PLOS ONE

RESEARCH ARTICLE

Geographic Wormhole Detection in Wireless Sensor Networks

Mehdi Sookhak[1]*, Adnan Akhundzada[1], Alireza Sookhak[2], Mohammadreza Eslaminejad[3], Abdullah Gani[1], Muhammad Khurram Khan[4], Xiong Li[5], Xiaomin Wang[6]

1 Center for Mobile Cloud Computing (C4MCC), University of Malaya, Kuala Lumpur, Malaysia, **2** Fiber Optics Communication Networks Project Manager, Fars Regional Electric Co., Shiraz, Iran, **3** Faculty of Computing and Information System, Universiti Teknologi Malaysia, Johor, Malaysia, **4** Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia, **5** School of Computer Science and Engineering, Hunan University of Science and Technology, Hunan 411201, Xiangtan, China, **6** School of Information Science & Technology, Southwest Jiaotong University, Chengdu, China

* m.sookhak@ieee.org

Citation: Sookhak M, Akhundzada A, Sookhak A, Eslaminejad M, Gani A, Khurram Khan M, et al. (2015) Geographic Wormhole Detection in Wireless Sensor Networks. PLoS ONE 10(1): e0115324. doi:10.1371/journal.pone.0115324

Academic Editor: Cheng-Yi Xia, Tianjin University of Technology, CHINA

Received: May 30, 2014

Accepted: November 21, 2014

Published: January 20, 2015

Data Availability Statement: Relevant data are included within the Supporting Information files. Source code is publicly available to readers and outside researchers without restrictions via Github through each of the following links:1. https://github.com/Afshinking/Wormhole.git.2. http://afshinking.github.io/Wormhole/.

Funding: This work is carried out as a part of the Mobile Cloud Computing research project funded by the Malaysian Ministry of Higher Education under the University of Malaya High Impact Research Grant with reference UM.C/HIR/MOHE/FCSIT/03. This work also is partly supported by the National Natural

Abstract

Wireless sensor networks (WSNs) are ubiquitous and pervasive, and therefore; highly susceptible to a number of security attacks. Denial of Service (DoS) attack is considered the most dominant and a major threat to WSNs. Moreover, the wormhole attack represents one of the potential forms of the Denial of Service (DoS) attack. Besides, crafting the wormhole attack is comparatively simple; though, its detection is nontrivial. On the contrary, the extant wormhole defense methods need both specialized hardware and strong assumptions to defend against static and dynamic wormhole attack. The ensuing paper introduces a novel scheme to detect wormhole attacks in a geographic routing protocol (DWGRP). The main contribution of this paper is to detect malicious nodes and select the best and the most reliable neighbors based on pairwise key pre-distribution technique and the beacon packet. Moreover, this novel technique is not subject to any specific assumption, requirement, or specialized hardware, such as a precise synchronized clock. The proposed detection method is validated by comparisons with several related techniques in the literature, such as Received Signal Strength (RSS), Authentication of Nodes Scheme (ANS), Wormhole Detection uses Hound Packet (WHOP), and Wormhole Detection with Neighborhood Information (WDI) using the NS-2 simulator. The analysis of the simulations shows promising results with low False Detection Rate (FDR) in the geographic routing protocols.

Introduction

Security of wireless sensor networks (WSNs) has gained considerable interest more recently. Mainly because the sensory nodes, having limited computational and communicational resources, providing a secure routing protocol is performing a complex task in WSNs [1, 2].

Routing in WSNs is challenging because of unique characteristics that make WSNs different from other wireless networks, such as Mobile Ad Hoc Networks (MANET). Such characteristics consist of (a) Traditional IP-based methods for WSNs are inapplicable because of the

Science Foundation of China under Grant no. 61300220 and NSFC project 61371098. Fars Regional Electric Co. provided support in the form of a salary for author AS, but did not have any additional role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript. The specific roles of these authors are articulated in the 'author contributions' section.

Competing Interests: The authors confirm that Dr. Muhammad Khurram Khan is a PLOS ONE Editorial Board member and this does not alter their adherence to PLOS ONE Editorial policies and criteria. Alireza Sookhak is an employee of Fars Regional Electric Co. There are no patents, products in development or marketed products to declare. This does not alter the authors' adherence to all the PLOS ONE policies on sharing data and materials.

deployment of the large number of sensor nodes in the network. (b) The majority of applications of sensor networks transmit the data to a specific base station. (c) Sensor nodes require a particular resource management due to the fact that the battery, storage, and processing capabilities of sensors are limited. (d) In contrast to traditional wireless networks, almost all nodes in WNSs are immobile after deployment or have a very low mobility. (e) The sensor nodes in WSNs require a particular hardware (e.g., GPS) to find the position of the other nodes due to the location-based data collection. (f) To augment the energy and bandwidth utilization of the routing protocols in WSNs, the data redundancy during data collection has to be reduced. Despite the fact that considerable progress has been made in the past few years pertaining to advancement in WSNs, providing a secured routing protocol has received more attention from the researchers [3–7]. There are several attacks that threaten the security of the routing protocols in WSNs that cause different problems, such as changing the routing protocol and threatening confidentiality, availability, and integrity of the transmitted packets. The WSN security attacks include selective forwarding, sinkhole, Sybil, wormholes, hello flood, and acknowledgement spoofing attacks [8–12]. However, the wormhole attack is more harmful than the others, because it does not need to compromise a sensory node within the network. Moreover, the wormhole attack is able to easily cause other types of attacks, such as Sybil attack. Furthermore, using a cryptographic technique cannot prevent wormhole attacks [13–16].

Significant amount of work has recently been carried out to prevent the wormhole attacks in wireless ad hoc networks. Such methods typically detect the attacks on the basis of indications that are generated by the wormholes. However, most of the existing methods require either particular hardware devices e.g., GPS [13, 17], directional antennas [18], special radio transceiver modules [19], or strong assumptions on the networks e.g., precise synchronized clock [13], guard nodes [20], unit disk communication models [21], or safe and attack-free environments [22]. Employing such requirements and assumptions restrict the application of the methods in geographical routing protocols that include a huge number of resource-constrained sensor nodes.

This paper presents a unique method to detect the dynamic and static wormhole attacks in geographic routing protocols (DWGRP). The main contribution of this paper is to create a new type of pairwise key predistribution [23] based on the beacon packets in order to detect the malicious nodes more efficiently. The proposed method is able to detect malicious nodes and select the best and most reliable neighbor without any specific assumptions and is not subject to any requirements for extra hardware devices. The simulation results demonstrate the effectiveness of the proposed method and indicate that the probability of wormhole detection in the DWGRP method is considerably higher than the related techniques.

0.1 Geographical Routing Protocols

Location-based routing protocols are an important group of protocols in WSNs in which position information is used to route data towards the desired regions (sinkhole). Location-based routing, is also known as position-based, directional, geographic, or geometric routing [24]. This section briefly reviews the geographic routing protocols.

The geographic routing protocols are classified into five groups, based on how the next hop is chosen. The Greedy Routing Scheme (GRS) is the first group of geographic routing protocol in which each node selects the best node among the neighbors that is closest to the destination. GPSR is an example algorithm falls in this category in which a packet should be forwarded hop by hop based on GRS and available local information, which is actually gathered by the Global Positioning System (GPS) until it meet a void area. In this way, the received message must be passed to the first neighbor counterclockwise about itself [25]. The next group of the geographic routing protocols is called Most-Forward-within-R strategy (MFR). In MFR, the packet is sent to

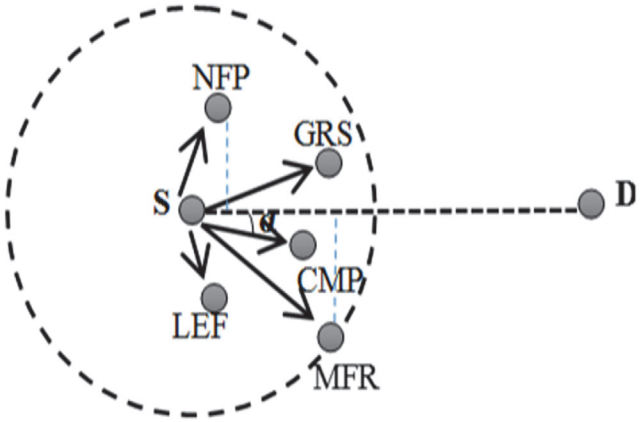

Figure 1. Forwarding approaches in geographic routing protocols.

doi:10.1371/journal.pone.0115324.g001

the most forward node to destination among the neighbors of the sender based on the transmission range (R). The third approach is the Nearest-Forward-Progress scheme (NFP) in which the nearest neighbor to the transmitter is chosen to send data. The compass routing scheme (CMP) is the fourth method among the geographical routing protocols. In this scheme, the neighbor that has a minimum angle to the imaginary line between the source and destination is selected as the next hop. Low-energy forward scheme (LEF) selects a neighbor that requires a minimum energy to transmit packets. However, among these geographic routing protocols, the GRS is more popular and more applicable than the other methods due to the rate of delay and energy of this method [26, 27]. Fig. 1 illustrates how the next node will be selected in the different type of forwarding approaches to transfer packet from source (S) to destination (D) node.

