Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 8354930, 13 pages
http://dx.doi.org/10.1155/2016/8354930

Research Article

WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks

Rupinder Singh, Jatinder Singh, and Ravinder Singh

I.K.G. Punjab Technical University, Kapurthala, Punjab, India

Correspondence should be addressed to Rupinder Singh; rupi_singh76@yahoo.com

Received 30 August 2016; Revised 23 October 2016; Accepted 2 November 2016

Academic Editor: Abdallah Makhoul

Wormhole attack is a challenging security threat to wireless sensor networks which results in disrupting most of the routing protocols as this attack can be triggered in different modes. In this paper, WRHT, a wormhole resistant hybrid technique, is proposed, which can detect the presence of wormhole attack in a more optimistic manner than earlier techniques. WRHT is based on the concept of watchdog and Delphi schemes and ensures that the wormhole will not be left untreated in the sensor network. WRHT makes use of the dual wormhole detection mechanism of calculating probability factor time delay probability and packet loss probability of the established path in order to find the value of wormhole presence probability. The nodes in the path are given different ranking and subsequently colors according to their behavior. The most striking feature of WRHT consists of its capacity to defend against almost all categories of wormhole attacks without depending on any required additional hardware such as global positioning system, timing information or synchronized clocks, and traditional cryptographic schemes demanding high computational needs. The experimental results clearly indicate that the proposed technique has significant improvement over the existing wormhole attack detection techniques.

1. Introduction

Wireless sensor networks (WSNs) are infrastructure-less and self-configured wireless networks to monitor the environment or physical conditions, such as temperature, sound, and humidity, and to cooperatively pass their data gathered through the network to a central location or sink (base station) so that the data can be analyzed for further processing. WSN is deployed in the environments that are usually unfriendly and unsafe. WSN has a large number of constraints which result in new challenges. The sensor nodes have unreliable communication medium and extreme resource limitations which make it very difficult to deploy security mechanism. Most of the protocols for WSNs in the past assumed that all nodes are trustworthy and cooperative. But this is not the case for many sensor network applications today and a variety of attacks are possible in WSN including wormhole.

Wormhole attack is a severe security threat to WSNs. Wormhole attack in WSNs is one of the main attacks in which a malicious node entraps the packets from a single position in the network so that they can be tunneled to another malicious node at a far off point. In a wormhole attack, since attackers are directly connected with each other, they can, therefore, communicate at a fast speed in comparison to the other nodes in the WSN. However, for the implementation of such communication, there is a need for support of special hardware. For the tunnel distances that are more than the single-hop normal wireless transmission range, it is easier for the attacker to compose packets in the tunnel as compared to a regular multihop route. This is done due to the use of a single long-range directional wireless link or direct wired link. It is also achievable for an attacker in the wormhole attack to move forward every bit directly without waiting for receiving of the complete packet. Wireless transmission nature also makes it possible for the attacker to construct a wormhole for packets that are not addressed to it; this is possible as an attacker can overhear these packets in wireless communication and tunnel them in order to collude attacker at the other end of the wormhole.

For the setting of wormhole attack in WSN, attackers construct a wormhole tunnel that makes a direct link

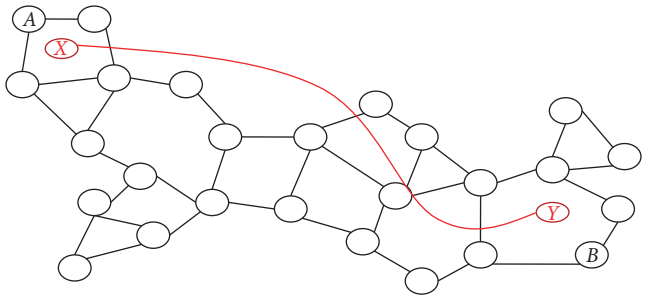

Figure 1: Wormhole tunnel constructed between nodes X and Y.

between two malicious nodes located at far off locations. Attackers make use of either a high-quality wireless out-of-band link or a wired link for the construction of wormhole tunnels. The tunnel constructed is used by malicious nodes for making Denial of Service (DoS) attack. It can also be used for traffic analysis or for dropping data or controlling packets. Wormhole attack can be made in the WSN, without compromising any sensor node or the authenticity and the integrity of the communication. Cryptographic methods are used for defending the network communications, but they fail for the detection of wormhole attacks as the success of the wormhole attack is independent of the cryptographic mechanism. Moreover, a wormhole attack is difficult to detect as it utilizes a limited amount of resources for the attack.

Attackers can establish the wormhole attack in WSNs without disclosing their identities. Most of the routing protocols like AODV (Ad hoc On-demand Distance Vector) and DSR (Dynamic Source Routing) are vulnerable against this attack. In wormhole attack, since attackers are directly connected to each other through tunnel, they can communicate at a fast rate as compared to other nodes in the sensor network. However, there may be need of special hardware to support such kind of communication. Figure 1 shows the tunnel constructed by malicious nodes under wormhole attack. Assume that sensor nodes A and B are not neighbors of each other. An attacker with tunnel is able to transmit packets at X and Y nodes, the two nodes that it controls. By transmitting packets from sensor node X to node Y, the attacker can make node A and node B believe that they are neighbors of each other and vice versa. The attacker can replay packets received by sensor node X at node Y and vice versa; it would otherwise take a number of hops for travelling a packet from a location near X to a location near Y. Packets that are transmitted near sensor node X travelling through the wormhole will arrive at node Y even before travelling of the packets through multiple hops to the network. The attacker can make the sensor nodes A and B believe that they are neighbors of each other, with the help of routing messages, and then can selectively drop out data messages in order to disrupt communications between sensor nodes A and B.

Many countermeasures for exposure of wormhole have been proposed in WSNs. Those solutions diagnose the partial symptoms induced by wormholes for their detection. Most of the detection methods either make use of a dedicated hardware device such as global positioning systems, antennas with specific directions, and particular radio transceiver modules or make very strong assumptions regarding sensor networks such as large-scale clock synchronization, unique guard nodes, attack-free environments, and communication models with unit disk. These special needs and suppositions restrict their applicability to the networks that are made of a huge number of small cost resources constrained nodes. In order to completely tackle wormhole attacks in WSNs, we have to reply to the following questions. (1) The most necessary characteristics of wormhole attack are caused by which symptoms feature? (2) How can one propose the countermeasures without using significant needs or supposition? Our goal in this research work relies exclusively on connectivity information of sensor network in order to detect and isolate the wormholes. We focus our research study on elementary view on the packet loss and delay in multihop wireless sensor network topologies, targeting catching the packet loss and delay at hop level and for the complete route.

In this paper, we propose a hybrid wormhole detection technique WRHT (wormhole resistant hybrid technique) that is based on the concept of watchdog [1] and Delphi [2]. We first calculate delay probability per hop and for the complete route caused by the wormhole in the selected route. In the next phase, WRHT finds the packet drop probability for each hop and the complete route in the sensor network. We also calculate the wormhole presence probability (WPP_P) for a path. The remainder of the paper is ordered as follows. We initially discuss present relevant countermeasures against wormhole attack in Section 2. In Section 3, the proposed WRHT is discussed. The simulation results are provided in Section 4, while performance evaluation is given in Section 5. Finally, we end with a conclusion and future work in Section 6.

