Wireless Personal Communications (2022) 124:1081–1108
https://doi.org/10.1007/s11277-021-09395-y

Wormhole Attack Detection System for IoT Network: A Hybrid Approach

Snehal A. Bhosale[1] · **S. S. Sonavane**[2]

Accepted: 14 November 2021 / Published online: 30 November 2021

Abstract
Many errors in data communication cause security attacks in Internet of Things (IoT). Routing errors at network layer are prominent errors in IoT which degrade the quality of data communication. Many attacks like sinkhole attack, blackhole attack, selective forwarding attack and wormhole attack enter the network through the network layer of the IoT. This paper has an emphasis on the detection of a wormhole attack because it is one of the most uncompromising attacks at the network layer of IoT protocol stack. The wormhole attack is the most disruptive attack out of all the other attacks mentioned above. The wormhole attack inserts information on incorrect routes in the network; it also alters the network information by causing a failure of location-dependent protocols thus defeating the purpose of routing algorithms. This paper covers the design and implementation of an innovative intrusion detection system for the IoT that detects a wormhole attack and the attacker nodes. The presence of a wormhole attack is identified using location information of any node and its neighbor with the help of Received Signal Strength Indicator (RSSI) values and the hop-count. The proposed system is energy efficient hence it is beneficial for a resource-constrained environment of IoT. It also provides precise true-positive (TPR) and false-positive detection rate (FPR).

Keywords Hop count · IoT · Intrusion detection system · Network security · RSSI · Wormhole attack

1 Introduction

IoT is an emerging technology nowadays with a wireless interconnection of sensory devices in the existing infrastructure. Most of the researchers in this field claim that more than 30.9 billion devices are expected to connect to the internet by 2022. Smart cities, smart homes, smart grids, smart medical treatments, smart agriculture, etc., are the demanding applications of IoT [1, 2]. Sensory devices are uniquely identified by IP addresses viz IPv4 and IPv6. IPv4 has limitations of providing IP addresses to the network with a large number

✉ Snehal A. Bhosale
sa_bhosale@yahoo.com

[1] RMD Sinhgad School of Engineering, SPPU, Warje, Pune, India

[2] Vijaybhoomi University, Karjat, Navi Mumbai, India

of devices whereas IPv6 protocol offers an infinite number of unique IP addresses. The performance of all these smart devices can be affected by battery power, memory, communication ranges, size, etc. For optimal performance of the network, all the above constraints are considered by avoiding the use of bulky and battery consuming encryption or security algorithms [3].

IoT network is vulnerable to internal (within the network) and external (through the internet) attacks. Currently, no Intrusion Detection Systems (IDSs) are reported fulfilling security requirements in the resource constrained IoT network efficiently. The existing IDSs are utilized either for Wireless Sensor Network (WSN) or conventional internet. A need for security in IoT as well as various security attacks on Routing Protocol for Low Power and Lossy Network (RPL) and IPv6 Low Power Wireless Personal Area Network (6LoWPAN) is discussed in a few research papers [4–6].

To design a security solution for an IoT network is a challenging task due to many new protocols like DTLS [7], IPsec [8], IEEE 802.15.4 link-layer security [9], RPL [10], 6LoWPAN [11], etc., that are involved in IoT communication. Also, the links used in IoT are lossy with resource-constrained devices connected to an insecure internet. Attacks like wormhole attack, sinkhole attack, blackhole attack, selective forwarding attack, etc., affect the performance of IoT network adversely [12, 13]. Routing errors are a prominent factor affecting the security of data communication at the network layer of the IoT protocol stack. A wormhole attack causes routing errors which subsequently affect data communication in IoT. In the proposed work, an IDS is developed to detect and remove wormhole attacks from the IoT network.

1.1 Security Issues in IoT

Because of IoT, the world has become smarter. However, as it is moving towards more intelligent applications, more hackers and attackers are getting many chances to interfere which adds to life-threatening security issues in many forms. Though communication between all the devices without the intervention of humans for a smart network is the bright side of IoT, on the other hand, it increases threats of security and privacy of the data that is shared, stored and generated in the network. It is crucial and necessary for the IoT system to provide safety and privacy to the user data for the IoT network to be successfully implemented.

Smart homes, smart cars or smart grids can be exploited by hackers and the data can be misused which may severely affect everyone's lives. Hackers may use personal, industrial or governmental data which is very sensitive for a wrong purpose [14, 15]. Security options of the traditional network are not applicable to the IoT network because of many reasons as discussed below:

- IoT network is exceptionally heterogeneous and distributed.
- The devices used in IoT networks are resource-constrained in processing or computational capability, memory, battery life and bandwidth which doesn't support conventional network security solutions that require higher resources.
- Internet Protocol (IP) is used to connect IoT devices to an insecure internet where it faces attacks from the internet.
- As IoT network is formed by various heterogeneous technologies and protocols, security solutions must be compatible with all these protocols and standards which again make a heavyweight solution that is not suitable for the constrained network.

- A considerable amount of data is generated and floated by the IoT devices in wireless media which has limited bandwidth. It is easy for attacker nodes to interrupt communication by destroying or modifying data packets.
- IoT network is open and flexible to accept new protocols, standards or devices for the scalability property. But this property makes it easier for attackers to break the security and insert attacks to disturb communication.
- IoT network has decentralized wireless communication skills; any new device can be easily added in the existing network which can further lead to attack insertion.
- Most of the time, IoT devices are placed in physically insecure areas because of which attackers quickly attack these devices physically by replacing or reprogramming the nodes or changing the batteries of the nodes [16, 17].

There are various types of errors caused in an IoT network that affect the quality of the data communication in IoT.

1.2 Overview of Wormhole Attack

A wormhole attack affects network performance devastatingly. Because of a wormhole attack, routing information gets corrupted by inserting incorrect route information in the network. Also, localization dependent protocols fail in the presence of a wormhole attack. It damages data delivery and network-based stations also get altered. A wormhole attack allows other attacks like blackhole, DoS, sinkhole, grayhole, eavesdropping and Man In The Middle attack to be launched in the network. Because of a wormhole attack, unauthorized access can be gained and security keys can be cracked. Hence a wormhole attack is identified as a severe attack present at the network layer of IoT protocol stack and needs to be addressed.

In a wormhole attack, two long-distance nodes form a tunnel between themselves, thus pretending to be close to each other. When any transmitted packet comes to either of the attacker nodes, it sends the packet to the other long-distance attacker node through the intermediate legitimate nodes. These intermediate nodes are not a part of the said communication, but due to the wormhole attack, they get involved in transmission and drain their battery power. The deletion of a wormhole attack is not simple because the existence of this attack is detected only after a considerable loss. Hence it is necessary to design a strong IDS which will detect the presence of the wormhole attack and the attacker nodes at an early stage of its occurrence [18–20]. In the proposed research work, an IDS which can expose a wormhole attack at an early stage is designed.