0.2 Complex Network

Complex network is theoretically defined as a graph with non-trivial topological, function and dynamical features of many real networks, which does not exist in a simple network such as lattices, random graphs, degree distribution, a high clustering coefficient, assortativity or disassortativity [28]. WSNs can be considered as a specific type of complex networks, because it includes large-scale distributed sensor nodes in which the sensor nodes have the capability to communicate with the sensor nodes in the predefined region.

Li et al. [29] presented a novel local-world model of WSN that consists of two types of nodes such as sensor node and sink node. The sensor nodes are responsible for gathering data information from the environment and transferring data to the sink nodes. The received data are finally sent to gateway through other sink nodes. The proposed model is able to balance the energy consumption by minimizing the connectivity of sink nodes on the basis of the energy of each sensor node. The authors also identified that the degree distribution can be described as an integral in relation to proportion of sink nodes and energy distribution by using mean-field theory [30].

The theory of complex network encounters new challenges due to the requirement of understanding appropriately the dynamical characterization of real systems, especially when the systems consist of two or more interconnected networks [31]. As a result, to understand the complicated changeability of real complex systems that include various time scales and structural patterns, it requires defining a new concept as a multiplex network. The multiplex network refers to a multilevel system in which each layer has particular and unique characteristics and the layers are connected by a richer structure of interactions. The interconnection between layers in such multilevel graph-based structure shows how the nodes of different levels are

connected and influence each other. This type of graphs can be used to analyse numerous biological systems and many social networks, such as Twitter and Facebook [32].

Since the epidemics are able to spread across the multiplex network, extensive studies have been carried out to analyse dynamical epidemics in recent years. However, most of the existing studies only focused on epidemics spread over single transmission route. Zhao et al. [33] was the first to analyse multiple routes transmitted epidemic on the multiplex network and propose a two routes transmitted epidemic spreading on two network layers. This method is adopted the Susceptible Infected Removed (SIR) model [34] in which each node includes three compartments, such as susceptible (disposed to be infected), infectious (already infected), and recovered from disease. The authors also accurately calculated outbreak size of the epidemic and the epidemic threshold of the multiplex network. Moreover, they suggested two measures for determining the level of inter-similarity of two layers, such as average similarity of neighbors (ASN) and degree degree correlation (DDC). The ANS is used to evaluate the average of similarity of nodes in different layers while the DDC indicates the correlation of node's degree in different layers.

One of the important application of the complex network is to analyze the traffic system of metropolises [35]. To achieve this goal, the researchers proposed multi-layered real-world systems as an interconnected network in which various social behavior roles are assigned to various layers. For example, in city traffic system, two interdependent networks need to be designed with two types of link, such as connectivity and dependency [36]. Recently, the researchers have found that the percolation and cascade failures properties in dynamic complex systems are affected by the topology of each interdependent layer. However, most of the existing models are unable to describe the complicated cascade failures of real complex traffic systems in which various attacking rules and load patterns exist simultaneously.

In [37], Su et al. considered this problem and designed a flow redistribution model for cascading failures on the basis of redistribution of traffic flow in two different types of interrelated networks, such as dependent network (subway network) and connected network (bus network). The authors exposed that there are non-equilibrium phase transitions at the point of low network capacity in the city traffic system. By using this characteristic, they explained why a small increase in the number of buses during rush hours has an impalpable effect on the traffic congestion. Moreover, they uncover that removing a node of the bus network randomly can cause a traffic jam. Nevertheless, when the damage is inconspicuous, this type of traffic jam can be released by increasing the number of buses.

Complex network also can be used to model the infectious diseases. In [38], Xia et al. explored the effects of delayed recovery and non-uniform transmission on the propagation of diseases on structured populations. They found that rescheduling the transition from the infectious to the recovered states resulted in diminishing the epidemic threshold. Sanz et al. [39] designed a comprehensive framework for explaining the spreading dynamics of two concurrent diseases. The authors also represented the epidemic thresholds of the two diseases and computed the temporal evolution to characterize the unfolding dynamics.

Our work is entirely based on simple classical networks, which includes a single layer. Considering it for multiplex networks will certainly have great contribution to the research community. Keeping in view, the complexity of multiplex networks; an extension of our work need to be redesigned and are considered in our future plans.

0.3 Wormhole Attack

Wormhole attack usually occurs by connecting at least two malicious nodes via an out-of-band connection that is called tunnel. The first malicious node eavesdrops or receives packets in one area and then tunnels the packets to the next malicious node that is placed at another point of

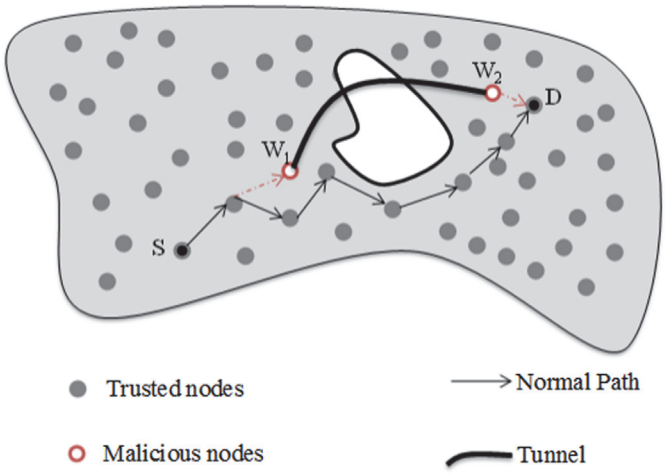

Figure 2. The wormhole attack.

doi:10.1371/journal.pone.0115324.g002

the network. The tunnel is created either by using direct wired link or by using a long-range directional wireless link [40, 41]. Fig. 2 depicts the following scenario, since the source node (*S*) directs packets to the destination node through the normal path, however, in the case of a wormhole attack; the packets are actually eavesdropped by the first malicious node (*W*1) and then tunneled to second malicious node (*W*2). Consequently, *W*2 pass on the packets to the terminus node (*D*). The tunneled packets arrive earlier than the packets through normal path. Therefore, the remaining packets that follow the normal path will be dropped by the destination node.

The wormhole attacks can be categorized into two groups based on the type of malicious nodes, such as static and dynamic wormhole. The static wormhole attack occurs when the malicious nodes are statically located along the path to the destination. For example, the wormhole attack that is created by the malicious nodes *W*1 and *W*2 in Fig. 3.(a) is static. In the dynamic wormhole attack, initial deployments of the malicious nodes are not placed within the normal path to the destination. However, the malicious nodes are able to obtain the routing information by overhearing and processing the data packets. Afterwards, such nodes move

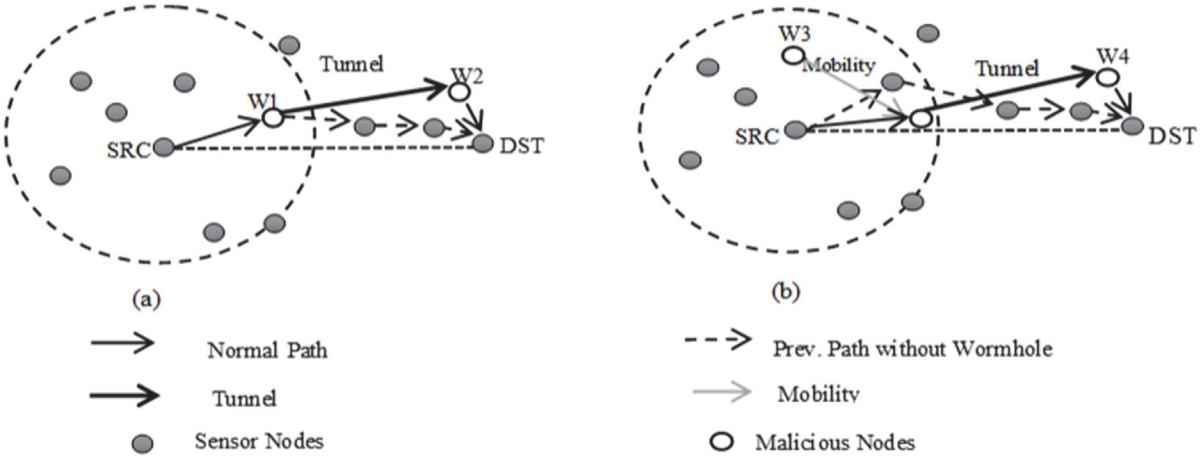

Figure 3. Wormhole attack in geographical routing protocols, (a) static wormhole, (b) dynamic wormhole.

doi:10.1371/journal.pone.0115324.g003

toward the specific path for receiving the message and create the dynamic wormhole. As a result, identification of the dynamic wormhole is more difficult than the static type [40]. Fig. 3.b illustrates the dynamic wormhole attack.