2. Related Works and Problem Formulation

2.1. Related Works. In this section of the paper, we review related works in the literature for dealing with wormhole attack. A detailed study of these proposed solutions will help in the formulation of the problem and its possible solution.

Cho et al. [3] in their paper discuss vulnerabilities that the technique of watchdog and trust mechanisms has and finally they propose protective approaches that can remove weaknesses of the trust mechanism and the watchdog technique. Dias et al. [4] provide a cooperative watchdog system for detecting and acting against misbehaving nodes and sequentially reducing their impact on performance in the overall network. Its operation depends on a cooperative exchange of nodes character along the network. Dromard et al. [5] make the assumption that the attacked nodes drop both the acknowledgement and forwarded packets with different frequencies. The authors offered an extension to the watchdog scheme in order to detect misbehaving nodes in WMNs while considering packets loss over the links. The proposed scheme matches the sharing of a node acknowledgment to its distribution of the forwarded packets of data in order to detect misbehaving nodes. Hernández-Orallo et al. [6] proposed CoCoWa (Collaborative Contact-based Watchdog), a collaborative technique based on the dispersal of local

self-centered nodes wakefulness in the case when a contact occurs. This is done so that the information about self-interested nodes can be rapidly propagated. Hernández-Orallo et al. [7] proposed a collaborative based watchdog that is based on the contact spreading of detected self-centered nodes. The authors also bring in an analytical model in order to evaluate the discovery time and cost of the collaborative scheme.

Existing countermeasures against wormhole attack mostly depend on the observation of symptoms that are created by wormholes existing in the WSNs. All of the existing techniques have their own individual advantages and limitations. Applicability of a particular approach mostly depends on the specific network configurations and their applications. Hu et al. [8] presented the geographic packet leash. Making use of appending location information about sending nodes in every packet, they check whether hop-by-hop transmission in the network is physically possible or not and consequently detect the presence of wormholes. Wang et al. [9] in their work verify the end-to-end distance limits between the source node and the destination node. Zhang et al. [10] in their work proposed a neighborhood scheme based on location for authentication in order to find the wormholes. These approaches make use of the preknowledge of the node locations so as to find the difference in the distance.

Some of the approaches for wormhole detection watch the symptom of time difference during packet forwarding. Hu et al. [8] introduced the temporal packet leash concept, which assumes the presence of fixed global clock synchronization. This detects the presence of wormholes from the exceptions in the packet transmission latency. Čapkun et al. [11] proposed the SECTOR concept, which calculates round trip travel time (RTT) for the packet delivery so as to detect presence of unusual wormhole channels. SECTOR removes the use of the clock synchronization; however, it assumes the presence of particular hardware that is prepared by each of nodes, enabling rapid sending of one-bit challenge messages without the involvement of the CPU in the network. Eriksson et al. [12] proposed one more RTT based technique called the TrueLink.

Some of the approaches for wormhole detection watch the symptom of mismatch neighborhood leading to the physical infeasibility in the network. Hu and Evans [13] make use of directional antennas in order to find communicating links that are infeasible in the network by making use of directionality of communication via antenna. Khalil et al. [14] proposed the scheme LiteWorp; it assumes the presence of attack-free situation before the launch of wormhole attack. During phase of deployment, each node in the network gathers its 2 hop neighbors and LiteWorp followed by selecting the guard nodes for detection of wormhole channels. This is done by overhearing transmissions that are infeasible among the nonneighboring nodes. They also proposed a complement to LiteWorp called MobiWorp [15], making use of the assistance of some location aware mobile node.

Some of the approaches for wormhole countermeasure study the symptom of mismatch graph. These approaches make use of particular assumptions of the network graph models used in the network. Poovendran and Lazos [16] presented a framework to deal with wormholes based on the graph. The approach makes assumptions regarding the existence of safeguarding nodes having a communication range that is extraordinary. Wang and Bhargava [17] suggested finding the presence of wormholes graphically. The design of the network is reconstructed by MDS (multidimensional scaling) so as to find the wrap that is introduced by the malicious nodes wormholes. Authors in [18] make use of illegal packing numbers in UDG (unit disk graph). They provided a completely localized technique so as to detect malicious nodes wormholes with the use of only connectivity in the network. This approach may fall short when UDG model is not followed by connectivity graphs or an increase of packing number is not caused by the wormhole. Some approaches make use of mismatch in the traffic flow symptom based on the analysis of statistic on the traffic in the network. Song et al. [19] in their work monitor the truth that wormhole links are chosen for high-frequency routing, and, by matching this with regular statistics, wormhole links can be identified. Buttyán et al. [20] propose another statistical approach that captures the abnormal increase in the number of neighbors and the decline in smallest path lengths because of wormholes. The BS (base station) of the network centrally finds the presence of wormholes by making use of hypothesis testing, which is further based on prestatistics of usual networks.

The protocol in [21] is based on the randomized neighbor discovery idea and it executes randomly neighbor discover process. However, the performance of this was not explained in a network with a single hop. This work requires the advance knowledge of a number of neighbors. Angelosante et al. [22] proposed a new algorithm for neighbor discovery. It makes use of the concept of multiuser detection approach. But, in order to use this algorithm, there should be synchronization between nodes and, furthermore, each node needs the signature of other nodes in the network. Keally et al. [23] proposed the watchdog, which is a modality agnostic based framework for event detection. The framework combines the sensors in order to meet up the user's specific detection correctness during run-time. It also considerably reduces right energy usage. Kim et al. [24] proposed a safe method for the wireless network coding. This scheme is called the algebraic watchdog. In this approach, the technique enables network nodes to find the malicious behaviors probabilistically. It uses the overheard messages in order to police downstream neighbors locally. The algebraic watchdog provides a protected global network that is self-checking.

Liu et al. [25] propose a scheme with observer prototype and finite state machine for the implementation of watchdog. According to the authors, by making use of observer prototype along with finite state machine, the watchdog will automatically notify when the state of the program changes. Maheshwari et al. [26] proposed a novel algorithm for wormhole detection using only connectivity information for detecting forbidden substructures in connectivity graph. Zhang et al. [27] discuss a distance vector based robust localization scheme which can be used in WSNs to fight against wormhole attacks. The proposed technique does not use extra hardware or too much computational cost. Khabbazian et al. [28] proposes a timing based countermeasure to defend

against the wormhole attack. The technique avoids the limitations of existing timing based solutions, no synchronized clocks are needed by the nodes, and they did not require guessing the sending time or being capable of quick switching among the receive and send nodes. Singh et al. [29] propose a cross-layer based intrusion detection method for wireless networks. In this work, a united weight value is calculated from Received Signal Strength (RSS) and time consumed for RTS-CTS handshake between the sender and receiver.