1.3 Intrusion Detection System

Intrusion detection is a security mechanism that depends on the analysis of data collected in the network to identify any abnormal activity symptoms to discover the attack and trigger an alarm. To design an IDS for the 6LoWPAN-RPL based IoT network, one must consider its characteristics. IoT networks are infrastructure-less, ad-hoc and heterogeneous networks. Also, they are formed by devices with resource-constrained characteristics in terms of memory, processor, bandwidth, storage capacity and battery. Hence a suitable IDS for any attack detection in the IoT network should be one that consumes fewer resources. This section discusses the classification of IDSs for IoT networks. There are two significant classifications of IDSs: (i) Placement Strategy, (ii) Detection Method [21–24].

In the proposed work, the IDS used is of both the types, centralized as well as a hybrid type of IDS with signature-based characteristics. For the implementation of the IDS the proposed system uses 6LoWPAN [25–27], RPL [28–33] and Ad-hoc On-demand Distance Vector (AODV) [34–36] protocols. These protocols function in the IoT communication network.

2 Survey of Available IDSs for Wormhole Attack in IoT

As has been mentioned above, a wormhole attack is activated in the network by forming a tunnel between two long-distance nodes. The presence of a wormhole attack modifies the routing table and misguides the nodes for packet transmission. It unnecessarily adds a delay in the transmission and drains the battery of resource-constrained devices. Researchers have developed IDSs for wormhole attacks in WSN and IoT networks. The proposed research work focuses on the IoT network hence the existing IDSs for wormhole attack detection in IoT are discussed next. To design IDS for a wormhole attack, one needs to know the symptoms of the existence of a wormhole attack. When a wormhole attack enters the network, path delays between the networks increase and the hop-count decreases abruptly. Data packets are received from far away nodes in the network. In the presence of a wormhole attack, the number of neighbour requests increases, and a particular link is utilized more than the others. These symptoms are considered while designing the IDS for the wormhole attack detection. Because of a wormhole attack, other attacks like eavesdropping and sinkhole attacks arrive in the network which further disrupts data communication completely. Researchers have used various approaches for wormhole attack detection in WSN and IoT. A detailed survey is as given below:

Gupta et al. [37] have developed a technique to detect wormhole attacks using the 'hound packet'. This technique is a software method of attack detection. In this method, a hound packet is transmitted from source to destination through every node with an already established path. Every node along this path stores the hound packet information. The source node keeps a count of the hop difference with single hop away node. The hop difference between intermediate nodes with a threshold level is compared by the destination node. After studying this method, it is observed that it has given a high false-positive detection rate. Also, the hound packet adds delay in processing the packet and the processing overhead is increased. For wormhole attack detection, Khan et al. [38] have used the merkle tree methodology for authentication of communication in the network. In this method, root-level nodes were chosen from where the merkle tree originated and dealt with authentication in the dense and complex networks by breaking it into smaller pieces to identify the presence of a wormhole attack in the network. The disadvantage of this method is that it adds communication and computational costs at the root level.

Ji et al. [39] have developed a distributed wormhole attack detection algorithm called DAWN which detects changes in the direction of packet flow caused by the wormhole attack. The DAWN algorithm gathers data from the steady network rather than the middleware of location information or global synchronization. Limitations of this method are, it requires extra processing time and extra overhead for network monitoring. Arai [40] in his research work, has detected a wormhole attack by using a location-aware methodology. In his method, the attacker node is identified by using the hop-count and the location information of the neighbouring node. For performance analysis, the author has considered parameters like several affected nodes, average hop-count reduction and a suspicious rate. The

limitation of this method is that it cannot be used for complex networks. Also, the author has not provided true and false-positive detection rates in his research work.

Acharjee et al. [41] have developed a hybrid algorithm for the detection and prevention of a wormhole attack. It is based on the High-Performance Adhoc On-demand Distance Vector (AODV-HP) routing protocol. This algorithm uses a communication node between neighbours, target hop-count and an anomaly value of all the nodes in the network. Using this algorithm, the wormhole link is effectively separated from the concerned network. The drawback of this method is that it has not been verified in real-time scenarios. Zheng et al. [42] have developed an IDS for wormhole attack detection. They have improved the localization accuracy by using the nodes which were outside the range of a normal attack. This method is efficient for a large distance attacker node with a higher communication radius. But it gives an inadequate response for attack detection for an isotropic sensor network.

Sharma et al. [43] have offered a high transmission power type wormhole attack detection method. They have improved parameters like average delay, throughput, packet delivery, etc., by modifying routing protocols. The disadvantage of their approach is that it requires more transmission power. Lai et al. [44] have offered wormhole detection techniques in RPL based IoT networks without using any extra hardware. In their method, the authors have used rank information for measuring the relative distance to the root node and neighbour nodes. In their approach, the presence of a wormhole attack is detected when an unreasonable rank is identified. They have considered the 'rank' of the node as the attack detection parameter where rank is nothing but a number of hops calculated from the child node to the root node by RPL. The rank represents the location of the node with respect to the root node. When nodes move away from the root, the rank increases. The authors have used geographic leashes to locate the attacker nodes. The limitation of this method is that it doesn't consider the integrity and confidentiality of the network.

Bendjima et al. [45] have proposed a neighbourhood discovery-based energy-efficient IDS using the principle of sectors and mobile agents operation. In their research work, using a mobile agent, the information about the network is gathered and sent to the sensor. By using the itinerary algorithm, the response time of lost packets is reduced, less energy is consumed and resources of the nodes are preserved. The developed method detects the attack and the attacker node by improving the security schemes available for the wormhole attack detection. The disadvantages of this method are, there is a high packet drop ratio and it consumes more energy. Patel et al. [46] have used neighbourhood and connectivity information to detect a wormhole attack in the network. In their method, to identify the wormholes, information regarding neighbouring nodes and the connectivity of sensor nodes is used as a detection feature. The drawback of their system is that the implemented approach is not applicable for non-stationary sensor networks.

Johnson et al. [47], in their research work, have used neighbour discovery and path verification mechanisms to detect a wormhole attack. They have removed the attack without adding any new hardware in the system. Their implementation is developed using the NS2 simulator with a modified AODV protocol. They have used neighbour information for identifying the attack. The validity of two-hop neighbours who have forwarded the control or data packets is checked. If it is found to be illegal then the attack detection alarm is raised. The authors have verified their results using delay, throughput and the packet delivery ratio. The limitation of their method is that it has a low packet delivery ratio. Tiruvakadu et al. [48] have implemented a wormhole attack detection system using a honeypot to monitor the activities of the attacker in the network. The authors have used the wormhole tree to analyse network traffic. The honeypot uses three steps to detect the attack: (i) Attack tree model for all observations which are

responsible for a wormhole attack. (ii) Analysis model of a wormhole attack configuration. (iii) Increase network observations for decision making. The authors have used the AODV protocol for attack detection. The disadvantage of this method is that it increases latency in communication.