The remaining paper is organized as follows. Section 2 presents a new classification technique of the wormhole detection methods to highlight the advantages and the disadvantages of the related works. Section 3 describes proposed wormhole detection method. The performance analysis of the proposed wormhole detection method and the comparison with other similar methods is presented in Section 4. Finally, the concluding remarks are provided in Section 5.

1 Related Works

Fig. 4 presents the new classification of wormhole detection methods on various routing protocols on the basis of the specific characteristics. The wormhole detection methods are classified into three categories, namely: (a) Time-based approaches, (b) Location-based approaches, and (c) Neighborhood- based approaches.

1.1 Time-based approaches

The first type of wormhole detection methods is the Time-based approach in which the anomaly is detected based on the time mismatch of the forwarding packets [42]. In [13], Yih-Chun et al. proposed temporal leash method based on tightly synchronized clocks to restrict the maximum transmission time from source to destination. Using this method in sensor networks requires applying time synchronization level that is impractical [43]. Another method is designed by Karlsson et al. [44] to detect the wormhole attack in MANET based on Traversal

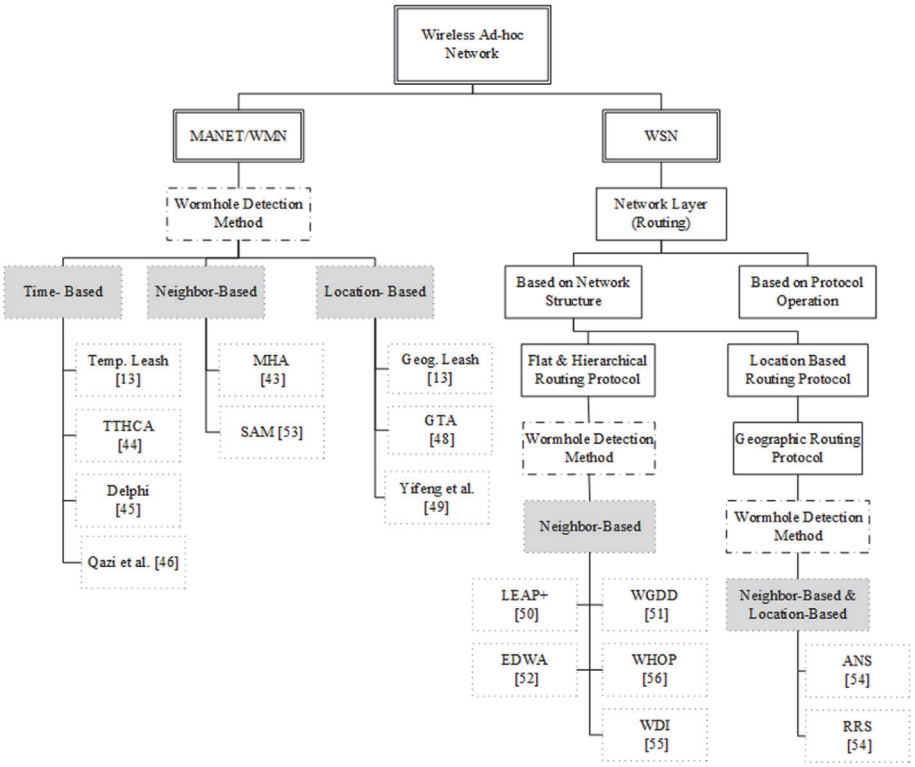

Figure 4. Taxonomy of wormhole detection methods.

doi:10.1371/journal.pone.0115324.g004

Time and Hop Count Analysis (TTHCA). Hon Sun et al. [45] considered the rate of delay per hop and introduced a method that is named DELPHI. By comparing the normal path and a path with wormhole attack with same hop, the authors found that when the wormhole happens, the rate of delay will be more than the normal path. Qazi et al. [46] enhanced the security of dynamic source routing (DSR) protocol against wormhole attacks based on calculation of round trip time (RTT).

1.2 Location-based approaches

The second group of wormhole detection approaches is known as the location-based approaches. The core idea behind such a method is to use the location information of the nodes to identify the malicious nodes [47]. Yih-Chun et al. [13] was the first to introduce a location-based approach, namely the Geographic Leashes in which all of the nodes know their location and use a loosely synchronized clock to achieve global serialization. When the packet is sent to the destination, each node attaches the transmission time and its location to packet. After the packet is successfully received by the next node, firstly, the distance to sender and the traversal time are calculated to determine the wormhole attack. The work of Lazos et al. [48] is an attempt to detect wormhole attack in ad hoc networks on the basis of establishing Local Broadcast Keys (LBK) for nodes, that is called graph theoretic approach (GTA). This method also needs to use a special localization equipment and GPS. However, the main drawback of such a model is that it is not readily applicable to mobile networks. In [49], the authors introduced a method to detect the wormhole attack in MANETs based on the distance verification and using the received signal strength (RSS) and statistical hypothesis testing. The main idea of the distance verification is to verify the computed distance using a RRS measured distance to the sender.

1.3 Neighborhood-based approaches

In the neighborhood-based approaches, the wormhole attack is detected by analyzing the characteristics of the neighbor nodes. The localized encryption and authentication protocol (LEAP+) is a detection approach implemented by Zhu et al. [50] based on clustering and defining four types of key for each sensor node: (a) a pairwise key shared with another sensor node, (b) an individual key shared with the base station, (c) a cluster key shared with multiple neighboring nodes, and (d) a group key that is shared by all of the nodes in the network. The drawback of this model is that it can only be applicable for static or immobile sensor networks and is not readily applicable to the mobile networks. The multipath hop-count analysis (MHA) is implemented based on analyzing the hops to avoid wormhole attack in MANETs [43]. The MHA method consists of three steps: (a) calculating the hop-count values of all routes to the destination, (b) selecting secure set of routes for data transmission, and (c) broadcasting the packet through the safe routes. Generally, it helps when the wormhole attacks occur in a way that the number of hops will be lesser than normal situation. However, this method is impractical when the malicious nodes are able to create the virtual hops to deceive the detection algorithm.

Xu et al. [51] proposed a wormhole geographic distributed detection (WGDD) approach to detect a wormhole by using a hop count technique, reconstructing local maps in each node, and then using a "diameter" feature to detect abnormalities caused by wormholes. Another mechanism is end-to-end detection of wormhole attack in wireless ad-hoc networks (EDWA) [52], which is used to detect wormhole attacks in an ad-hoc routing protocol based on hop-count scenario. EDWA has two steps: (1) detection of a wormhole by estimating shortest path, and (2) identifying the malicious nodes based on the shortest path. After that the source

node compares the hop-count which is retrieved from the Route Reply (h_r) with the number of hops within the shortest path to the destination (h_e). The wormhole attack has occurred if and only if $h_r \leq h_e$. However, this model also has several assumptions which have to be considered like using Global Positioning System (GPS) and using TESLA for authentication. Song and Li [53] designed another mechanism in multi-path routing wireless ad-hoc networks based on Statistical Analysis of the Multi-path (SAM). The main idea behind this method is to monitor the statistics of the route discovery that dramatically changes under wormhole attack.

Wormhole attack is able to effect geographic routing protocols. However, there is a little work that focused on detecting wormhole on the basis of geographic routing protocols such as RRS and ANS. Poornima and Bindhu [54] proposed two different methods for dynamic and static wormholes. Reverse Routing Scheme (RRS) is the first technique that attempts to recognize static wormhole attack by means of Hop-Count mechanism. The author of RRS method has indicated that this method is related to choosing a proper threshold. However, selecting a threshold is not always easy. Furthermore, this method cannot identify a high number of malicious nodes. Authentication of Nodes Scheme (ANS) [54] is the next method that uses digital signature to prevent the wormhole attacks. Once a packet is directed to the destination, each node is responsible to insert its digital signature in the forwarding packet. Since the malicious nodes are not able to sign the transmitted packet without the key, the author claims, the destination node can find them easily. However, the performance of this method is based on digital signature (RSA). It is assumed that just the trusted nodes have a reliable signature. If the adversary is able to break RSA, then there are no obstacles to create wormholes. Furthermore, the computational cost involved in signing every packet is very high. On the other hand, the verification of intermediates nodes is determined just in the destination node. This process has several consequences for the network functionality

2 Proposed Wormhole Detection Method

This section presents the proposed scheme of wormhole attack detection in geographical routing protocol (DWGRP). One of the main characteristics of our scheme, which makes it different from the previous approaches, is to detect and eliminate the malicious nodes before the packet is sent to the destination. Furthermore, if the adversary breaks the trust level between two adjacent nodes that is generated using an updated version of the pairwise key [23], the certification of this path is denied in the destination. The DWGRP approach consists of three main steps, as follows:

(a) Deploying nodes: generating the new pairwise key to construct neighborhood tables.
(b) Intermediate step: identifying trust neighbors and detecting malicious nodes with respect to the secure shared keys.
(c) Destination step: identifying untrusted packets upon receiving them at the destination.