Ji et al. [30] proposed a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, DAWN, a distributed detection algorithm against wormhole in wireless network coding systems, is proposed by exploring the change of the flow directions of the innovative packets caused by wormholes. Ji et al. [30] rigorously prove that DAWN guarantees a good lower bound of successful detection rate. Tsitsiroudi et al. [31] proposed a tool, called EyeSim, which is a human-interactive visual-based anomaly detection system that is capable of monitoring and promptly alerting to the presence of wormhole links. In addition, it is capable of indicating the malicious nodes that form the wormhole link. EyeSim may expose adversaries by conducting cognitive network data analysis based on dynamic routing information. The efficacy of EyeSim is assessed in terms of detection accuracy. Biswas et al. [32] have proposed a novel wormhole attack detection technique in which node authentication has been used to detect malicious nodes and remove the false positive problem that may arise in wormhole detection techniques. Node authentication not only removes false positive but also helps in the mapping exact location of the wormhole and is a kind of double verification for wormhole attack detection. Patel and Aggarwal [33] projected two-phase detection method for wormhole attack in dynamic sensor networks. This method has a better accuracy rate than most of the existing techniques.

2.2. Problem Formulation. Before the formulation of the problem, we first discuss the concept of watchdog and Delphi. Every intrusion detection technique for wormhole has its own advantages and limitations. The proposed technique is a hybrid technique based on watchdog and Delphi techniques. The proposed work is derived from the limitations of these techniques. The concept and the limitations of watchdog and Delphi are discussed below.

2.2.1. Watchdog Technique and Its Limitations. The watchdog intrusion detection technique detects the presence of a malicious node in the network. In this scheme, source node forwards the message to destination node through a middle node; this node after receiving a packet from source forwards it to the destination. Figure 2 shows the working of watchdog technique in which node A will plan to send one of the packets to node C. Node A can eavesdrop sent traffic of node B in order to determine whether node B in the network will send the packet to C or not. If node B does not forward the packet to node C after a threshold, then watchdog technique declares that node B is malicious. As a result, a new route from node A in the network to node C is discovered in order

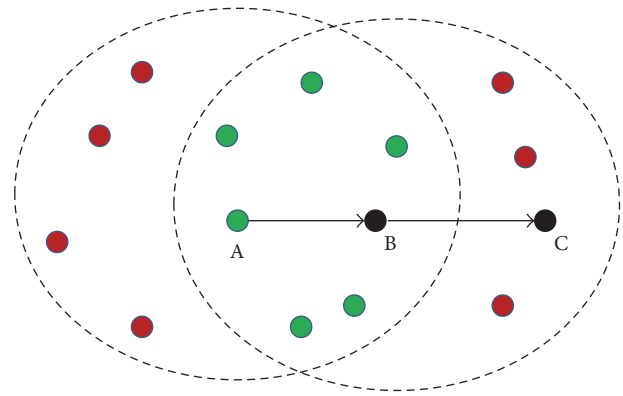

Figure 2: Watchdog technique.

to isolate the malicious node B. Let α be the set of nodes in the network that can listen to messages sent from node A to node B and let β be the set of nodes that can hear the messages sent from node B to node C. The set of possible watchdogs of node B can be defined as an intersection of α and β. Any node that lies in the intersection of above regions is able to hear messages from both. These nodes are able to decide whether or not node B forwards messages or not.

Cho et al. [3] discussed the below given limitations of watchdog technique for the intrusion detection of misbehaving node. Each of the cases discussed below makes use of following path sequence:

$$S \rightarrow A \rightarrow B \rightarrow C \rightarrow BS.$$

(1) Uncertain Collision. Let us consider a state in which node A forwards one fake packet to node B. Node A starts to listen in whether node B will send the packet to node C. When node B sends packets to C, node A might not be able to listen in this transmission in case some other neighborhood node (say S) at the same time sends packets to node A. This uncertain collision may result in misleading node A to assume that node B is malicious.

(2) The Collision of Receiver. Collision is also possible on the other side of the receiver. Receiver node C may not receive the packet correctly because of this collision. Node A can only listen to node B whose packets are sent for forwarding. Node A has no idea whether the packet is received by node C or not. In such type of situation, a malicious node in network B can purposely skip the retransmissions of packets or malicious node in network C can result in generating collision for the reason to avoid the receiving of packets and forcing node B into the retransmitting.

(3) Power Transmission Limitation. If node B adjusts the signal transmission power in such a way that node A can listen in but node C in the network cannot receive, node B may drop the packets in order to increase the honesty (to node A). In the routings of geographic systems, where each node has idea about the location of itself and the neighbors, node B can with

no trouble launch this type of attack by choosing a destination node C in the network from its list in such a way that distance (B, C) > distance (B, A), where distance (i, j) is the distance between nodes i and j.

(4) Detection of Fake Misbehavior. This happens in the situation when a mean node purposely reports about the misbehavior of other nodes. Consider the example in which node A might report that node B is reducing packets, although node B is not doing so. Then, node A's neighbor nodes (such as S) cannot openly communicate with node B (and therefore monitor) which will judge that node B is malicious.

(5) Collusion. In the network multiple-colluding, attackers are able to launch more complicated attacks. Consider two malicious colluding nodes A and B. These nodes can entirely deceive node S if node A sends all the packets from node S to B but node B crashes all packets. Since node S cannot listen in node B misbehavior, node S will not judge nodes A and B to be malicious.

(6) Packets Partial Dropping. Instead of dropping each of the packets, node B may drop limited packets in such a way that the total failure rate will not go beyond the threshold of node A watchdog. This is very much similar to the gray hole attack.

2.2.2. Delphi Technique and Its Limitations. Delay per hop indication (Delphi) detection mechanism is a solution to the wormhole attack. In this intrusion detection mechanism, in every path, delay per hop is determined. It is proven that wormhole path is usually longer than delay per hop for actual path in the wireless sensor network. It is assumed that the path is having wormhole attack, if the path in the network has markedly high delay per hop. In order to detect wormhole attack, the delays of various paths to the receiver are used as an observation. Delphi mechanism works by checking presence of any malicious node in the path from the sender to the receiver trying for the launch of wormhole attack. In order to identify the malicious node which is trying to trigger wormhole attack, the hop count and delay information about paths between sender and receiver will be utilized. Delphi technique can be used for the detection of both hidden and exposed attacks. The Delphi detection technique is based on the distinguishable difference of the DPH (delay per hop) values between the normal paths and the tunneled paths. The main limitation of the Delphi technique is that it does not work well in the case when all or most of the paths in the sensor network are tunneled due to wormhole attack.

The above limitations of watchdog and Delphi techniques indicate that none of the two are purely reliable for the detection of wormhole attacks in WSNs. Therefore, these limitations motivated us to propose a hybrid intrusion detection technique, WRHT, for detection of wormhole attack in sensor networks. The technique makes use of the advantages of both techniques so that the wormhole attack is not left untreated during the detection process. WRHT is discussed in detail in the next section of the paper.

3. Wormhole Resistant Hybrid Technique (WRHT)

The proposed technique, WRHT, is a hybrid technique based on the concept of watchdog and Delphi. Watchdog (packet drop) and RTT based technique Delphi are based on the assumption that the packet drop and RTT of a route in the network are very closely related to the value of its HC (hop count) and distance. In practical WSN environments, there exist probability that a normal route without wormhole with a small distance and short value of HC may produce a high value of RTT and packet drop value due to traffic congestion and other reasons. Conversely, a route in the sensor network that is infected with wormhole with a lengthy distance may result in providing a low value of RTT. This may be due to the small packet processing delays by all in-between nodes. Furthermore, there may be less packet drop by an attacker to force AODV to follow the wormhole affected path. For these reasons, sometimes wormhole exposure performance is compromised when separately watchdog and Delphi are used in realistic WSN environments.

