows nodes to establish routes through wormhole links but based on their performance they are ignored. On the other hand, WARP considers link-disjoint multiple paths during path discovery and provides greater path selections to avoid malicious nodes but eventually uses only one path to transmit data. WARP allows nodes to monitor the number of routes created through each neighbour and isolates a particular neighbour whose anomaly value (route-building rate) is greater than the threshold. WARP suffers from rapid fluctuation of anomaly values which results in frequent isolation and recovery of nodes. Isolation of a node simply involves ignoring the route replies transmitted by a particular neighbour. Even though the route replies are not processed from such a neighbour whose anomaly value is greater than threshold, the route reply count maintained in the routing table for that neighbour is still incremented. This allows a node to recover from the isolation phase. But since the anomaly value changes rapidly for each received RREP, a malicious node can also recover very quickly from isolation phase. Therefore, determining the threshold value for a network is one of the major limitations of WARP.

Table 4 Impact of wormhole length on WRSR

Length of wormhole	3R	4R	5R	6R
Detection rate (%)	98.33	100	100	100

ODSBR [5] addresses all kinds of Byzantine attacks including Byzantine wormhole. However, ODSBR has several limitations. One of the major limitation of ODSBR is that it can only work with a source routing protocol, such as DSR, where the source knows all the intermediate nodes on a selected path. Second, the diagnosis packets have to be encrypted with a shared key between the source and the intermediate nodes. Third, the isolation is done per link rather than per node, i.e. blacklisting a malicious node results in isolating a honest node. Finally, the blacklisting of malicious nodes is done at the source of packet and not locally at the neighbours of the malicious node. Therefore, even if a malicious node is already blacklisted by some nodes in the network, it continues to be active and cause harm to traffic from other sources.

WRSR performs better as compared to other wormhole detection mechanisms. This is because of its ability to prevent a wormhole link from being selected during the path establishment. Thus, by avoiding malicious wormhole nodes, WRSR prevents malicious packet loss. The only scenario in which a path traversing through the wormhole link may be selected by WRSR is if it satisfies the necessary wormhole-free path criterion. This case can arise only when the wormhole nodes are neighbours to each other, i.e. wormhole link of length ($< 2R$), in which, an alternate path within a maximum of four hops may exist. However, as a wormhole link between two neighbouring nodes has very less impact on path selection decisions, it can be safely ignored.

Apart from that, WRSR overcomes the limitations of WARP and SPROUT, without relying on multiple link-disjoint paths. It does not require multiple routes to be considered before selecting an optimal route, thus reducing the route discovery latency. Lastly, the static nature of

Table 5 Security comparison of various existing protocols

Protocol	Employed mechanism	Extra hardware	Hidden mode	Participation mode
WRSR	Connectivity information	No	Yes	Yes
Packet leashes [3]	GPS & clock	Yes	Yes	No
Wang et al. [14]	Neighbourhood information	No	Yes	No
DeWorm [20]	Neighbourhood information	No	Yes	No
ODSBR [5]	Binary search	No	Yes	Yes
SPROUT [22]	Multipath routing	No	Yes	Yes
EDWA [7]	Neighbourhood information	No	Yes	No
Znaidi et al. [16]	Neighbourhood information	No	Yes	No
WARP [17]	Multiple link-disjoint paths	No	Yes	Yes

wireless mesh routers makes WRSR well suited to WMN. The comparison of security of the existing protocols is summarised in Table 5.

8 Conclusions

Addressing wormhole attacks is a crucial issue to ensure security in a wireless mesh network. In this paper, we proposed a novel wormhole-resistant secure routing (WRSR) protocol that relies on shorter alternate paths to detect a wormhole link. During route discovery, WRSR monitors for alternate paths for a cached RREQ and quarantines such RREQ that fails to meet the necessary and sufficient condition. The necessary and sufficient condition to differentiate a normal path from wormhole link is derived using unit disk graphs. The probability of finding such alternate paths has been analytically computed and shown to be high in a uniformly distributed network.