Fig. 5 displays the flowchart of the proposed wormhole detection method (DWGRP) [55]. The rest of this section explains in detail the wormhole attack proposed detection method in geographical routing protocol.

2.1 Key Management phase

Each sensor node requires a pair of public and private keys to communicate with the other nodes through the secure channel. We propose a new pairwise distributed key secure based on one-way hash function to generate the public and private key for sensor node, as follows:

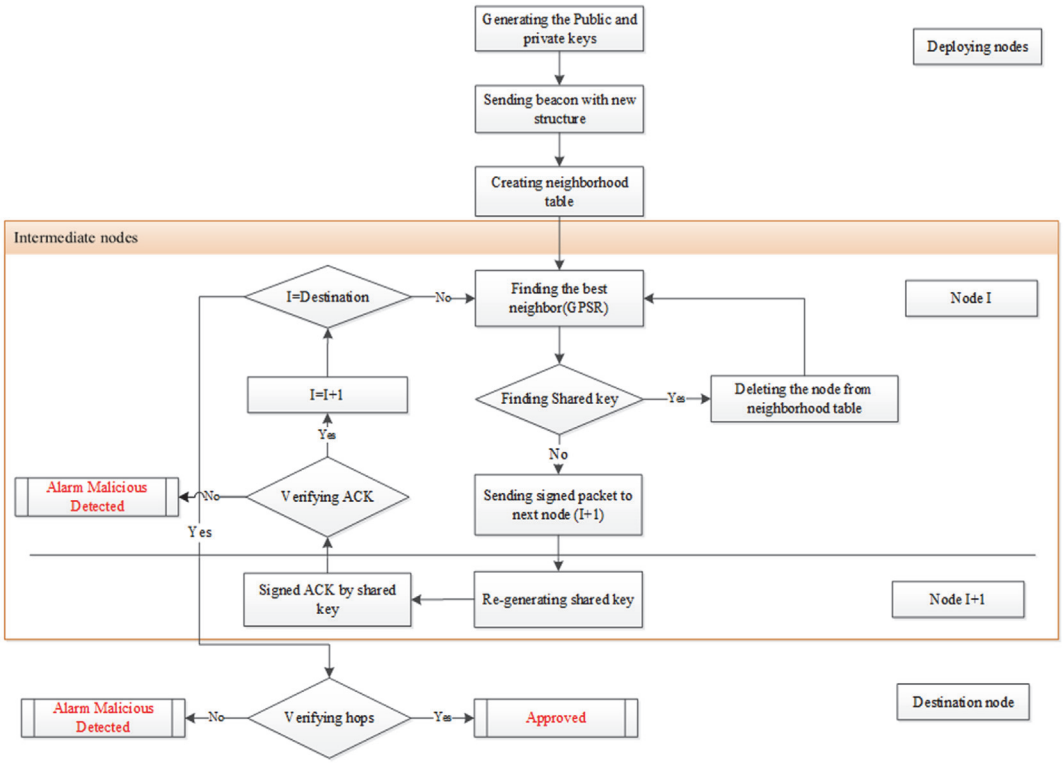

Figure 5. Wormhole detection algorithm.

doi:10.1371/journal.pone.0115324.g005

2.1.1 Public key generation

The key pool (KP) is a matrix with size $(y + 1) \times N$ where N is number of sensor nodes and y is desired level of trust or the number of potential private keys. We construct this matrix by using a secure one-way hash function $x_i = Hash(k, N)$, where k is assumed the smallest prime number larger than 2^{64}. Then, a key pool can be designed as follows:

$$KP = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ x_i & x_i^2 & x_i^3 & \dots & x_i^N \\ x_i^2 & (x_i^2)^2 & (x_i^2)^3 & \dots & (x_i^2)^N \\ & \ddots & & \vdots & \\ x_i^y & (x_i^y)^2 & (x_i^y)^3 & \dots & (x_i^y)^N \end{bmatrix}_{(y+1)\times N} \quad (1)$$

Since the sensor nodes have constrained resources, each node i only need to store the corresponding seed x_i to generate its column as a public key.

2.1.2 Private Key generation

After generating the key pool, the private key of the sensor nodes needs to be computed. Firstly, y symmetric matrixes with size $(y + 1) \times (y + 1)$ are calculated by using a secure one-way hash

function, as follows:

$$Pr_i = \begin{bmatrix} 1 & x_i & x_i^2 & \dots & x_i^y \\ x_i & x^2 & (x_i^2)^2 & \dots & (x_i^y)^2 \\ x_i^2 & (x_i^2)^2 & (x_i^2)^3 & \dots & (x_i^y)^3 \\ & \ddots & & \vdots & \\ x_i^y & (x_i^y)^2 & (x_i^y)^3 & \dots & (x_i^y)^y \end{bmatrix}_{(y+1)\times(y+1)} \quad (2)$$

where $x_i = Hash_{i-1}(k, N)$, and $1 \leq i \leq y$. Then, the private key matrixes of sensor nodes with size $(y + 1) \times N$ are computed by:

$$P_i = (Pr_i * KP)^T \quad (3)$$

As a result, y potential private keys are computed for each node (i) that consists of the corresponding row (row_i) from matrixes $P_1\ P_2 \ldots P_y$. Due to the resource restriction of sensor nodes, we select α private keys for each node ($2 \leq \alpha \leq y$) randomly among of these y potential private keys.

2.2 Creating neighborhood table

After generating the private keys, each node sends a beacon packet which includes ID, location and destination, to find its neighbor nodes and update its neighborhood table. In order to find malicious nodes, we modify the beacon packets and the neighborhood tables structure of the sensor nodes by inserting the list of the private key matrixes (P_i) into the beacon packet. In other words, the new beacon packet includes Node ID, Location, ID of Public key (KP), a list of matrix numbers of private keys and destination. The structure of beacon is illustrated in Fig. 6.

When the beacon packet is received by the neighbor nodes, they update their neighborhood table. If the node ID is found in the table, its location, the public key and list of private keys are updated otherwise one row is added to the neighboring table of the node. Fig. 7 shows the structure of neighborhood table.

2.3 Intermediate step

Regarding the GPSR protocol, the best neighbor node is the nearest node to the destination. We modify this rule in GPSR and add a restriction for selecting the best neighbors based on the list of private keys. In other words, when node A finds the best neighbor B from its neighborhood table, the list of private keys of node A needs to be compared with the list of private keys of node B. Then, node B is selected as a next node if and only if at least one private key of node

Node ID	Public key ID	List of private keys	Destination

Figure 6. Structure of beacon Packet.

doi:10.1371/journal.pone.0115324.g006

Neighbor ID	Location	Public key ID	List of private keys

Figure 7. Neighborhood table.

doi:10.1371/journal.pone.0115324.g007

A and B is selected from the same matrix. If they have no similar matrices, node B is eliminated from the neighborhood table and this phase repeats again to find the best neighborhoods.

$$B = \textit{best neighbour of } A \leftrightarrow \exists P_i | Pr_B \subset P_i \textit{and} Pr_A \subset P_i \tag{4}$$

where the list of private keys of node B is Pr_B and Pr_A is the list of private keys of node A.

2.3.1 Shared key generation phase

When the best neighbor is selected, the node needs a shared key to communicate with its neighbors securely. The shared key is created for each pair of two nodes that have a private key from the same matrix Pi. For example, if nodes i and j have a key form matrix P_1, the shared key can be calculated by:

$$P_1 * K\mathrm{P} = (Pr_1 * \mathrm{K}P)^T * K\mathrm{P} = KP^T * Pr_1^T * KP \tag{5}$$

We have mentioned it earlier that Pr is symmetric matrix, then $Pr_1^T = Pr_1$. Therefore, $P_1 * kP$ is equal to:

$$\begin{aligned} &P_1 * KP = KP^T * Pr_1 * KP = KP^T * (Pr_1 * KP) \\ &\Rightarrow P_1 * KP = ((Pr_1 * KP)^T * KP)^T \end{aligned} \tag{6}$$

Then, the result of $P_1 * kP$ is a symmetric matrix with size $N \times N$ in which $SK_{ij} = SK_{ji}$ is the shared key between nodes i and j. After generating the shared secret key, the packet and the selected index are sent to the best neighbor by using the shared key. It is important to mention that we assume our network is completely dense and each node has at least one neighbor with the same specification.