WRHT makes use of the information about the packet drop and the delay per each hop and for the complete route in the sensor network. The foundation behind WRHT is to build up a wormhole detection methodology that is able to manage every category of wormholes and is possible for every type of WSN device and scenarios of the network, without the earning of significant computational costs. WHRT is considered as an extension to AODV protocol. The proposed WRHT allows the source node in the sensor network to calculate the wormhole presence probability (WPP_P) for a path in addition to HC information.

During the AODV route discovery phase, per hop time delay probability (TDP_H) is calculated in order to discover the presence of wormhole in the path. This information can be further used for the calculation of time delay probability for the complete path, that is, TDP_P. In the next phase of the WRHT, per hop packet loss probability (PLP_H) is calculated. This is further used for the calculation of packet loss probability for the complete path, that is, PLP_P. The values of TDP_P and PLP_P are used for making the decision whether a path P contains a wormhole or not. This will help the AODV to take a secure path for the transmission. The complete working of the proposed WRHT is given in Figures 3 and 4.

The sender at time t_s initiates process of detection broadcast of the RREQ (route request) packet and at time t_i it receives RREP (route reply) packet from its neighboring node. Assume that round trip time (RTT) of a path in the sensor network through node i is specified by $\mathrm{RTT}_i = t_i - t_s$; then delay/hop value (DPH) of the path to the receiver via node i is given by $\mathrm{DPH}_i = (\mathrm{RTT}_i)/2h_i = (t_i - t_s)/2h_i$. Here, h_i is the hop count field in the RREP of node i. Per hop time delay probability (TDP_H) is the probability of time delay caused at each hop in the established path from the source to the destination. The difference between the times when the packet was forwarded by hop to the time when the packet was received is used for the calculation of TDP_H. Total time delay probability per hop is calculated by adding value during the

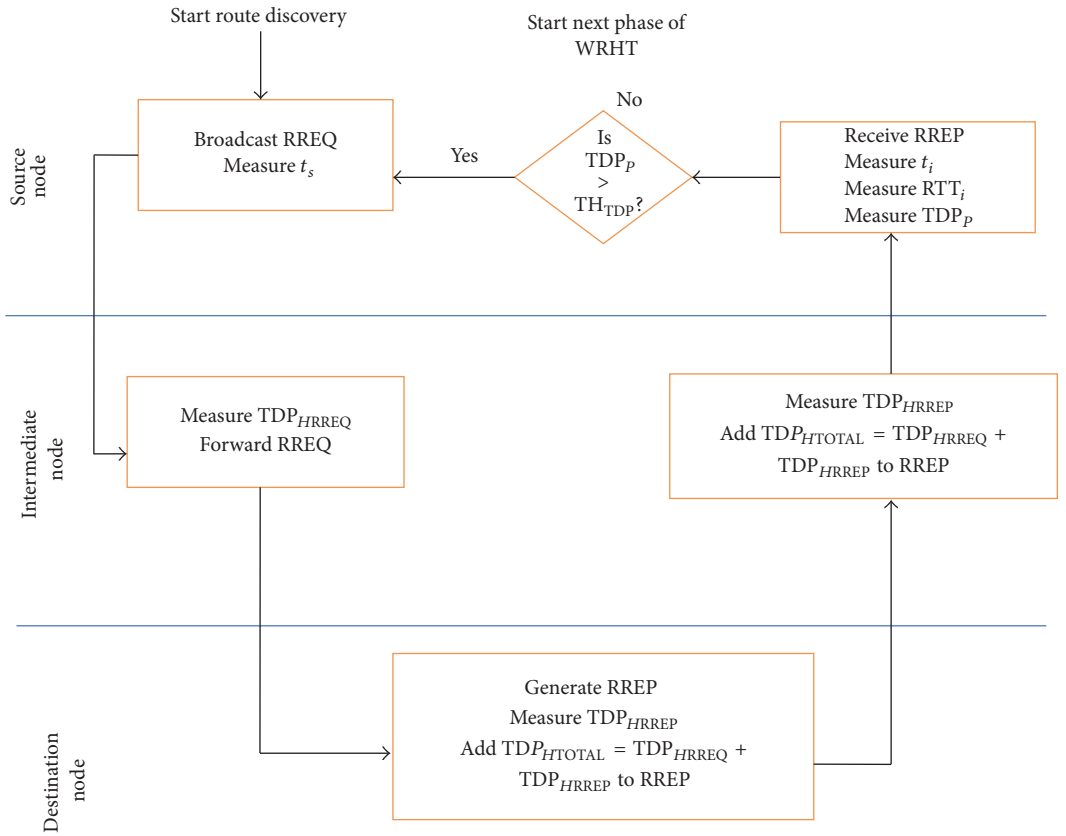

Figure 3: Route discovery process of WRHT.

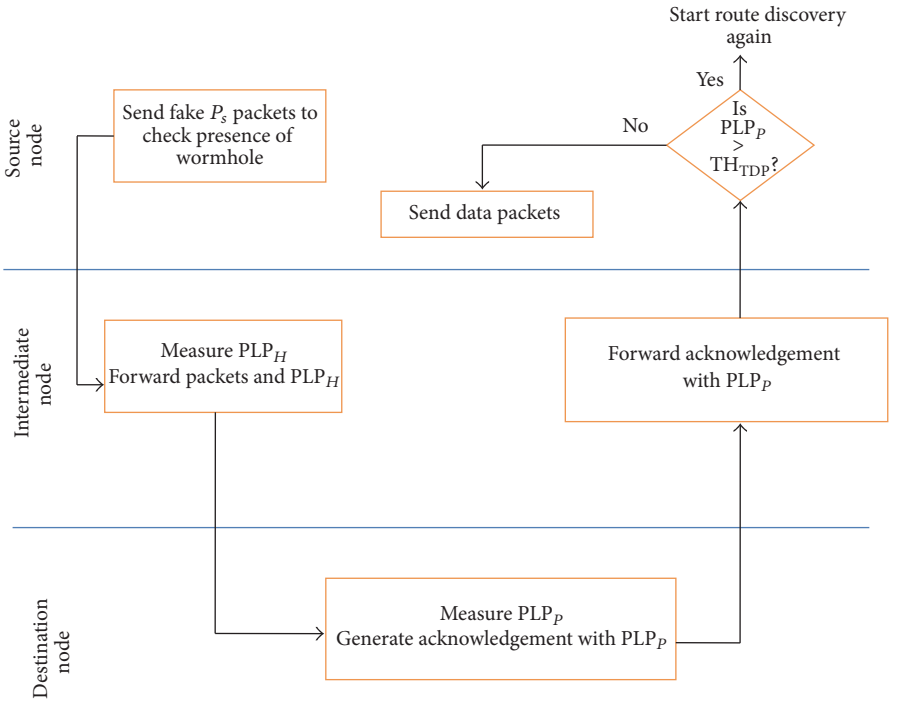

Figure 4: Wormhole detection process of WRHT.

broadcast of RREQ and RREP; mathematically it is defined as

$$\mathrm{TDP}_{H\mathrm{TOTAL}} = \mathrm{TDP}_{H\mathrm{RREQ}} + \mathrm{TDP}_{H\mathrm{RREP}}, \quad (1)$$

where $\mathrm{TDP}_{H\mathrm{RREQ}}$ is the time delay probability of a node during RREQ and $\mathrm{TDP}_{H\mathrm{RREP}}$ is the time delay probability of a node during RREP.