Perazzo et al. [20] have implemented a wormhole attack detection method by inserting attacker nodes using two endpoints deployed in different areas of the network. Their work is operated at the MAC layer of the IoT protocol stack. For implementation, they have interfaced with Python and Cooja simulators where the python process runs on the CC2650 Launchpad board and the Cooja simulator on the laptop. They have verified their results using a packet loss and frame loss. They have used a proxy-acker technique to increase the impact of the attack. They have used three parameters, namely, local packet loss, global packet loss, and the wormhole nodes for attack detection. Though they have not got optimum results for attack detection, they have concluded that the wormhole attack detection can be improved if related attacks like traffic eavesdropping and selective packet dropping are detected.

Qazi et al. [49] have provided an extension of the DELPHI algorithm for wormhole attack detection, where it is assumed that the base wireless rate is fixed. In DELPHI with this assumption, the detection rate is higher than 80%. There are many drawbacks of the original DELPHI algorithm, such as it is not able to protect the AODV protocol in a multiple transfer space. Multirate-DELPHI has improved the functionality by developing three factors, namely, Multi-channel, Processing delay and neighbouring supervision. The authors have used circular delay time which measures time duration in which confirmation of signal reception is received. With the help of this technique the detection rate of a wormhole attack is improved. The disadvantages of this method are that it consumes more energy and it increases the processing time.

Luo et al. [50] have used the CREDND algorithm for wormhole attack detection in WSN. In their research work, the authors have proposed CREDND, a protocol for creating a Credible Neighbour Discovery against the wormholes in WSN. The CREDND algorithm can detect an external as well as internal wormhole attack with the hop difference between two neighbours and monitoring authentication packets forwarded by attacker nodes by enabling common neighbour nodes, respectively. Their method does not perform well when different types of nodes with various transmission ranges are used. For a more complex network, this method doesn't give good results.

This is the survey of the existing IDS for wormhole attack detection. The next section discusses the limitations of earlier research work and the necessity to design a new attack detection system that will detect the presence of a wormhole attack efficiently considering IoT characteristics.

2.1 Limitations of Earlier Wormhole Attack Detection Systems

As per the discussion on the survey of an available wormhole attack detection system, there are many limitations as stated below:

i. Very little work has been done on the design of IDS in the IoT network as compared to WSN.
ii. No IDS has given optimum values for True and False-Positive Detection Rate for wormhole attack detection in IoT.

iii. Power consumption is one of the most significant criteria for attack detection in resource-constrained networks such as IoT. Many IDSs consume high power to achieve attack detection.
iv. Many IDSs cannot justify the optimum values of Accuracy, F1 Score and Mathews Correlation Coefficient.

After surveying the research work on wormhole attack detection, this research work has focused on RSSI and Hop-count as the attack detection parameters. RSSI is the preferred tool for wormhole attack detection because it doesn't require any additional hardware for signal strength detection. However, it has been observed that if only RSSI is used for wormhole attack detection, it doesn't give optimum results for a false-positive detection rate (FPR). FPR is when there is no attack and still an alarm for an attack is raised. To avoid this, the hop-count is used along with the RSSI value which improves the FPR in the proposed research work.

After discussing the limitations of the available methods for wormhole attack detection, a novel design technique is developed for the said attack detection in the proposed research work. For the development of the IDS, a proper simulation tool needs to be finalized. In the proposed system the Contiki OS with the Cooja simulator is used for the purpose of simulation.

3 Wormhole Attack Detection System for IoT Network: A Hybrid Approach

The proposed system is an 'RSSI and Hop-Count Based Energy Efficient Wormhole Attack Detection System for IoT Network' (RHE2WADI). For attack detection using simulation, the proposed system uses two parameters, namely, 'RSSI' from the range-based localization method and 'Hop-count' from the range-free localization method. Thus, the developed system uses a 'Hybrid' approach for attack detection. Due to two different parameters, the proposed method is divided into two stages. Common suspicious nodes from both the stages are declared as attacker nodes and their entries are removed from the routing table by a border router. To obtain the simulation results for 'RHE2WADI', the Cooja simulator of the Contiki OS is used. The detection result is observed for a number of nodes, ranging from 20 to 100.

While designing the IDS for the wormhole attack, different parameters are finalized after studying its symptoms. Symptoms such as the strength of the signal, attraction of the path advertised by the attacker nodes, the difference between the actual path and the advertised path, and the delay in transmitting packets from the source to the destination are considered for designing the IDS. By considering this, the presence of the wormhole attack is detected with the 'RSSI' and 'hop-count' parameters.

When any node sends a neighbor request packet to nearer nodes, the distance between these two nodes is calculated using the RSSI value of the received packet. An alert is generated if it is higher than the transmission range of already existing nodes in the network. That particular link and the respective nodes are kept under observation by sending their IDs to the *suspect list 1*. By using the strength of the incoming signal, the distance between transmitter and receiver nodes can be estimated by using standard Eq. (1) for distance calculation.

$$Distance = 10^{\left(\frac{Transmitted\ Power - Received\ Power}{10*N}\right)} \quad (1)$$

where received power is the RSSI value and N is the constant that depends on the Environmental factor with a range of 2–4. In the current experimentation, it is considered as '2'. The RSSI value is negative and its unit is dBm (decibel-milliwats). Ideally, it must be zero. However, practically, it is in range of − 30 dBm to − 50 dBm. For the experimentation, a signal with an RSSI value of more than − 30 dBm is considered a strong signal, whereas a signal with an RSSI value of less than − 60 dBm is considered a weak signal.

The RSSI value alone detects the presence of the wormhole attack successfully; however, it increases the FPR which is not desirable. FPR is explained in detail in Sect. 4. Hence to reduce the FPR, along with RSSI, another parameter, i.e., the 'hop-count' is used, which gives the precise value of the FPR [51, 52]. Its details are discussed in the next section.

In the presence of a wormhole attack, the attacker nodes which are physically at a fair distance from each other form a tunnel between themselves. This reduces the hop-count drastically. When suspicious nodes are under observation at the border router, the actual hop-count in the database of the 6LoWPAN Border Router (6BR) and the advertised hop-count are compared. If the actual hop-count is below the threshold level then the node IDs of the suspicious nodes are sent to the *suspect list 2* of the second stage. If there are common nodes present in the *suspect lists* of both the stages consecutively for three times then a wormhole attack is confirmed and the attacker nodes are disabled from the network.

3.1 The Architecture of 'RHE2WADI' Method

In this section the architecture of the IDS to detect the wormhole attack is discussed. It requires at least a single node with extra features of battery power, processing power, etc., and which is treated as a border router (6BR). General sensor nodes connected to the internet through a 6BR, are as shown in Fig. 1.