Appendix

Hybrid wireless mesh protocol

Hybrid wireless mesh protocol (HWMP) is the default path-selection (routing) protocol for IEEE 802.11-based WMN. As the name implies, HWMP is a combination (hybrid) of on-demand route selection mode and proactive tree-based approach. The on-demand path-selection mode of HWMP is based on AODV. The set of protocol elements (like route request, route reply and route error), their generation and processing rules of HWMP are similar to AODV. HWMP supports two modes of operation depending upon the network configuration. The on-demand route selection mode does not require root MR support and can be employed by any node that needs to establish a route. Whereas, the proactive tree building mode that compliments the existing on-demand mode can be employed only when a root MR is configured. The proactive tree routes can be established either using proactive route request (PREQ) or route announcement (RANN) messages. The proactive and on-demand modes are not exclusive and can be used concurrently, because the proactive modes are extensions to the on-demand mode.

Whenever a source node needs to find a route to a destination using the on-demand path-selection mode, it broadcasts a route request with the target address set to the address of destination and the metric initialized to initial value of the active route selection metric. The default route selection metric employed by HWMP is airtime. Airtime reflects the amount of channel resources consumed to transmit a frame over a particular link. The essence of airtime metric is to capture the status of a wireless link in terms of required time units to transmit a frame. On the other hand, there are two ways to proactively establish routes to the root node. The first method uses a proactive route request element and is intended to create paths between all mesh routers and the root node in the network. The second method uses a root announcement message and is intended to distribute path information for reaching the root node. The mesh router configured as root node sends either PREQ or RANN messages periodically.

The proactive tree building process begins when a root MR sends out a PREQ message with the target address set to all ones, implying all the MRs in WMN. Similarly, the root MR can also periodically propagate a RANN into the network. On receiving a RANN message, each MR that needs to create or refresh a path to the root MR, sends an individually addressed route request to the root MR via the MR from which it received the RANN. The root MR sends a route reply in response to each received route request. Thus, the proactive and reactive path-selection elements collectively allow HWMP to meet the path-selection requirements of WMN.

Competing interests

Both authors declare that they have no competing interests.

Acknowledgements

We would like to sincerely thank Dr. Sukhamay Kundu, Associate Professor, Dept. of Computer Science, Louisiana State University, for his valuable comments and suggestions. We would also like to thank the anonymous reviewers for their suggestions which helped us to improve this paper.