The time delay probability of the complete path (TDP_P) is calculated as the product of time delay probabilities of individual sensor nodes in the path. Consider a sensor network having n sensor nodes in the path to the receiver. Then, mathematically, TDP_P is defined as

$$\left(\mathrm{TDP}_P\right) = 1 - \left(\prod_{j=1}^{n}\left(1 - \mathrm{TDP}_j\right)\right), \quad (2)$$

where TDP_j is the time delay probability measured at node j.

If the value of TDP_P is less than a predefined threshold ($\mathrm{TH}_{\mathrm{TDP}}$), then the route discovery process is over and the next phase of WRHT starts; otherwise the routing protocol looks for a new route to the destination. The process is shown in Figure 3.

Next, in the working of WRHT, the sender sends Ps fake packets to the constructed route to check the possibility of wormholes and the destination node receives those packets. The destination node sends back the acknowledgement of the number of the packets received, that is, PR. The source node calculates the packet loss per path (PLP) through node i by $\mathrm{PLP}_i = P_s - P_r$. The per hop packet loss probability (PLP_H) is calculated by finding the number of dropped packets at hop H to the number of packets received by hop H. Mathematically, it is calculated as

$$1 - \mathrm{PLP}_H. \quad (3)$$

The packet loss probability of the complete path (PLP_P) is calculated as the probability product of individual sensor nodes in the path. Mathematically, it is defined as

$$\left(\mathrm{PLP}_P\right) = 1 - \left(\prod_{j=1}^{n}\left(1 - \mathrm{PLP}_j\right)\right), \quad (4)$$

where PLP_j is the packet loss probability measured at node j.

The complete process of calculating PLP_P is shown in Figure 4. If the value of PLP_P is less than a predefined threshold ($\mathrm{TH}_{\mathrm{PLP}}$), then the route is free from the wormhole and is safe for the data transmission; otherwise a new path is to be discovered again by broadcasting the RREQ. After calculating the values of TDP_P and PLP_P, we create a decision table in order to decide whether the current path is under a wormhole attack or not. The decision table is given in Table 1. We use the following symbols in order to define the entries of the table.

Let $\delta_{\min}$ be the time delay probability for a path less than $\mathrm{TH}_{\mathrm{TDP}}$, let $\delta_{\max}$ be the time delay probability for a path more than $\mathrm{TH}_{\mathrm{TDP}}$, let $\lambda_{\min}$ be the packet loss probability for a path less than $\mathrm{TH}_{\mathrm{PLP}}$, and let $\lambda_{\max}$ be the packet loss probability for a path more than $\mathrm{TH}_{\mathrm{PLP}}$.

Table 1: Decision table for detecting wormhole attack.

TDP_P	PLP_P	Node status	Node ranking
$\delta_{\min}$	$\lambda_{\min}$	No wormhole attack	1
$\delta_{\min}$	$\lambda_{\max}$	Suspected to be under wormhole attack	2
$\delta_{\max}$	$\lambda_{\min}$	Suspected to be under wormhole attack	2
$\delta_{\max}$	$\lambda_{\max}$	Malicious (under wormhole attack)	3

The nodes in the path are ranked according to their corresponding values as given in Table 1. A node with value 1 has no wormhole attack and a node with value 3 is under wormhole attack. A node with value 2 is suspected to be under wormhole attack, so that it cannot be used for forming a path to the destination.

Since the two events time delay and packet loss are not mutually exclusive (as there may be loss of packets and time delay at the same time), the wormhole presence probability (WPP_P) for a path can be defined as

$$\mathrm{WPP}_P = \left\{\mathrm{TDP}_P + \mathrm{PLP}_P - \left(\mathrm{TDP}_P, \mathrm{PLP}_P\right)\right\}. \quad (5)$$

WPP_P values of the normal paths having no wormhole tunnel usually appear to be small when matching up with those of the tunneled paths. Observations also show that TDP_H values of the normal and the tunneled paths formulate two different groups, one for normal paths and another for tunneled paths. Let α and β be the set of TDP_H values for normal and tunneled groups, respectively. Let $\alpha_{\max}$ and $\beta_{\min}$ be the maximum and minimum values in their groups. Also, let λ_{gap} be the maximum difference between any two values of α or β. Then, mathematically, we can write

$$\alpha_{\max} - \beta_{\min} > \lambda_{\mathrm{gap}}. \quad (6)$$

Let $\mathrm{TDP}_{Hn}, \mathrm{TDP}_{Hn-1}, \ldots, \mathrm{TDP}_{H1}$ be the descending order values of TDP_H. If TDP_{Hi} is larger than TDP_{Hi+1} by a threshold (T_v), then the path through sensor node i is under wormhole attack. Furthermore, all other paths having TDP_H values greater than TDP_{Hi} are also under wormhole attack.

4. Simulation-Based Implementation

The performance of WRHT was thoroughly tested in a wireless sensor network simulation environment developed in NS2, with the simulation parameters used being defined in Table 2.

We firstly deploy WSNs nodes by defining the network source node and destination nodes. As shown in Figure 5, source node 0 will flood packets of route request in the network to find the path to destination node 10. The adjacent nodes of the destination node will respond back to the source node with the route reply packets. The source node selects the best path from the source to the destination on the basis of the sequence number and hop count. It is assumed in the simulation that all the sensor nodes have identical hardware of IEEE 802.11b. These sensor nodes with the exception of

Table 2: Simulation parameters.

Parameter	Value
Simulator used	NS-2.3
Area (meter)	800 × 800
Number of nodes	50 to 500
Routing protocol	AODV
Channel type	Wireless
Packet size	8196 bytes
Mobility model	Two-ray ground propagation model

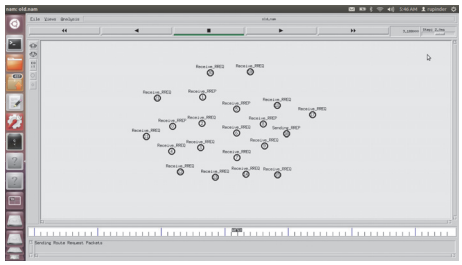

Figure 5: Sensor network during route discovery.

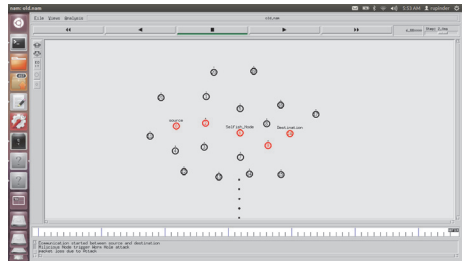

Figure 6: Detection of selfish node (i.e., wormhole).

Figure 7: Monitor mode processing.

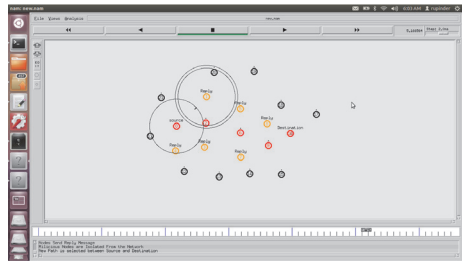

Figure 8: Wormhole node not sending RREP.

wormhole node are arbitrarily dispersed within the network area.