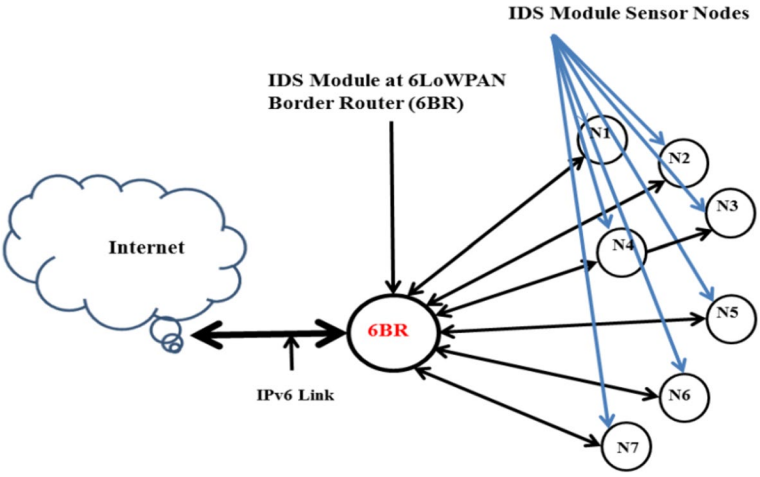

Fig. 1 Architecture of 'RHE2WADI' method

The 'RHE2WADI' monitors the behaviour of nodes before and after the insertion of an attack in the network. In the implemented work, the 6BR acts as a root node through which the hop-count is calculated using the RPL protocol. The RSSI value plays a significant role in locating the attacker node. The RSSI value of each packet travelling from the source to the destination node is converted into distance as per Eq. (1). When a large discrepancy in the RSSI amount and the hop-count is observed, then an attack and attacker nodes are identified [53, 54].

In the implemented method, the IDS module is placed at the 6BR as well as at each node. Initially, neighbour information is sent to the 6BR. If the requesting neighbour is in the transmission range of the original node, then the regular operation is continued. If the requested nodes are not in the transmission range of the original node, then the 6BR sends a victim packet. The victim packet collects the RSSI value from the requesting node. The distance (d1) is calculated using RSSI values received from the neighbouring nodes and verified with the actual distance calculated using the formula of the Euclidean distance given by using Eq. (2), where X and Y coordinates are the coordinates of the location of the nodes.

$$d1 = \sqrt{\left(X_1 - X_2\right)^2 + \left(Y_1 - Y_2\right)^2} \tag{2}$$

3.2 Implementation of 'RHE2WADI' Method

The Cooja simulator is a feasible simulator for the IoT application as it met all the requirements of 'RHE2WADI', related to routing and communication protocol [55, 56]. Power consumption is measured by including Mica [57] and Sky mote platforms [58]. Cooja is a GUI based simulation software and it also supports testing and debugging of IoT applications. Because of these reasons, the Cooja simulator is used in the current research work. Table 1 gives the parameters used for simulation in the 'RHE2WADI' method.

The design of the IDS for wormhole attack detection in the current research work is divided into two stages, as discussed below:

Stage 1: Implementation of an RSSI based, hybrid type IDS module at the 6BR and at each node;

Table 1 Simulation environment parameters for 'RHE2WADI' method

Parameter	Value
Simulator	Cooja simulator
Range of nodes	RX and TX: 100 m
Radio medium model	Unit disk graph medium (UDGM)
Number of nodes	10, 20, 30, 40, 50, 60, 70, 80, 90, 100
Mote type	Tmote Sky
Number of malicious nodes	10% of total nodes
Number of sinks	1
Transport layer	UDP
Network layer	Contiki RPL, IPv6, 6LoWPAN
Physical layer	IEEE 802.15.4
Objective function	RSSI and Hop-count

Stage 2: Implementation of a hop-count based on a centralised type of IDS module at 6BR to confirm the attack and attacker nodes.

A detailed explanation of both the stages is given in the next section.

3.3 RSSI-Based, Hybrid Type IDS Module

In stage 1, to implement the IDS at the 6LoWPAN Border Router or 6BR, the 6BR must be added to the network using the Contiki OS 2.7 and the Cooja simulator. Skymote nodes are used for the implementation of the 6BR and other nodes. In IoT, the 6BR is equivalent to the sink node of the WSN which connects the nodes of the network to the internet through the IPv6 protocol. As the IoT network is resource-constrained, the heavyweight IPv6 protocol is not suitable for it. Hence, the 6LoWPAN, which is a compressed version of the IPv6 protocol, is used for communication. The 6BR works between IPv6 of the internet and 6LoWPAN of the local nodes as shown in Fig. 1.

For the hybrid type of IDS implementation, heavy processing is done at centralized modules placed at the 6BR whereas lightweight modules are run to save energy at the sensor nodes. This section discusses the different modules used at the 6BR to discover the presence of an attack and the attacker nodes. It uses the RSSI value to detect the attack. The hypothesis is used as when a new neighbour request comes the 6BR node validates the claim. It checks whether a new neighbour is within the transmission range of the original neighbour or not. If it is not then an attack is detected. More details about the IDS based on RSSI and hop-count are discussed in the following section.

There are two modules in the RRSI based hybrid type IDS module: Distributed module and centralised module. Details of these modules are explained below.

3.3.1 Distributed Module

In the distribution module, the following four steps are proposed:

i. **Neighbour Validation**

Sensor nodes in the network contain the ID of the destination node and the ID of the neighbouring node. In the ‘neighbour validation’ step, this information is collected from all sensors to validate the original neighbours.

ii. **Distance Calculation**

By using Eq. (1), the distance between two nodes is calculated. This distance is verified using the Euclidian distance formula given in Eq. (2). Here the RSSI value gives the distance between the coordinates of the two nodes. The value of X and Y coordinates of the nodes are calculated with the help of the Cooja simulator.

iii. **RSSI Collection**

The RSSI collection module is activated after the detection of an attack in the network. It collects the RSSI value from the victim node and its neighbour node using victim packets. The 6BR maintains two RSSI values, one from the victim node and the other from its neighbour which is in the range of the attacker node. To avoid multiple RSSI values coming from the same node, the 6BR compares the node ID of the latest RSSI value with an already sent node ID.

iv. **Attacker Node Detection**

The working of this module is based on the RSSI values received from the nodes. This module finds the nodes in the range of distance 'd' by converting RSSI values into distance 'd', as per Eq. (1). If some nodes are found consecutively for three times, then these nodes are considered as suspicious nodes and sent to suspectlist1.