2.3.2 Verification phase

When the packet is received by the best neighbor (for example node B), this node extracts the index from the packet and regenerate the shared key. Then, node B creates an ACK message, signs it by using a shared key, and sends it to node A. If the ACK message is verified by node A, node B is a trusted node, otherwise node B is a malicious node. Therefore, Node A generates an alarm message and broadcast to the network that the node for eliminating the malicious node from their neighborhood tables.

2.4 Destination Step

When a packet is received by the destination node, the probability of wormhole attack happening is checked based on the distance between source node to the destination node and the number of hops from source to destination. A necessary condition for detecting wormhole in destination node is:

$$\sqrt{(x_d - x_s)^2 + (y_d - y_s)^2} > R * h \tag{7}$$

where the location of the source node is (x_s, y_s), (x_d, y_d) is the location of the destination, R is the radio range of nodes, number of hops from source to destination is shown by h. When the wormhole is detected, a request packet is sent to source node in order to send a packet again from another path.

3 Evaluation

We conduct the mathematical modelling and extensive simulations under various situations to evaluate the effectiveness of our wormhole detection approach. We evaluate the probability of miss detection and successful wormholes detection by altering the node density and the number and type of wormholes inside the network.

3.1 Miss detection probability analysis

Miss detection probability is a crucial metric to evaluate wormhole detection methods. According to key distribution of this method, there are y potential private keys for N sensor nodes in the network and each sensor node randomly selects α private keys ($\alpha \leq y$). Therefore, the probability of a specific key belonging to one node is equal to $\lfloor \frac{\alpha}{y} \rfloor$ while the malicious nodes do not have a private key. If the adversary is able to compromise x nodes, the probability that just m nodes from x nodes ($m \leq x \leq N$) contain the specific key (K_i) from y potential private keys is computed by:

$$P(k_i) = \binom{x}{m} \left(\frac{\alpha}{y}\right)^m \left(1 - \frac{\alpha}{y}\right)^{x-m} \tag{8}$$

Therefore, the probability of breaking one link by an adversary is calculated in below formula:

$$P(l) = \sum_{m=1}^{x} \binom{x}{m} \left(\frac{\alpha}{y}\right)^m \left(1 - \frac{\alpha}{y}\right)^{x-m} \tag{9}$$

Where x is the number of compromised nodes, numbers of selected nodes are shown by m, y is the number of potential private keys and α is equal to the number of private keys for each node.

To create a wormhole in geographic routing protocol necessitates two or more malicious nodes to receive packets at one point of the network and forward those packets to another location by a wireless or wired tunnel. Therefore, as shown in Fig. 8, the adversary needs to break more than 1 link to create the wormhole attack in the network.

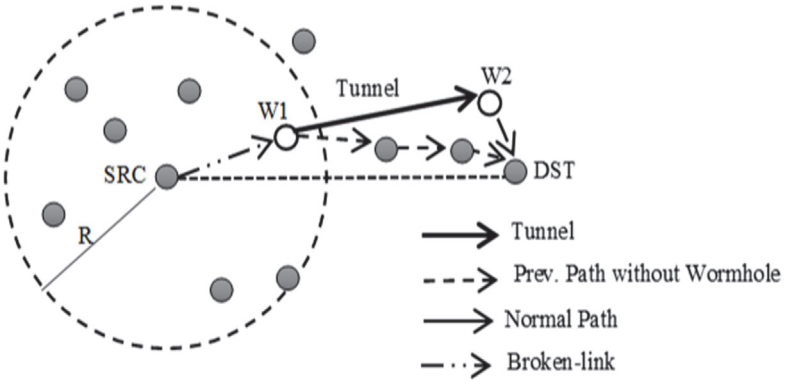

Figure 8. Creating wormhole by breaking two link in geographic routing protocols.

doi:10.1371/journal.pone.0115324.g008

If there are h hops from source node to destination, the adversary needs to break j link ($j < h$) to create wormhole attack. Then, the probability of creating wormholes by the attacker is:

$$\begin{aligned} P(Wormhole) &= \binom{j}{h} P(l)^j (1 - P(l))^{h-j} \\ &= \binom{j}{h} \cdot \left(\sum_{m=1}^{x} \binom{x}{m} \left(\frac{\alpha}{y}\right)^m \left(1 - \frac{\alpha}{y}\right)^{x-m} \right)^j \\ &\quad \cdot \left(1 - \sum_{m=1}^{x} \binom{x}{m} \left(\frac{\alpha}{y}\right)^m \left(1 - \frac{\alpha}{y}\right)^{x-m} \right)^{h-j} \end{aligned} \tag{10}$$

where h = the number of hops, j = the number of broken links, x = the number of compromised nods, α indicates the number of private keys for each node and y is the number of potential private keys.

Fig. 9 shows the probability of a broken link where the number of potential private keys is 6 ($y = 6$), the number of private keys is 3, 4, or 5 ($\alpha = 3$, 4, or 5), the maximum number of compromised nodes is 100 (x = 100) and the number of hops from source to destination node is equal to 10 ($h = 10$). It can be seen that when the amount of compromised nodes are less than 55, the attacker cannot break the link, but with the increase of the number of compromised nodes, the probability of broken link is increasing too till the number of compromised node is equal to 70 and the attacker can break the link. Fig. 9 also shows that when the number of compromised nodes is less than 55 or more than 65, the adversary cannot create the wormhole attack otherwise the maximum rate of miss detection wormhole is about 0.3 when the number of compromised nodes is from 55 to 65 (S1 Table).

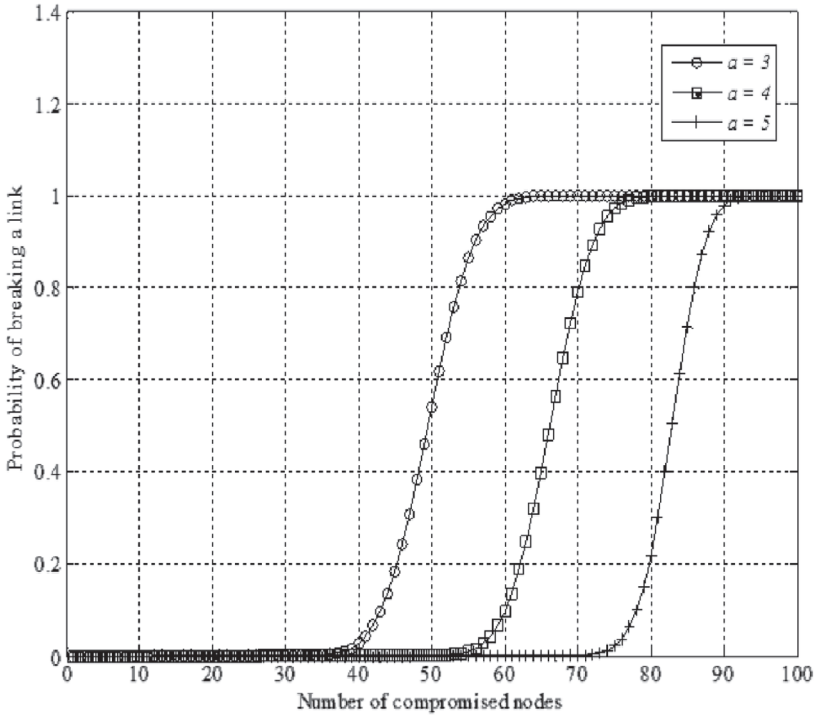

Figure 9. Probability of breaking a link when $y = 6$ and ($\alpha = 3$, 4, or 5).

doi:10.1371/journal.pone.0115324.g009

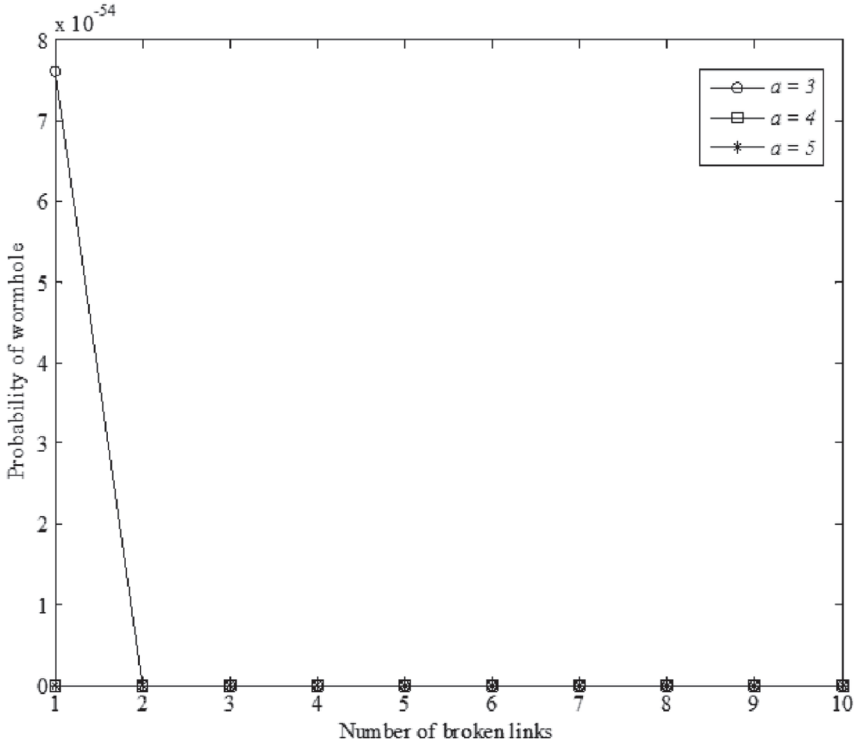

Figure 10. Probability of miss detection $y = 6$ and ($\alpha = 3$, 4, or 5).

doi:10.1371/journal.pone.0115324.g010

In Fig. 10, the comparison of the probability of miss detection is illustrated when the number of private keys is 3, 4, or 5 ($\alpha = 3$, 4, or 5) and the number of hops from source to destination node is equal to 10 ($h = 10$). As it is shown, our method is able to detect almost all wormhole attacks (S2 Table).