Figure 6 provides a scenario of the sensor network having selfish node (i.e., wormhole node) in the network. Node 6 in Figure 6 is the selfish node. In Figure 6, the established path from source node 0 to destination node 10 is represented with red color.

The algorithm for the WRHT works as the source waits for the destination to send an acknowledgement to it after every 10th packet. If source receives the acknowledgement, then there is no misbehavior in the WSN and the process continues as normal. But if the destination fails to acknowledge the data packets for a time period, then detection methodology starts its functionality. The established path will be tested to detect and isolate the presence of malicious nodes (if any) from the WSN. Here, we first apply the approach of the Delphi technique to locate any possible wormhole node during the process of route discovery. If a malicious node is detected, it will be the node for further processing in Table 1. But if Delphi fails to detect wormhole node (due to the presence of wormhole on most of the routes), the watchdog technique (using monitor mode) is applied to the sensor network in which nodes start observing their neighbor nodes and watch for possible packet dropping.

In order to calculate the packet drops by the nodes, the network must operate in promiscuous mode. In promiscuous mode, each sensor node in the network listens to the packets transmitted by its own neighbor nodes. The code below will put all the sensor nodes in the WSN in promiscuous mode. The code in function tap() is used if node A wants to listen to the packets from some other node B in promiscuous mode. This is used to check whether node B is forwarding the packets which are sent by A. To test the established path to the source node sends ICMP messages in the network. The nodes receive ICMP messages and go to monitor mode to watch their adjacent nodes. For this purpose, we make use of TclObject and MAC layer function tap in ns2.

Figure 7 shows that the proposed technique puts all nodes in the route to the monitor mode. The source node sends fake packets to check the possibility of any malicious node (wormhole) in the established route.

Figure 8 provides the scenario where the entire nodes other than malicious node (i.e., node 6) reply back to source node 0 with a RREP.

We make use of (1) to (5) for the wormhole detection processing. Equation (6) is used for finding out the presence of any wormhole in the established path; that is, we add the values of TDP_P and PLP_P. The nodes are given different rating values according to their behavior and those suspected to be malicious are given least rating value. A route table shown in Table 3 (sample) is created for this purpose. The scale rate has three values, namely, 1, 2, and 3, as shown in Table 1: a node gets value of 1 if it is not malicious, value of 2 if it is expected to be malicious, and value of 3 if it is malicious. The nodes are colored according to their rating values and the colors used are red, green, and yellow. Scale 1 node is represented by the color green, scale 2 node is represented by yellow, and scale 3

Table 3: Sample rating of nodes.

Source	Neighbor	SX-Pos	SY-Pos	Distance	Rating
0	1	−76	417	208	1
0	2	−76	417	145	2
0	3	−76	417	172	3
0	4	−76	417	123	3
0	5	−76	417	328	3
0	6	−76	417	318	1
0	7	−76	417	354	3
0	8	−76	417	449	2
0	9	−76	417	465	2
0	10	−76	417	566	1
0	11	−76	417	138	2
0	12	−76	417	228	2
0	13	−76	417	327	2
0	14	−76	417	433	2
0	15	−76	417	573	3
0	16	−76	417	566	2
0	17	−76	417	695	3
0	18	−76	417	529	1
0	19	−76	417	469	3
0	20	−76	417	325	1
0	21	−76	417	159	1
1	0	73	563	208	3
1	2	73	563	132	2
1	3	73	563	250	2
1	4	73	563	309	2
1	5	73	563	178	3
1	6	73	563	245	3
1	7	73	563	344	3

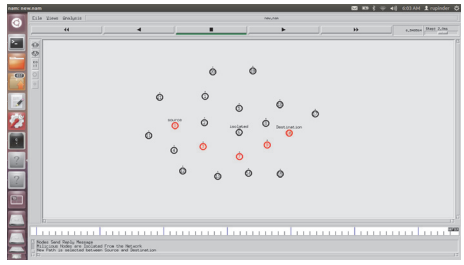

Figure 9: Isolation of wormhole node number 6.

node is represented by red in the simulation. The node with green color is most trusted, with yellow color being averagely trusted and red color being the least trusted. Figure 9 shows the isolation of the wormhole node from the established path in the sensor network. A new path is established for the safe transmission of data from the source node to the destination node.

5. Performance Evaluation

In order to assess the efficiency and competence of the proposed technique, that is, WRHT, and some other well-known wormhole detection techniques, NS-2.3 based simulation is done for WSNs coding organizations and running wormhole detection techniques.

5.1. Experimental Set-Up. The existing and proposed wormhole detection techniques are implemented on a Linux workstation (2.4 GHz Intel i5 processor with 8 GB RAM and 512 GB memory). The encryption library Beecrypt [41] is utilized to simulate the cryptographic and signature techniques. We adopted RSA [42] and MD5 [43] techniques with 9192-bit key size. The certificate authority (CA) is also implemented, which handles public keys and the individuality of sensor nodes. Therefore, a public key infrastructure is utilized in the experiments. The simulation is done several times by considering different set of sensor nodes every time.

5.2. Performance Measures. The primary metrics considered in this paper are accuracy (A_{cc}), $F1$ score (F_1), and Matthews correlation coefficient (M_{cc}). These metrics are defined as follows.

(a) Accuracy (A_{cc}). A_{cc} represents the effectiveness of the given wormhole detection techniques. It states how much effective the detection rate is, which is calculated as

$$A_{cc} = \frac{TP + TN}{TP + TN + FP + FN}. \tag{7}$$

Here, TP represents the accurate prediction of those in which wormhole attacks are detected successfully, whereas FP represents those in which non-wormhole nodes are detected as attackers. TN indicates those in which non-wormhole nodes are evaluated successfully, whereas FN represents in which wormhole nodes are detected as genuine nodes.

(b) F1 Score (F_1). F_1 can be demonstrated as a weighted mean of the precision and recall, where F_1 attains its effective value at 1 and worst score at 0:

$$F_1 = \frac{2 * TP}{2 * TP + FP + FN}. \tag{8}$$

(c) Matthews Correlation Coefficient (M_{cc}). M_{cc} represents the degree of correlation between the actual wormhole nodes and predicted wormhole nodes. M_{cc} lies between −1 and 1, where being close to value 1 indicates more effectiveness of the wormhole detection techniques:

$$M_{cc} = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP) * (TP + FN) * (TN + FP) * (TN + FN)}}. \tag{9}$$

5.3. Experimental Results. The proposed and the existing well-known wormhole detection techniques are applied on the designed simulation 15 times. The mean values of the simulation are taken for evaluating the best technique. However, the nodes are varied between 50 and 500 only, but the proposed and existing works are not limited to this set only.

Table 4: Accuracy (A_{cc}) analysis.