3.3.2 Centralised Module

In the centralised module the following three steps are proposed:

i. **Send Neighbour Info**

This module is placed in the regular nodes and it saves the initial neighbours as the original neighbours at initialization. If new neighbour information is received, this module sends it to the 6BR as 'neighbour information packet info'. The IoT uses the UDP protocol for data transmission which does not guarantee packet delivery. For assured packet delivery, intermediate nodes forward the sender's packet through its default root and broadcasting. When intermediate nodes receive the 'victim forward packet' from the 6BR, they send it to the destination node by local unicast.

ii. **Monitoring RSSI**

After receiving the victim packet through broadcasting or from the border router, the receiver node initializes the monitoring process. When the receiving node finds its ID in second position and the ID of another victim colleague in the third position, it interchanges the two IDs; i.e., it puts the node ID of the other victim colleague in second place and its own ID in the third place. These two nodes record each other's RSSI values. To locate the attacker node, the two victim notes broadcast the end victim packets.

iii. **Send RSSI**

The previous module collects the RSSI value from the nodes and their neighbours. This recorded RSSI value must be sent to the border router through broadcast, unicast and through the default route. RSSI packets are forwarded after a pause of 2 s to avoid packet loss because of collision and buffer overflow.

These steps are shown in Algorithms 1 and 2.

• **Algorithm 1** The wormhole Attack Detection at 6BR

```
1)  if new neighbour is formed then,
2)     send nbr_info to 6BR
3)     if all neighbors are in transmission range, then
4)              no attack, normal traffic
5)     else send victim packets to  both the neighbors
6)              run algorithm for monitoring the node (Algorithm 'A')
7)              if victim packet transmission is completed then
8)                 wait for RSSI value
9)              else continue with packet transmission
10)                    if RSSI value is received then
11)                       find the attacker node
12)                       generate the alert
13)                       send attacker node ID to graylist1
14)                    else continue normal operation
15)                    endif
16)            endif
17)        endif
18) endif
```

The process of wormhole attack detection is given in Algorithm 1. Algorithm 'A' is explained in Algorithm 2 which runs at the individual nodes.

• **Algorithm 2** Node Monitoring (Algorithm A)

```
1)  if victim packet is received then
2)              if both victims are neighbors then
3)                 no monitoring, normal traffic
4)              else record RSSI for both the neighbors
5)              endif
6)                  if  victim_1is  original_nbr then
7)                      monitor RSSI value for victim_2
8)                  else victim_2 is original_ nbr
9)                      monitor RSSI value for victim_1
10)                 endif
11)                     monitoring is done
12) endif
```

3.4 Hop-Count Based, Centralized Type IDS Module

The AODV protocol is used for the hop-count metric. This module is placed at the 6BR hence, it is called the centralised module. It is used for broadcast as well as unicast routing where sequence numbers are used to find the routing messages. The destination sequence numbers are used to find the fresher path. AODV uses Route Request (RREQ) and Route Reply (RREP) as control messages. The source node broadcasts the RREQ message to the destination node and a RREP message is unicasted by the destination to the source node.

The RREP message includes the information of the hop-count of the route traversed from the destination to the source. On receiving the RREP, the source node checks the signature and if the signature matches the specific signature, the source node sends the encapsulated data packet through the route where the destination address is mentioned.

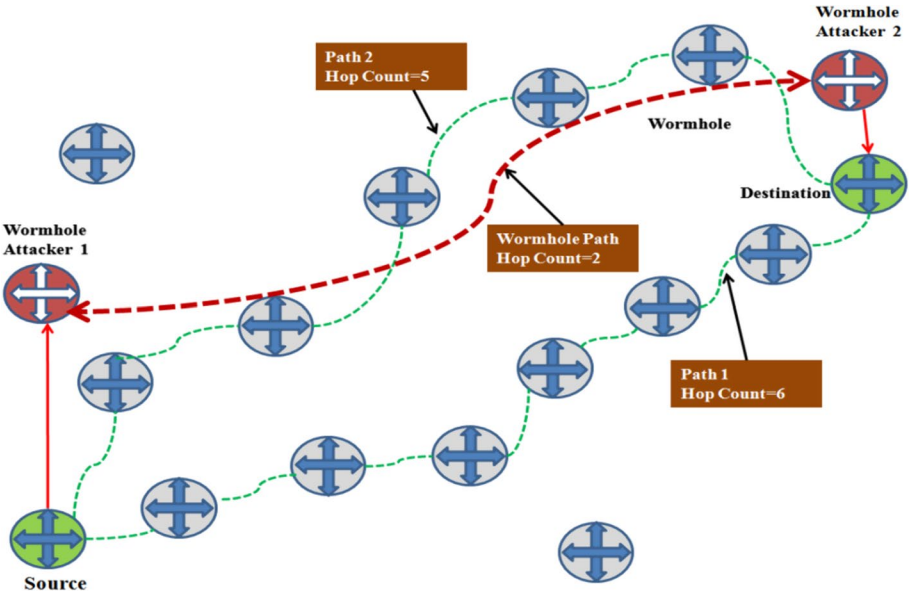

Fig. 2 Different routes with hop-count metric

Type (1 Byte)	VF (2 bits)	Hop Count (1 Byte)	RREQ ID (2 Bytes)	Destination IP Address (2 Bytes)	Source IP Address (2 Bytes)

Fig. 3 RREQ frame format

If some malicious activities are found, the data packet is sent via a different safe route. The hop-count is calculated. If it does not match, the route may contain the wormhole node. Thus, that path is avoided. Hop-count information is also maintained in the routing table of each node for further cross verification.

As shown in Fig. 2, the normal count from source to destination is considered as 5 or 6. However, when a wormhole tunnel is formed, the hop-count goes down to 2. The lower hop-count value attracts other nodes to send their packets through the wormhole tunnel.

In the 'RHE2WADI', method, initially, a hop-count of all the roots is examined. To avoid an attack, a threshold of the lower hop-count is set; if a count is below the threshold value, then that root is avoided and those nodes having the lowest hop-count are declared as attacker nodes. Minimum threshold hop count value is 10% of total nodes. In the AODV protocol, the RREQ packet is used for route request that discovers the root and RREP is used as the root replay. Figure 3 shows a packet format for a RREQ where the verification flag (VF) is used for distinguishing the new RREQ packet with the old one with RREQ ID. VF is also a part of the RREP packet. If VF = 0, then the RREQ packet is declared as normal route discovery. When VF $\neq$ 0, then it is considered a suspicious link.

3.4.1 Route Establishment with RREQ and RREP

Initially, the source node sends RREQ packets for route discovery when communication is required. In the RREQ packet, it adds the source IP (IP_S), the destination IP (IP_D), and the RREQ ID, ($RREQ_{ID}$). The hop-count is set to 0 and the expiration time of the RREQ packet is also set. This RREQ packet is broadcast in the network and received by the neighbouring nodes. Algorithm 3 demonstrates how a route is established with RREQ packets.