Received: 13 February 2013 Accepted: 20 June 2013
Published: 3 July 2013

References

1. IF Akyildiz, X Wang, W Wang, Wireless mesh networks: a survey. J. Comput. Netw. ISDN Syst. **47**(4), 445-487 (2005)
2. W Zhang, Z Wang, SK Das, M Hassan, in *Book, Wireless Mesh Networks: Architectures and Protocols*. Security Issues in Wireless Mesh Networks (Springer, New York, 2008)
3. Y Hu, A Perrig, D Johnson, in *Proceedings of the 22nd IEEE International Conference on Computer Communications*. Packet leashes: a defence against wormhole attacks in wireless networks (IEEE, San Francisco, 30 March–3 April 2003)
4. IEEE P802.11s Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking. (IEEE, New York, 2011)
5. B Awerbuch, R Curtmola, D Holmer, C Nita-Rotaru, H Rubens, ODSBR: an on-demand secure Byzantine resilient routing protocol for wireless *ad hoc* networks. ACM Trans. Inf. Syst. Security. **10**(4), (2008)
6. M Khabbazian, H Mercier, VK Bhargava, Severity analysis and countermeasure for the wormhole attack in wireless *ad hoc* networks. IEEE Trans. Wireless Commun. **8**(2), 736-745 (2009)
7. S Choi, DY Kim, DH Lee, JI Jung, in *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*. WAP: Wormhole attack prevention algorithm in mobile *ad hoc* networks (IEEE, Taichung, 11–13 June 2008), pp. 343–348
8. X Wang, J Wong, in *Proceedings of the Thirty-First Annual International Computer Software and Applications Conference*. An end-to-end detection of wormhole attack in wireless *ad hoc* networks (IEEE, Beijing, 24–27 July 2007), pp. 39–48
9. Z Tun, AH Maw, Wormhole attack detection in wireless sensor networks. J. World Acad. Sci. Eng. Technol. **46**(2), 545–550 (2008)
10. P Tran, LX Hung, YK Lee, S Lee, H Lee, in *Proceedings of Fourth IEEE Consumer Communication and Networking Conference*. TTM: an efficient mechanism to detect wormhole attacks in wireless *ad-hoc* networks (IEEE, Las Vegas, January 2007), pp. 593–598
11. T Korkmaz, in *Proceedings of International Conference on Information Technology: Coding and Computing*. Verifying physical presence of neighbors against replay-based attacks in wireless *ad hoc* networks (IEEE, Las Vegas, 4–6 April 2005), pp. 704–709
12. S Capkun, L Buttyan, JP Hubaux, in *Proceedings of the First ACM Workshop on Security of ad hoc and Sensor Networks*. SECTOR: Secure tracking of node encounters in multi-hop wireless networks (ACM, Virginia, 31 October 2003), pp. 21–32
13. R Poovendran, L Lazos, A graph theoretic framework for preventing the wormhole attack in wireless *ad hoc* networks. ACM J. Wireless Netw. **13**(1), 27–59 (2007)
14. Y Wang, Z Zhang, J Wu, in *Proceedings of IEEE Fifth International Conference on Networking, Architecture and Storage*. A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information (IEEE, Macau, 15–17 July 2010), pp. 63–72
15. X Ban, R Sarkar, J Gao, in *Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. Local connectivity tests to identify wormholes in wireless networks (ACM, Paris, 16–20 May 2011)
16. W Znaidi, M Minier, JP Babau, in *Proceedings of IEEE international Symposium on Personal, Indoor and Mobile Radio Communications*. Detecting wormhole attacks in wireless networks using local neighborhood information (IEEE, Cannes, 15–18 September 2008), pp. 1–5
17. MY Su, WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Comput. Security. **29**(2), 208–224 (2010)
18. R Matam, S Tripathy, in *Proceedings of the 8th International Conference on Information Systems and Security*. Defence against wormhole attacks in wireless mesh networks (Springer LNCS, Guwahati, 15–19 December 2012), pp. 181–193
19. J Zhou, J Cao, J Zhang, C Zhang, Y Yu, in *Proceedings of IEEE 26th International Conference on Advanced Information Networking and Applications*. Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed (IEEE, Fukuoka, 26–29 March 2012), pp. 59–66
20. T Hayajneh, P Krishnamurthy, D Tipper, in *Proceedings of Third International Conference on Network and System Security*. DeWorm: A simple protocol to detect wormhole attacks in wireless *ad hoc* networks (IEEE, Gold Coast, 19–21 October 2009), pp. 73–80
21. DB Johnson, DA Maltz, YC Hu, The dynamic source routing protocol for mobile ad-hoc network (DSR), IETF internet draft. (IETF MANET Working Group, Fremont, 2004)
22. J Eriksson, M Faloutsos, S Krishnamurthy, in *Proceedings of IEEE International Conference on Network Protocols*. Routing amid colluding attackers (IEEE, Beijing, 16–19 October 2007)
23. CE Perkins, EM Royer, SR Das, *Ad hoc* on-demand distance vector (AODV) routing, IETF internet draft. (IETF MANET Working Group, Fremont, California USA, 2004)
24. B Swathi, S Tripathy, R Matam, Secure peer-link establishment in wireless mesh networks. Adv. Intell. Syst. Comput. **176**, 189–198 (2012)
25. BN Clark, CJ Colbourn, DS Johnson, Unit disk graphs. Discrete Math. J. **86**(1-3), 165–177 (1990)
26. D De Couto, D Aguayo, J Bicket, R Morris, in *Proceedings of MobiCom*. A high-throughput path metric for multi-hop wireless routing (ACM, San Diego, 14–19 September 2003), pp. 134–146
27. R Draves, J Padhye, B Zill, in *Proceedings of ACM MobiCom*. Routing in multi-radio multi-hop wireless mesh networks (ACM, Philadelphia, 26 September–1 October 2004), pp. 114–128
28. The OMNeT++ Network Simulator. www.omnetpp.org. Accessed 23 September 2011

doi:10.1186/1687-1499-2013-180
Cite this article as: Matam and Tripathy: **WRSR: wormhole-resistant secure routing for wireless mesh networks.** *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:180.