Nodes	Chiu and Lui (2006) [2]	Hayajneh et al. (2009) [34]	Wang et al. (2010) [35]	Kim et al. (2011) [24]	Ji et al. (2015) [30]	Tsitsiroudi et al. (2016) [31]	Biswas et al. (2014) [32]	Patel and Aggarwal (2016) [33]	WRHT
50	0.74	0.80	0.82	0.85	0.90	0.92	0.91	0.94	0.95
100	0.75	0.77	0.81	0.83	0.87	0.91	0.93	0.95	0.97
150	0.76	0.79	0.72	0.85	0.89	0.92	0.95	0.94	0.98
200	0.77	0.82	0.84	0.87	0.92	0.94	0.97	0.98	0.99
250	0.76	0.81	0.82	0.84	0.91	0.92	0.94	0.94	0.98
300	0.74	0.82	0.80	0.82	0.92	0.90	0.92	0.93	0.96
350	0.77	0.79	0.79	0.84	0.88	0.89	0.94	0.96	0.99
400	0.75	0.79	0.80	0.82	0.89	0.90	0.92	0.95	0.97
450	0.74	0.82	0.79	0.83	0.92	0.89	0.93	0.93	0.95
500	0.76	0.77	0.84	0.87	0.87	0.94	0.97	0.95	0.98

Table 5: $F1$ score (F_1) analysis.

Nodes	Chiu and Lui (2006) [2]	Hayajneh et al. (2009) [34]	Wang et al. (2010) [35]	Kim et al. (2011) [24]	Ji et al. (2015) [30]	Tsitsiroudi et al. (2016) [31]	Biswas et al. (2014) [32]	Patel and Aggarwal (2016) [33]	WRHT
50	0.7249	0.696	0.7134	0.7395	0.783	0.84	0.791	0.817	0.826
100	0.7327	0.6699	0.7047	0.7221	0.7569	0.791	0.809	0.826	0.843
150	0.7446	0.6873	0.6264	0.7395	0.7743	0.81	0.826	0.817	0.852
200	0.7327	0.7134	0.7308	0.7569	0.82	0.817	0.843	0.852	0.861
250	0.7181	0.7047	0.7134	0.7308	0.791	0.83	0.817	0.817	0.852
300	0.7446	0.7134	0.696	0.7134	0.82	0.783	0.81	0.809	0.835
350	0.7249	0.6873	0.6873	0.7308	0.765	0.774	0.817	0.835	0.861
400	0.7136	0.6873	0.696	0.7134	0.774	0.783	0.82	0.826	0.843
450	0.7327	0.7134	0.6873	0.7221	0.84	0.774	0.809	0.809	0.826
500	0.7136	0.6699	0.7308	0.7569	0.756	0.817	0.843	0.826	0.852

Table 4 clearly demonstrates that the proposed technique has an optimistic wormhole detection rate compared to existing techniques. The mean A_{cc} of the best known wormhole detection technique in literature, that is, Patel and Aggarwal (16) [33], is 0.947, whereas in the case of the proposed technique it is 0.972. Therefore, proposed technique has minimum improvement in terms of A_{cc} and it is 0.025, that is, 2.5%. Thus, the proposed technique is more effective than most of the existing techniques.

Table 5 represents the fact that the proposed technique has an optimistic wormhole detection rate compared to existing techniques. The mean F_1 of the best known wormhole detection technique in literature, that is, Patel and Aggarwal (16) [33], is 0.8234, whereas in the case of the proposed technique it is 0.8451. Therefore, proposed technique has minimum improvement in terms of A_{cc} and it is 0.0217, that is, 2.17%. Thus, the proposed technique is more effective than most of the existing techniques.

Table 6 proves that the proposed technique has an optimistic wormhole detection rate compared to existing techniques. The mean M_{cc} of the best known wormhole detection technique in literature, that is, Patel and Aggarwal (16) [33], is 0.9127, whereas in the case of the proposed technique it is 0.9447. Therefore, proposed technique has minimum improvement in terms of A_{cc} and it is 0.032, that is, 3.2%. Thus, the proposed technique is more effective than most of the existing techniques.

Most of the techniques proposed in the literature are able to gain high performance in their experiments. However, some of them need impractical assumptions about the sensor network or special hardware as listed in Table 7. So, we also compare WRHT with some of them as the proposed technique does not need impractical assumptions, such as zero delay time, precise synchronized time, or the awareness of locations of nodes, which are usually assumed in the schemes in the literature adopting the viewpoint of the administrator. In addition, WRHT does not need the use of any particular hardware either. Due to its robust, simple concept, WRHT can improve most of the routing protocols in wireless sensor network.

6. Conclusion and Future Works

Wormhole attacks in WSNs are rigorous attacks that can be launched easily even in sensor networks with implementing authenticity and confidentiality. Addressing of wormhole

Table 6: Matthews correlation coefficient (M_{cc}) analysis.

Nodes	Chiu and Lui (2006) [2]	Hayajneh et al. (2009) [34]	Wang et al. (2010) [35]	Kim et al. (2011) [24]	Ji et al. (2015) [30]	Tsitsiroudi et al. (2016) [31]	Biswas et al. (2014) [32]	Patel and Aggarwal (2016) [33]	WRHT
50	0.793	0.768	0.787	0.816	0.864	0.883	0.873	0.902	0.912
100	0.899	0.739	0.777	0.796	0.835	0.873	0.892	0.912	0.931
150	0.852	0.758	0.691	0.816	0.854	0.883	0.912	0.902	0.980
200	0.826	0.787	0.806	0.835	0.883	0.902	0.931	0.980	0.950
250	0.852	0.777	0.787	0.806	0.873	0.883	0.902	0.902	0.980
300	0.812	0.787	0.768	0.787	0.883	0.864	0.883	0.892	0.921
350	0.826	0.758	0.758	0.806	0.844	0.854	0.902	0.921	0.950
400	0.899	0.758	0.768	0.787	0.854	0.864	0.883	0.912	0.931
450	0.793	0.787	0.758	0.796	0.883	0.854	0.892	0.892	0.912
500	0.852	0.739	0.806	0.835	0.835	0.902	0.931	0.912	0.980

Table 7: Security comparison of various existing techniques.

Technique	Mechanism used	Special hardware	Hidden mode	Participation mode
WRHT (proposed)	Probability of wormhole presence	No	Yes	Yes
WAP [36]	Neighborhood information	No	Yes	No
SPROUT [37]	Multipath routing	No	Yes	Yes
Wang et al. [35]	Neighborhood information	No	Yes	No
WRSR [38]	Connectivity information	No	Yes	Yes
Packet leashes [8]	GPS & clock	Yes	Yes	No
WARP [39]	Multiple link-disjoint paths	No	Yes	Yes
De Worm [34]	Neighborhood information	No	Yes	No
ODSBR [40]	Binary search	No	Yes	Yes

attacks is a crucial issue as far as security of WSNs is concerned, since wormhole attacks are difficult to detect. This is because wormhole attacks can be launched in several modes, with each one enforcing its own unique requirements for the detection method. In this paper, we propose WRHT (wormhole resistant hybrid technique) for detection of wormhole attack in WSNs. The proposed technique is a combination of the concepts based on two techniques, namely, watchdog and Delphi. The proposed techniques make use of the advantages of both Delphi and watchdog techniques. WRHT ensures that the wormhole will not be left untreated in the sensor network as it makes use of dual detection mechanism. WRHT calculates probability factor TDP_P and PLP_P in order to find the value of WPP_P; that is, WRHT finds out the wormhole presence probability of the path established by the source node. The nodes in the path are given different ranking and subsequently colors according to their behavior. The simulation results have clearly shown that the proposed technique has quite effective results over the available techniques. In addition, WRHT scheme does not require any additional hardware or impractical sensor network assumptions and, therefore, it can be directly used in sensor networks. In the future work, simulation will be done by increasing the number of wormhole tunnels to check the effectiveness of the proposed technique for different performance parameters.