• **Algorithm 3** Route Establishment with RREQ

```
RREQ packets broadcasted by source node are received by intermediate nodes
if VF=0
    if IP_S, IP_D, and RREQ_ID same as cached value then
        drop RREQ packet
    else cache new IP_S, IP_D, and RREQ_ID
        add intermediate node id to cached list
        hop_count= hop_count +1
        construct reverse path to last hop
        endif
        else activate suspect list algorithm
endif
```

3.4.2 Route Establishment with RREP

An RREP packet is unicasted from the destination to the source node. In the reverse path, when intermediate nodes receive the RREP packets, the hop-count is incremented by 1. If IP_S, IP_D and $RREP_{ID}$ are the same as the cached value of the intermediate nodes then the hop-count of the received packet is compared with the cached hop-count. If the received hop-count is more than the cached hop-count, then the RREP packet is dropped, otherwise the IP_S, IP_D, and $RREP_{ID}$ and hop-count values are updated in the cache memory of intermediate nodes. A new route path from the node from which the RREP is received is formed. If IP_S, IP_D and $RREP_{ID}$ do not match the cached value of the intermediate nodes, then the new values of IP_S, IP_D, and $RREP_{ID}$ are saved in the cache and a new route path is established. Algorithm 4 explains the Route establishment with RREP in detail.

• **Algorithm 4** Route Establishment with RREP

```
RREP packet is unicasted
 if intermediate nodes receive the RREP then
     hop_count = hop_count +1
 else
    if IP_S, IP_D, and RREP_ID are same as the cached value, then
          if   received_ hop_count < cached_hop_ count, then
               new IP_S, IP_D, and RREP_ID and hop-count value are updated in the cache memory of intermediate nodes
          else RREP packet is dropped
               new route path from one node from which RREP received is established
          endif
            else new IP_S, IP_D, and RREP_ID and hop-count value are updated in the
             cache memory of intermediate nodes
     endif
endif
```

3.5 Hop-Count Number Limit and Suspect List Broadcast

When a wormhole attack is activated in the network, the hop-count is reduced drastically. The attacker node broadcasts the RREQ packet with the lowest hop-count which is accepted by the surrounding nodes by dropping the RREQ packets of legitimate nodes. Thus, only the route through the wormhole nodes is established as shown in Fig. 4.

The solution for this situation is to set a lower limit of the hop-count with a $\text{Hop\_Count}_{\text{lim}}$ register. The hop-count limit is set to 10% of the total number of nodes. For the condition shown in Fig. 4, if the $\text{Hop\_Count}_{\text{lim}}$ is set to 2 and if the received hop-count is compared and found to be less than or equal to $\text{Hop\_Count}_{\text{lim}}$, then the presence of a wormhole attack is declared. The suspect list is broadcast by the 6BR to identify the attacker nodes. The source node of the modified value is alerted, and then the suspect IP address is sent to *suspectlist2*. These IP addresses are compared with the IP addresses of suspectlist1. If common IP addresses are found in suspectlist1 and *suspectlist2* then the 6BR removes those nodes from the routing table permanently.

Algorithm 5 gives a better understanding of attack detection using the hop-count.

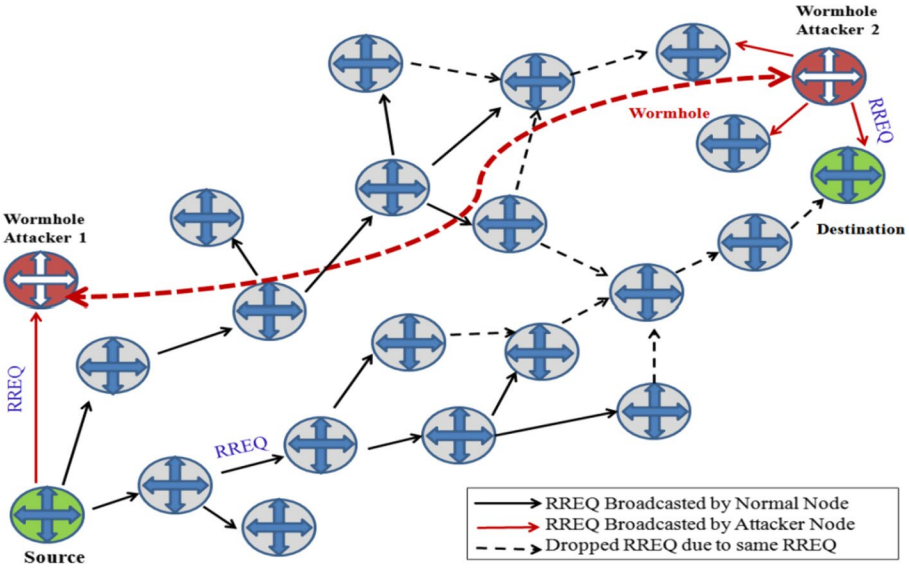

Fig. 4 Route formation in presence of wormhole attack

• **Algorithm 5** RREP number limit and Suspect List Broadcast

```
1)  if Hop_Count ≤ Hop_Count_lim then
2)     broadcast suspect list
3)  else normal traffic
4)     if IP_S, IP_D, and RREQ_ID same as cached value then
5)           if received VF = cached VF then
6)              if received_suspect_list = cached_suspect_list then
7)                drop RREQ packet
8)              else alteration of source code is identified
9)                source node confirms the attacker node
10)                  elseif IP_last_hopcount same as suspect_list then
11)                     drop the packet
12)                  else  update VF value and add the new_suspect_list
13)                     hop-count = hop-count +1
14)                     construct reverse path to last hop
15)                  endif
16)             endif
17)        endif
18)     endif
19)  endif
```

4 Results and Discussions

In this section, the evaluation of the implemented system is presented. After describing the experimental setup, quantitative assessment, the true and false-positive detection rates for each experimental set-up are investigated. Initially, the network is simulated without inserting the attacker node. At this stage, the routing table is built and the 6BR collects the information of all nodes. The experimentation starts with 20 nodes and two attacker nodes. After 15 min of network settlement, attacker nodes are inserted in the network with a long-distance node as a destination address in their routing table.

As new nodes are added in the network, a request about its validity is sent to the 6BR. The 6BR node starts collecting the RSSI and hop-count information from all the nodes. After verifying the RSSI values and the hop-count, the attacker node is identified by observing the RSSI values which show that the attacker nodes are not in the transmission range of the original node. The attacker also gives fewer hop-counts than the actual hop-counts. These symptoms show the presence of an attack and the attacker node is displayed on the output window of Cooja simulator.

In the implementation of the 'RHE2WADI' method, the readings are taken for nodes ranging from 20 nodes to 100 nodes with an interval of 10. Till 20 nodes, readings are constant, hence for analysis, readings taken after 20 nodes are considered. As the total number of nodes is increased, attacker nodes are inserted at the rate of 10% of the total nodes. For example, for 20 nodes, two attacker nodes are inserted and for 40 nodes, four attacker nodes are inserted and so on. The implemented IDS in the current research work is evaluated using performance and security-based metrics where attack detection rate, energy consumption and propagation delay are assessed under performance-based metrics. The obtained results are compared with state of art results obtained by Luo et al. [50]. Whereas, accuracy, F1 score and Mathew's

Coefficient Correlation (MCC) are evaluated under security-based metrics. The obtained results are compared with state of art results obtained by Johnson et al. [47], Perazzo et al. [20] and Luo et al. [50]. Their work is already discussed in section 2.