3.2 Simulation Setup

We use simulator NS-2 to evaluate the performance of our scheme for detecting wormhole attack in geographic routing protocols. We deploy 200 nodes randomly in a square area of size $1000 * 1000\ m^2$ square area with multiple holes inside. The transmission range of each node is set to 150 m. The number of malicious nodes is considered between 2 to 10 nodes, which can change their location to create the wormhole attack. We implement the GPSR routing protocol and then improve the structure of beacon and neighborhood table based on our method. Each node broadcasts the beacon packets periodically with a nominal interval of 0.3 seconds to update its neighborhood table. We present our results after averaging of 100 simulation runs. All simulation parameters are shown in the Table 1.

Before simulating our method, the impact of wormhole attacks on geographic routing protocols is illustrated in Fig. 11. We transfer 1250 packets within 20 hops and monitor the network to find the number of packets that are sent through the malicious nodes, are called untrusted packets. As it is clear, the wormhole attack is capable of transferring nearly 60% of the packets. Since the malicious nodes are able to change or drop the packets, it is necessary to protect this network against wormhole attack (S3 Table).

Table 1. Simulation Parameters.

Simulation Parameters	Value
Routing Protocol	GPSR
Number of Nodes	200
Transmission range	150 *m*
Malicious nodes	2–10
Packet Size(bytes)	512
Traffic Type	CBR
Paused time	50 sec
Movement Model	Random Way Point
Number of wormhole	1–5
Simulation area(m^2)	1000*1000

doi:10.1371/journal.pone.0115324.t001

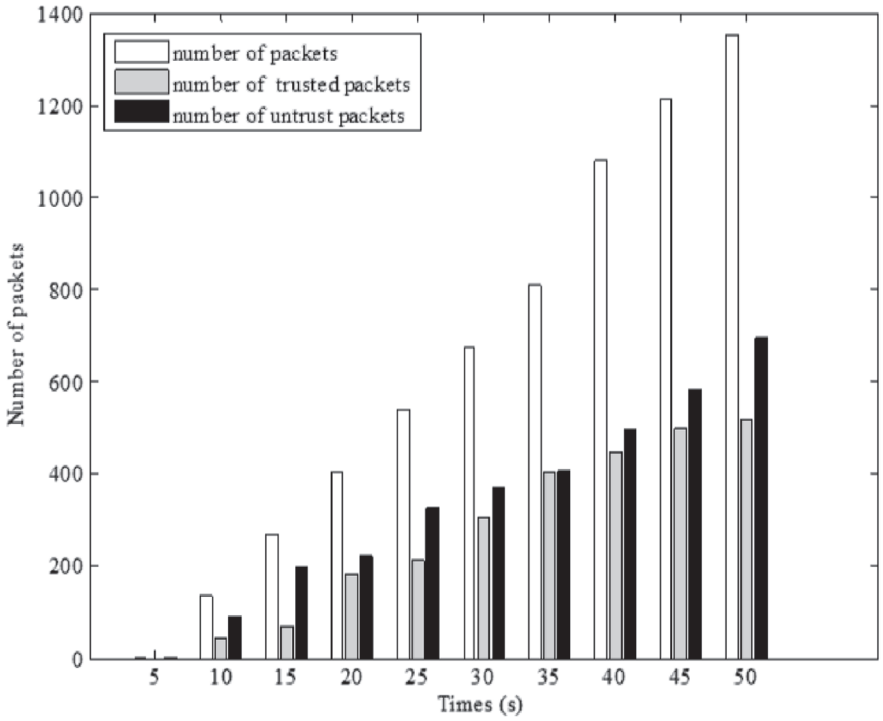

Figure 11. The effect of wormhole attack on geographic routing protocols.

doi:10.1371/journal.pone.0115324.g011

3.2.1 Wormhole detection rate

The wormhole detection rate is defined as the ratio of the number of detected wormhole over the total number of attacks by the adversaries in the network. Fig. 12 plots the wormhole detection rate versus the tunnel length. We randomly place one wormhole in the network in each run. It can be seen that our scheme (DWGRP) is able to detect all wormhole attacks (100%). However, the rate of wormhole detection in ANS method is approximately 80 percent. RRS method has the minimum rate of wormhole detection which is about 50 percent when the length of the tunnel reaches to 10. Generally, the performance of the DWGRP method to detect the wormhole attack is satisfactory and better than the other methods (S4 Table).

Then, we compare the rate of wormhole detection for our scheme (DWGRP) with WHOP [56] and WDI [57]. We simulate the WHOP and WDI methods on GPSR protocols to

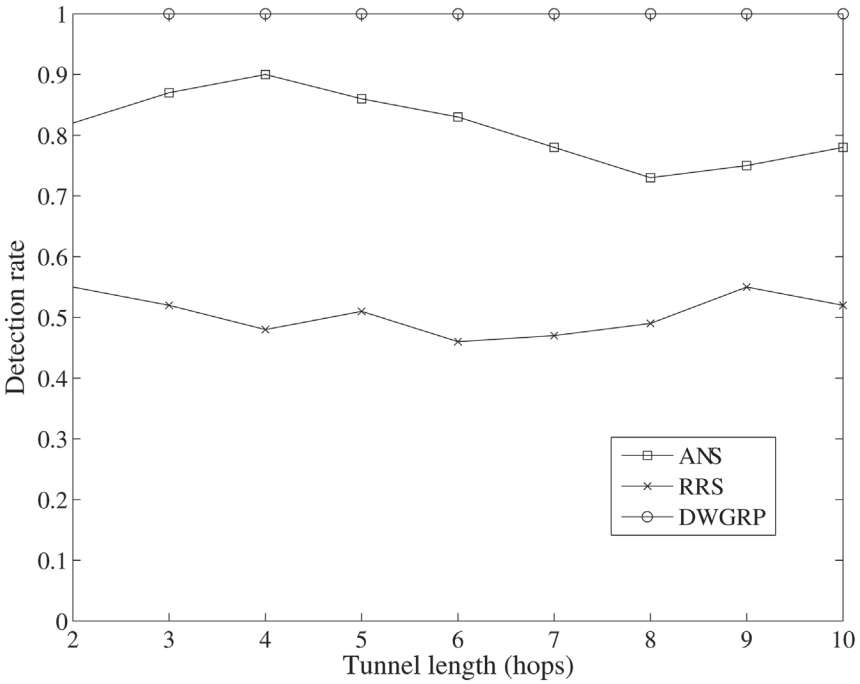

Figure 12. Wormhole detection rate against different tunnel length.

doi:10.1371/journal.pone.0115324.g012

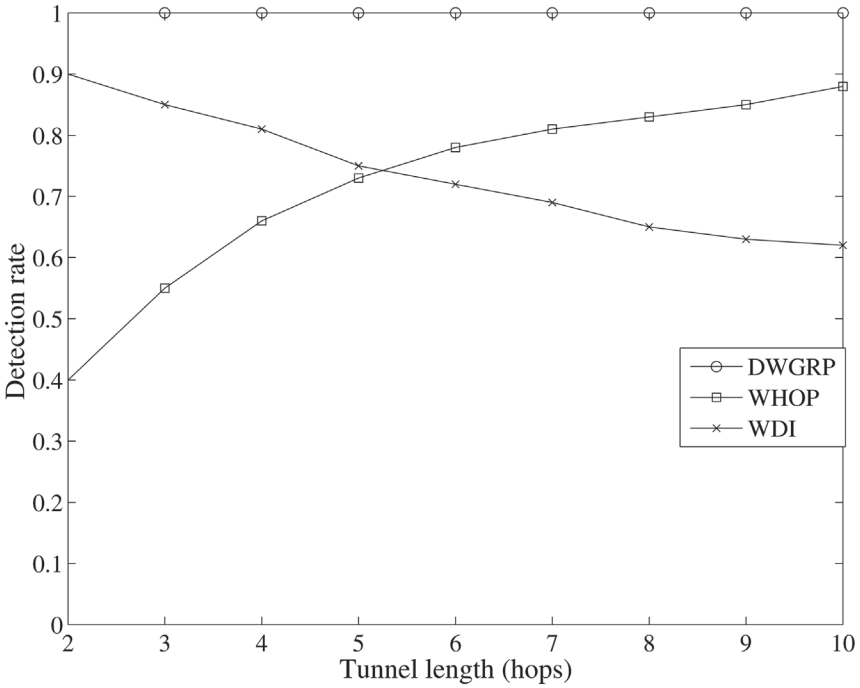

Figure 13. Wormhole detection rate versus tunnel length in WDI, WHOP and DWGRP.