Competing Interests

The authors declare that there are no competing interests.

Acknowledgments

The authors are highly thankful to the Department of RIC, I. K. G. Punjab Technical University, Kapurthala, Punjab, India, for providing the opportunity to conduct this research work.

References

[1] S. Marti, T. J. Giul, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 255–265, ACM, Boston, Mass, USA, August 2000.

[2] H. S. Chiu and K. S. Lui, "DePHI: wormhole detection mechanism for ad hoc wireless networks," in *Proceedings of the IEEE 1st International Symposium on Wireless Pervasive Computing*, pp. 1–6, Phuket, Thailand, January 2006.

[3] Y. Cho, G. Qu, and Y. Wu, "Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks," in *Proceedings of the 1st IEEE Security and Privacy Workshops (SPW '12)*, pp. 134–141, May 2012.

[4] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior

nodes in vehicular delay-tolerant networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7929–7937, 2015.

[5] J. Dromard, R. Khatoun, and L. Khoukhi, "A Watchdog extension scheme considering packet loss for a reputation system in wireless mesh network," in *Proceedings of the 20th International Conference on Telecommunications (ICT '13)*, pp. 1–5, Casablanca, Morocco, May 2013.

[6] E. Hernández-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "CoCoWa: a collaborative contact-based watchdog for detecting selfish nodes," *IEEE Transactions on Mobile Computing*, vol. 14, no. 6, pp. 1162–1175, 2015.

[7] E. Hernández-Orallo, M. D. Serrat, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," *IEEE Communications Letters*, vol. 16, no. 5, pp. 642–645, 2012.

[8] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, vol. 3, pp. 1976–1986, April 2003.

[9] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 6, no. 4, pp. 483–503, 2006.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247–260, 2006.

[11] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, pp. 21–32, Fairfax, Va, USA, 2003.

[12] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "TrueLink: a practical countermeasure to the wormhole attack in wireless networks," in *Proceedings of the 14th IEEE International Conference on Network Protocols (ICNP '06)*, pp. 75–84, November 2006.

[13] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proceedings of the Network and Distributed System Security Symposium*, San Diego, Calif, USA, February 2004.

[14] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN '05)*, pp. 612–621, Yokohama, Japan, June 2005.

[15] I. Khalil, S. Bagchi, and N. B. Shroff, "Mobiworp: mitigation of the wormhole attack in mobile multihop wireless networks," in *Proceedings of the IEEE Secure Communication*, pp. 1–12, September 2006.

[16] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27–59, 2007.

[17] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04)*, pp. 51–60, Philadelphia, Pa, USA, October 2004.

[18] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proceedings of the IEEE 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 107–115, Anchorage, Alaska, USA, May 2007.

[19] N. Song, L. Qian, and X. Li, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," in *Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium (IEEE IPDPS '05)*, p. 289, Denver, Colo, USA, April 2005.

[20] L. Buttyán, L. Dóra, and I. Vajda, "Statistical wormhole detection in sensor networks," in *Security and Privacy in Ad-Hoc and Sensor Networks*, R. Molva, G. Tsudik, and D. Westhoff, Eds., vol. 3813 of *Lecture Notes in Computer Science*, pp. 128–141, Springer, Berlin, Germany, 2005.

[21] S. A. Borbash, A. Ephremides, and M. J. McGlynn, "An asynchronous neighbor discovery algorithm for wireless sensor networks," *Ad Hoc Networks*, vol. 5, no. 7, pp. 998–1016, 2007.

[22] D. Angelosante, E. Biglieri, and M. Lops, "Neighbor discovery wireless networks: a multiuser-detection approach," in *Proceedings of the Information Theory and Applications Workshop (ITA '07)*, pp. 46–53, 2007.

[23] M. Keally, G. Zhou, and G. Xing, "Watchdog: Confident event detection in heterogeneous sensor networks," in *Proceedings of the 16th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS '10)*, pp. 279–288, April 2010.

[24] M. J. Kim, M. Medard, and J. Barros, "Algebraic watchdog: mitigating misbehavior in wireless network coding," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 1916–1925, 2011.

[25] X. Liu, S. Chen, and W. Song, "A design and implementation of watchdog based on observer pattern and finite state machine," in *Proceedings of the 10th IEEE International Conference on Reliability, Maintainability and Safety (ICRMS '14)*, pp. 407–411, August 2014.

[26] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 107–115, Barcelona, Spain, May 2007.

[27] T. Zhang, J. He, Y. Zhang, Y. Zhang, and X. Song, "DV-based robust localization against wormhole attacks in wireless sensor networks," *Journal of Computational Information Systems*, vol. 7, no. 13, pp. 4732–4739, 2011.

[28] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 736–745, 2009.

[29] J. Singh, S. Gupta, and L. Kaur, "A cross-layer based intrusion detection technique for wireless networks," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 201–207, 2012.

[30] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 660–674, 2015.

[31] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs," in *Proceedings of the 9th IFIP Wireless and Mobile Networking Conference (WMNC '16)*, pp. 103–109, Colmar, France, July 2016.

[32] J. Biswas, A. Gupta, and D. Singh, "WADP: a wormhole attack detection and prevention technique in MANET using modified AODV routing protocol," in *Proceedings of the 9th IEEE International Conference on Industrial and Information Systems (ICIIS '14)*, pp. 1–6, December 2014.

[33] M. M. Patel and A. Aggarwal, "Two phase wormhole detection approach for dynamic wireless sensor networks," in *Proceedings*

of the IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET '16), pp. 2109–2112, Chennai, India, March 2016.

[34] T. Hayajneh, P. Krishnamurthy, and D. Tipper, "DeWorm: a simple protocol to detect wormhole attacks in wireless ad hoc networks," in *Proceedings of the 3rd IEEE International Conference on Network and System Security (NSS '09)*, pp. 73–80, Gold Coast, Australia, October 2009.

[35] Y. Wang, Z. Zhang, and J. Wu, "A distributed approach for hidden wormhole detection with neighborhood information," in *Proceedings of the IEEE 5th International Conference on Networking, Architecture and Storage*, pp. 63–72, Macau, China, July 2010.

[36] S. Choi, D.-Y. Kim, D.-H. Lee, and J.-I. Jung, "WAP: wormhole attack prevention algorithm in mobile ad hoc networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing(SUTC '08)*, pp. 343–348, Taichung, Taiwan, June 2008.

[37] J. Eriksson, M. Faloutsos, and S. V. Krishnamurthy, "Routing amid colluding attackers," in *Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP '07)*, pp. 184–193, IEEE, Beijing, China, October 2007.

[38] R. Matam and S. Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, article 180, 2013.

[39] M.-Y. Su, "WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," *Computers & Security*, vol. 29, no. 2, pp. 208–224, 2010.

[40] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," *ACM Transactions on Information and System Security*, vol. 10, no. 4, article 18, 2008.

[41] Beecrypt, http://sourceforge.net/projects/beecrypt/.

[42] R. L. Rivest, A. Shamir, and L. Adleman, "Method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[43] R. Rivest, "The md5 message-digest algorithm," RFC 1321, 1992.