4.1 Performance-Based Metrics

Performance-based metrics measure the system's performance under which the attack detection rate, energy consumption, and propagation delay are observed. These terms are explained next.

i. **Detection Rate**

The true-positive and false-positive detection rates of the wormhole attacks are observed in the performed experimentation. True-Positive Detection Rate (TPR) is defined as how correctly the IDS identifies the presence of the attack and attacker nodes. Ideally, the TPR must be nearer to 100%. The developed system detects a wormhole attack successfully when an attack is present in the system. The detection rate reduces as the complexity of the network increases. It is calculated using equation (3):

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{3}$$

A False-Positive Detection Rate (FPR) is defined as how many times the IDS falsely raises an alarm for attack when the network is not under attack. Ideally, this value must be nearer to zero. It is calculated using Eq. (4):

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{4}$$

where

True-Positive (TP): the number of correctly recognized malicious nodes.
True-Negative (TN): the number of correctly recognized legitimate nodes.
False-Positive (FP): the number of incorrectly identified legitimate nodes, when a detector recognizes a legitimate node as malware.
False-Negative (FN): the number of incorrectly recognized malicious nodes, when a detector recognizes malware as a legitimate node.

ii. **Energy Consumption**

Energy consumption for a sensor node is defined as the amount of energy required per unit second for data processing and transmission. In the IoT, nodes are battery-powered and therefore, energy efficiency is an essential aspect in IoT devices. The Contiki's power-trace tool is used to measure the power consumption of the implemented IDS [59]. For calculation, the working voltage is considered as 3V. Energy consumption is calculated using nominal values of the Tmote sky, as shown in Table 2 and standard equation (5) [60].

$$\begin{aligned}&\text{Energy (mJ)}\\&= ((\mathrm{TX} * 19.5\,\mathrm{mA} + \mathrm{RX} * 21.8\,\mathrm{mA} + \mathrm{LPM} * 54.5\,\mathrm{mA} + \mathrm{CPU} * 1.8\,\mathrm{mA}) *\\&\quad 3\mathrm{V})/(4096 * 8).\end{aligned} \tag{5}$$

Table 2 Tmote sky operating conditions

Typical operating conditions	Min	NOM	Max	Unit
Voltage	2.1		3.6	V
MCU on, Radio RX		21.8	23	mA
MCU on, Radio TX		19.5	21	mA
MCU on, Radio off		1.8	24	mA
MCU idle, Radio off		54.5	120	mA
MCU standby		5.1	21.0	mA

Table 3 Parameters list to calculate propagation delay

Symbol	Parameter	Value
L	Packet size (bit)	125 bytes
R	Bit rate (bps)	250kbps
D	Distance between node and sink (m)	Maximum transmission range is 30 m
C	Speed (m/s)	3×10^8 for wireless communication (m/s)

iii. **Propagation Delay**

Propagation delay is defined as time taken by a packet for transmission from source to destination in the wireless environment. In the implemented system, propagation delay is calculated by using standard equation (6). The parameter values used in Eq. (6) are given in Table 3.

$$\text{Propagation delay} = \frac{\text{L}}{\left(\left(2*\frac{\text{L}}{\text{R}}\right)+\frac{\text{D}}{\text{C}}\right)} \tag{6}$$

4.2 Security-Based Metrics

Security based metrics measure the security related outcome of the given system. Under this, accuracy, the F1-score and MCC are measured. These terms are explained next.

i. **Accuracy (Acc)**

Accuracy represents the effectiveness of the given wormhole attack detection techniques. Total accuracy is the proportion of accurately classified instances, either positive or negative. It states how effective the detection rate is, which is calculated as Eq. (7):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{7}$$

ii. **F1-Score**

In the statistical analysis of binary classification, the F1 score is a measure of the accuracy of a test. It considers both, the precision p and the recall r, of the test to compute the score. Here p is the number of correct positive results divided by the number of all positive results returned by the classifier. And r is the number of accurate positive results divided by the number of all relevant samples. The F1 score is the harmonic mean of the precision and recall, where the F1 score reaches its best value at 1 (perfect precision and recall) and worst at 0. It is calculated as Eq. (8):

$$\text{F1 Score} = \frac{2*\text{TP}}{2*\text{TP} + \text{FP} + \text{FN}} \tag{8}$$

iii. **Mathew's Correlation Coefficient (MCC)**

For binary classification, there is another solution which is, treat the true class and the predicted class as two (binary) variables, and compute their correlation coefficient. The higher the correlation between the true and predicted values, the better is the prediction. This is the MCC when applied to classifiers. MCC represents the degree of correlation between the actual wormhole nodes and the predicted wormhole nodes. MCC lies between − 1 and 1, where being close to the value 1 indicates a higher effectiveness of the function. It is calculated as Eq. (9):

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

4.3 Performance Analysis of the Implemented System

4.3.1 Attack Detection Rate

The TPR and FPR of a wormhole attack are compared with results obtained by recent research work done by Luo et al. [50]. By considering attacker nodes 10% of the total nodes, the readings are taken as per Tables 4 and 5.

From Table 4, the average TPR values of the IDS developed by Luo et al. [50] and the IDS developed by the current research work are 90.24% and 95.01% respectively. Thus, the TPR value of the IDS using the 'RHE2WADI' method is 4.77% better than the most recent research work.

The average FPR for the research method of Luo et al. [50] is 18.07%. Whereas the FPR value for the proposed research work is 11.96% thus giving 6.11% better results than the earlier research work.

4.3.2 Energy Consumption

For energy consumption measurement, a comparison of the implemented IDS with a basic application 'hello world' is made using the powertrace tool. Energy consumption is calculated by using Eq. (5) and Tmote Sky Operating conditions as shown in Table 2. Energy

Table 4 True positive attack detection rate

No. of nodes	True positive detection rate (%)	
	Luo et al. [50]	'RHE2WADI' method
20	98.57	100.00
30	94.22	100.00
40	93.37	95.83
50	91.72	96.67
60	90.58	94.29
70	89.47	92.86
80	88.56	91.49
90	84.29	92.60
100	81.35	91.37
Average	90.24	95.01

Table 5 False positive attack detection rate

No. of nodes	False positive detection rate (%)	
	Luo et al. [50]	'RHE2WADI' method
20	11.23	7.10
30	12.57	8.22
40	13.90	10.70
50	16.17	10.76
60	17.14	11.90
70	19.11	12.22
80	22.51	14.28
90	23.29	15.28
100	26.67	17.14
Average	18.07	11.96

consumption for nodes ranging from 20 to 100 with an interval of 10 nodes is observed. The powertrace tool is applied to get the readings of work done by Luo et al. [50] and the proposed work. The obtained result is as shown in Table 6.