doi:10.1371/journal.pone.0115324.g013

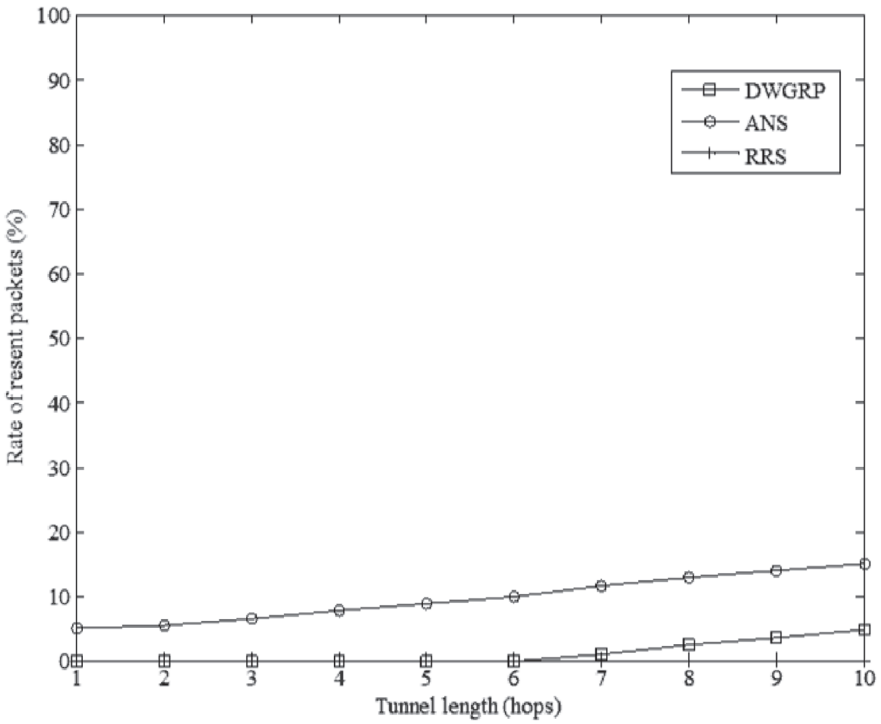

Figure 14. The rate of re-send packets against different tunnel length.

doi:10.1371/journal.pone.0115324.g014

compare their performance. As it is shown in Fig. 13, the wormhole detection rate in WDI method has a slightly downward trend in which by increasing the tunnel length, the detection rate decreases from 90% to 70%. In WHOP scheme, the detection rate rises up to nearly 85% when the number of hops approaches 10. Since the DWGRP scheme is able to detect 100% of wormhole attacks, the performance of our scheme is better than WHOP and WDI in geographic routing protocols (S5 Table).

3.2.2 Resend packet rate

If a wormhole attack is detected by the sink in our scheme, this packet will be eliminated and the packet will be re-sent. The ratio of the number of re-send packets over the total number of packets from source to destination is defined as the rate of re-send packets. Therefore, by increasing the rate of re-send packets, the rate of wasted energy is increased in the network. Fig. 14 shows the rate of re-send packets against different tunnel lengths for DWGRP, ANS and RRS. The rate of re-send packets in our scheme is zero when the tunnel length is less than 7. When the tunnel length reaches to 10, less than 5 percent of packets need to be re-sent in DWGRP because the attacker cannot break the link in the network. However, approximately 15 percent of packets which arrive to the sink will be re-sent in ANS method when the tunnel length is equal to 10. In the RRS scheme, the sink node cannot detect the wormhole attack and request re-sending packets. Therefore, this rate is zero for RRS (S6 Table).

4 Conclusion

Wormhole attack is recognized as a severe threat to wireless sensor networks and geographic routing protocols. Detection of wormhole attack is difficult because such attacks appear in various modes. In this paper we categorize the wormhole attacks based on their characteristics and

impact on different routing protocols. Then, we present a novel detection method of wormhole attacks in geographic routing protocols by improving the pairwise key pre-distribution scheme based on the beacon packets. Our scheme has the capability to detect the malicious nodes before receiving the message. The proposed scheme does not need any special hardware devices and additional assumptions, such as network synchronization, special guard nodes, or unit disk communication model. Simulation results and analytical modeling show that DWGRP approach achieves superior performance and applicability with the minimum restrictions compared with the related works in geographic routing protocols or wireless sensor networks. For the future work, we intend to improve this method by modifying the pairwise key pre-distribution scheme to detect all malicious nodes. We will also improve our method to prevent the Sybil attack.

Supporting Information

S1 Table. Probability of breaking in different scenarios.
(XLSX)

S2 Table. Probability of miss detection in different scenarios.
(XLSX)

S3 Table. The effect of wormhole attack on geographic routing protocols.
(XLSX)

S4 Table. Comparison of wormhole detection rate in ANS, RRS, and the proposed method based on length of tunnel.
(XLSX)

S5 Table. Comparison of wormhole detection rate in WDI, WHOP and the proposed method based on length of tunnel.
(XLSX)

S6 Table. Comparison of re-send packets in traditional and the proposed method based on length of tunnel.
(XLSX)

Acknowledgments

This work was carried out as part of the Mobile Cloud Computing research project funded by the Malaysian Ministry of Higher Education under the University of Malaya High Impact Research Grant, reference number UM.C/HIR/MOHE/FCSIT/03.

This work was partly supported by the National Natural Science Foundation of China under Grant no. 61300220 and NSFC project 61371098.

Author Contributions

Conceived and designed the experiments: AG MKK MS. Performed the experiments: MS XL XW. Analyzed the data: AS ME MS MKK. Contributed reagents/materials/analysis tools: AG AA. Wrote the paper: MS.

References

1. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 1: 293–315. doi: 10.1016/S1570-8705(03)00008-8

2. Giruka VC, Singhal M, Royalty J, Varanasi S (2008) Security in wireless sensor networks. Wireless communications and mobile computing 8: 1–24. doi: 10.1002/wcm.422
3. Al-Karaki JN, Kamal AE (2004) Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communications 11: 6–28. doi: 10.1109/MWC.2004.1368893
4. von Mulert J, Welch I, Seah WKG (2012) Security threats and solutions in MANETs: A case study using AODV and SAODV. Journal of Network and Computer Applications 35: 1249–1259. doi: 10.1016/j.jnca.2012.01.019
5. Eslaminejad M, Razak SA (2012) Fundamental lifetime mechanisms in routing protocols for wireless sensor networks: A survey and open issues. Sensors 12: 13508–13544. doi: 10.3390/s121013508 PMID: 23202008
6. Wang X, Guo W, Zhang W, Khan M, Alghathbar K (2013) Cryptanalysis and improvement on a parallel keyed hash function based on chaotic neural network. Telecommunication Systems 52: 515–524. doi: 10.1007/s11235-011-9457-9
7. Khan MK, Zhang J (2008) Multimodal face and fingerprint biometrics authentication on space-limited tokens. Neurocomputing 71: 3026–3031. doi: 10.1016/j.neucom.2007.12.017
8. Loo CE, Ng MY, Leckie C, Palaniswami M (2006) Intrusion detection for routing attacks in sensor networks. International Journal of Distributed Sensor Networks 2: 313–332. doi: 10.1080/15501320600692044
9. Xie M, Han S, Tian B, Parvin S (2011) Anomaly detection in wireless sensor networks: A survey. Journal of Network and Computer Applications 34: 1302–1325. doi: 10.1016/j.jnca.2011.03.004
10. Whaiduzzaman M, Sookhak M, Gani A, Buyya R (2014) A survey on vehicular cloud computing. Journal of Network and Computer Applications 40: 325–344. doi: 10.1016/j.jnca.2013.08.004
11. Sookhak M, Talebian H, Ahmed E, Gani A, Khan MK (2014) A review on remote data auditing in single cloud server: Taxonomy and open issues. Journal of Network and Computer Applications 43: 121–141. doi: 10.1016/j.jnca.2014.04.011
12. Akhunzada A, Sookhak M, Anuar NB, Gani A, Ahmed E, et al. (2014) Man-At-The-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions. Journal of Network and Computer Applications 2014.
13. Yih-Chun H, Perrig A, Johnson DB (2006) Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications 24: 370–380. doi: 10.1109/JSAC.2005.861394
14. Sookhak M, Karimi R, Ithnin N, Haghparast M, ISnin IF (2011) Secure Geographic Routing Protocols: Issues and Approaches. International Journal of Computer Science Issues(IJCSI) 8: 382–389.
15. Znaidi W, Minier M (2012) Key establishment and management for WSNs. Telecommunication Systems 50: 113–125. doi: 10.1007/s11235-010-9391-2
16. Zhang L, Zhang H, Conti M, Di Pietro R, Jajodia S, et al. (2013) Preserving privacy against external and internal threats in WSN data aggregation. Telecommunication Systems 52: 2163–2176. doi: 10.1007/s11235-011-9539-8
17. Wang W, Bhargava B, Lu Y, Wu X (2006) Defending against wormhole attacks in mobile ad hoc networks. Wireless communications and mobile computing 6: 483–503. doi: 10.1002/wcm.292
18. Hu L, Evans D (2004) Using Directional Antennas to Prevent Wormhole Attacks. In: The 11th Annual Network and Distributed System Security Symposium (NDSS). San Diego, California, p. 11.
19. Čapkun S, Buttyán L, Hubaux JP (2003). SECTOR: secure tracking of node encounters in multi-hop wireless networks.
20. Poovendran R, Lazos L (2007) A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks 13: 27–59. doi: 10.1007/s11276-006-3723-x
21. Maheshwari R, Jie G, Das SR (2007) Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In: 26th IEEE International Conference on Computer Communications. Anchorage, AK, pp. 107–115.
22. Khalil I, Bagchi S, Shroff NB (2007) LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks. Computer Networks 51: 3750–3772. doi: 10.1016/j.comnet.2007.04.001
23. Du W, Deng J, Han YS, Varshney PK, Katz J, et al. (2005) A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC) 8: 228–258. doi: 10.1145/1065545.1065548
24. Akkaya K, Younis M (2005) A survey on routing protocols for wireless sensor networks. Ad Hoc Networks 3: 325–349. doi: 10.1016/j.adhoc.2003.09.010
25. Eslaminejad M, Shukor AR, Sookhak M, Haghparast M (2011) A review of routing mechanisms in wireless sensor networks. International Journal of Computer Science and Telecommunications 2: 1–9.

26. Sohraby K, Minoli D, Znati T (2007) Wireless Sensor Networks: Technology, Protocols, and Applications. Wiley- Interscience.
27. Eslaminejad M, Shukor AR, Sookhak M (2012) Classification of energy-efficient routing protocols for wireless sensor networks. Ad-hoc & sensor wireless networks 17: 103–129.
28. Kim J, Wilhelm T (2008) What is a complex graph? Physica A: Statistical Mechanics and its Applications 387: 2637–2652. doi: 10.1016/j.physa.2008.01.015
29. Li S, Li L, Yang Y (2011) A local-world heterogeneous model of wireless sensor networks with node and link diversity. Physica A: Statistical Mechanics and its Applications 390: 1182–1191. doi: 10.1016/j.physa.2010.11.034
30. Barabási AL, Albert R, Jeong H (1999) Mean-field theory for scale-free random networks. Physica A: Statistical Mechanics and its Applications 272: 173–187. doi: 10.1016/S0378-4371(99)00291-5
31. Newman M (2010) Networks: An Introduction. Oxford University Press, Inc., 720 pp.
32. Gomez S, Diaz-Guilera A, Gomez-Gardenes J, Perez-Vicente CJ, Moreno Y, et al. (2013) Diffusion Dynamics on Multiplex Networks. Physical Review Letters 110: 5. doi: 10.1103/PhysRevLett.110.028701
33. Zhao D, Li L, Peng H, Luo Q, Yang Y (2014) Multiple routes transmitted epidemics on multiplex networks. Physics Letters A 378: 770–776. doi: 10.1016/j.physleta.2014.01.014
34. Barrat A, Barthelemy M, Vespignani A (2008) Dynamical processes on complex networks, volume 1. Cambridge University Press Cambridge.
35. Li G, Reis SDS, Moreira AA, Havlin S, Stanley HE, et al. (2010) Towards Design Principles for Optimal Transport Networks. Physical Review Letters 104: 18701. doi: 10.1103/PhysRevLett.104.018701
36. Parshani R, Buldyrev SV, Havlin S (2010) Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. Physical Review Letters 105: 48701. doi: 10.1103/PhysRevLett.105.048701
37. Su Z, Li L, Peng H, Kurths J, Xiao J, et al. (2014) Robustness of Interrelated Traffic Networks to Cascading Failures. Sci Rep 4. doi: 10.1038/srep05413
38. Xia Cy, Wang Z, Sanz J, Meloni S, Moreno Y (2013) Effects of delayed recovery and nonuniform transmission on the spreading of diseases in complex networks. Physica A: Statistical Mechanics and its Applications 392: 1577–1585. doi: 10.1016/j.physa.2012.11.043
39. Sanz J, Xia CY, Meloni S, Moreno Y (2014) Dynamics of Interacting Diseases. Physical Review X 4: 41005. doi: 10.1103/PhysRevX.4.041005
40. Sookhak M, Eslaminejad M, Haghparast M, Fauzi I (2011) Detection Wormhole in Wireless Ad-hoc Networks. International Journal of Computer Science and Telecommunications 2: 28–34.
41. Cayirci E, Rong C (2008) Security in wireless ad hoc and sensor networks. Wiley.
42. Kim Du, Kim Hw, Kim G, Kim S (2013) A Counterattack-Detection Scheme in Transmission Time-Based Wormhole Detection Methods. International Journal of Distributed Sensor Networks 2013: 6. doi: 10.1155/2013/184931
43. Jen SM, Laih CS, Kuo WC (2009) A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET. Sensors 9: 5022–5039. doi: 10.3390/s90605022 PMID: 22408566
44. Karlsson J, Dooley LS, Pulkkis G (2011) A new MANET wormhole detection algorithm based on traversal time and hop count analysis. Sensors 11: 11122–11140. doi: 10.3390/s111211122 PMID: 22247657
45. Hon Sun C, King-Shan L (2006) DelPHI: wormhole detection mechanism for ad hoc wireless networks. In: 1st International Symposium on Wireless Pervasive Computing. p. 6 pp.
46. Qazi S, Raad R, Mu Y, Susilo W (2013) Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications 36: 582–592. doi: 10.1016/j.jnca.2012.12.019
47. Lu X, Dong D, Liao X (2012) MDS-Based Wormhole Detection Using Local Topology in Wireless Sensor Networks. International Journal of Distributed Sensor Networks 2012: 9. doi: 10.1155/2012/145702
48. Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW (2005) Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. In: IEEE Conference on Wireless Communications and Networking. volume 2, pp. 1193–1199 Vol. 2.
49. Yifeng Z, Lamont L, Li L (2009) Wormhole attack detection based on distance verification and the Use of hypothesis testing for wireless ad hoc networks. In: IEEE Conference on Military Communications. Boston, MA, pp. 1–7.
50. Zhu S, Setia S, Jajodia S (2006) LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Trans Sen Netw 2: 500–528. doi: 10.1145/1218556.1218559

51. Xu Y, Chen G, Ford J, Makedon F (2007) Detecting Wormhole Attacks in Wireless Sensor Networks. In: Goetz E, Shenoi S, editors, Critical Infrastructure Protection, Springer US, volume 253, chapter 19. pp. 267–279. URL http://dx.doi.org/10.1007/978-0-387-75462-8_19.

52. Xia W, Wong J (2007) An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks. In: 31st Annual International Conference on Computer Software and Applications. Beijing, volume 1, pp. 39–48.

53. Qian L, Song N, Li X (2007) Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. Journal of Network and Computer Applications 30: 308–330. doi: 10.1016/j.jnca.2005.07.003

54. Poornima E, Bindhu C (2010) Prevention of WormholeAttacks in Geographic Routing Protocol. International Journal of Computer Network and Security (IJCNS): 42–50.

55. Sookhak M, Haghparast M, Gani A (2012) Anomaly detection in geographic routing protocols. In: International Conference on Education and e-Learning Innovations (ICEELI),. Sousse: IEEE, pp. 1–6.

56. Gupta S, Kar S, Dharmaraja S (2011) WHOP: Wormhole attack detection protocol using hound packet. In: Innovations in Information Technology (IIT), 2011 International Conference on. pp. 226–231.

57. Yun W, Zhongke Z, Jie W (2010) A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information. In: Fifth International Conference on Networking, Architecture and Storage (NAS). Macau: IEEE, pp. 63–72. PMID: 20799070