After running the 'hello world' application, using the IDS developed by Luo et al. [50] and the IDS developed by the current research work, the average energy consumption readings are 261623 mJ, 2969401 mJ and 2575811 mJ respectively. It is observed that the IDS in 'RHE2WADI' requires less energy to run.

4.3.3 Propagation Delay

Propagation delay is computed as a function of distance over wave propagation speed (d/s). By using the parameters shown in Table 3 and by using Eq. (6), propagation delay values are calculated for nodes ranging from 20 to 100 with an interval of 10.

A test packet is transmitted by the border router to all the nodes and the average propagation delay is calculated using Eq. (6). Similarly, the delay is calculated after attack

Table 6 Energy consumption

No. of nodes	Energy consumption (mJ)		
	Helloworld	IDS by Xiao et al. [50]	IDS in 'RHE2WADI' method
20	820,086	855,191	825,191
30	1,230,129	1,768,094	1,237,786
40	1,640,172	2,062,977	1,768,094
50	2,052,312	2,475,573	2,062,977
60	2,460,258	2,888,161	2,475,573
70	2,625,532	3,610,724	2,888,161
80	2,700,012	3,913,359	3,610,724
90	3,625,678	4,400,430	3,913,359
100	4,100,430	4,750,098	4,400,430
Average	2,361,623.22	2,969,400.78	2,575,810.56

activation, with the IDS developed by Luo et al. [50] and the IDS in the 'RHE2WADI' method.

It is observed that for 20 nodes, when there is no attack detected, the propagation delay is 0.22 mS. After activation of the wormhole attack, the propagation delay for the same packet is 0.62 mS. It happens because in the presence of the wormhole attack, the attacker node misguides the valid nodes to transmit the packet through the wrong route by changing the routing table. For the remaining nodes observations are taken as shown in Table 7.

The average propagation delay when no attack is detected is 0.3667 mS, the average delay in the presence of an attack and without an IDS is 0.7522 mS. The average propagation delays with the IDS by Luo et al. [50] and the IDS in the 'RHE2WADI' method

Table 7 Propagation delay

No. of nodes	Propagation delay (mS)			
	Delay when no attack	Delay in presence of attack	Delay in Luo et al. [50]	Delay in 'RHE2WADI' method
20	0.22	0.62	0.48	0.27
30	0.25	0.72	0.52	0.29
40	0.34	0.73	0.56	0.38
50	0.37	0.75	0.62	0.42
60	0.40	0.71	0.68	0.46
70	0.42	0.78	0.69	0.50
80	0.45	0.80	0.69	0.58
90	0.42	0.81	0.70	0.59
100	0.43	0.85	0.73	0.61
Average	0.3666	0.7522	0.63	0.4555

Table 8 Accuracy

No. of nodes	Accuracy			
	Johnson et al. [47]	Perazzo et al. [20]	Luo et al. [50]	'RHE2WADI' method
20	0.8635	0.8717	0.9322	1
30	0.8512	0.8549	0.9124	1
40	0.8576	0.8623	0.8823	0.9625
50	0.8428	0.8564	0.8756	0.9600
60	0.8386	0.8425	0.8700	0.9417
70	0.8310	0.8331	0.8513	0.9286
80	0.8154	0.8015	0.8354	0.9125
90	0.8075	0.7925	0.8221	0.9056
100	0.7715	0.7723	0.8157	0.8950

are 0.63 mS and 0.4555 mS respectively. This shows that the 'RHE2WADI' method requires less time for data transmission in the presence of attack.

4.4 Comparison of Security Based Metrics Results with State-of-the-Art Results

The evaluation and comparison of security-based metrics results are carried out by applying the latest and best techniques to earlier research work and the proposed method for a number of nodes ranging from 20 to 100 but are not limited to this set only. The primary metrics considered in the current research work are accuracy (Acc), F1 score, and MCC.

4.4.1 Accuracy

The results obtained in the 'RHE2WADI' method are compared with the results obtained from earlier research work. The latest research work by Johnson et al. [47], Perazzo et al. [20] and Luo et al. [50] are used as reference. For 20 nodes, when all systems have been run to detect the attack, the accuracy is calculated using Eq. (7). The same procedure is followed for nodes from 30 to 100.

In percentage, the average accuracy by Johnson et al. [47], Perazzo et al. [20] and Luo et al. [50] are 83.10%, 83.19%, and 86.63% respectively. Whereas accuracy in the current research work is 94.51% which is better than earlier research work as shown in Table 8.

4.4.2 F1 Score

The F1 score is used to measure the performance of the model. It is a weighted mean of the precision and recall, where F1 attains its effective value at '1' and worst score at '0'. The values of F1 score are obtained based on Eq. (8).

Table 9 F1 Score

No. of nodes	F1 Score			
	Johnson et al. [47]	Perazzo et al. [20]	Luo et al. [50]	'RHE2WADI' method
20	0.7832	0.8221	0.8447	1
30	0.7651	0.8163	0.8331	1
40	0.7569	0.8092	0.8264	0.9388
50	0.7484	0.8001	0.821	0.9355
60	0.7452	0.793	0.8156	0.8947
70	0.739	0.7724	0.8012	0.8864
80	0.7311	0.7653	0.7957	0.86
90	0.7253	0.7593	0.7883	0.8547
100	0.719	0.752	0.7811	0.8374

A comparison of the F1 Score obtained in the 'RHE2WADI' method with the latest existing techniques is shown in Table 9. In terms of percentage, the average F1 score by Johnson et al. [47], Perazzo et al. [20] and Luo et al. [50] are 74.59%, 78.77%, and 81.19% respectively. Whereas the F1 score in the current research work is 91.19% which is better than earlier research work.

4.4.3 Matthews Correlation Coefficient (MCC)

MCC defines the degree of correlation between the predicted wormhole nodes and actual wormhole nodes. MCC values are obtained between − 1 and 1. It is given by Eq. (9). Table 10 gives a comparison of MCC values obtained for state-of-the-art implementation and the IDS of the current research work.

In terms of percentage, the average MCC value obtained by Johnson et al. [47], Perazzo et al. [20] and Luo et al. [50] are 72.61%, 73.66%, and 74.94% respectively. Whereas the

Table 10 Matthews correlation coefficient

No. of nodes	Matthews Correlation Coefficient			
	Johnson et al. [47]	Perazzo et al. [20]	Luo et al. [50]	'RHE2WADI' method
20	0.8000	0.8019	0.8412	1
30	0.7822	0.7921	0.8123	1
40	0.7656	0.7838	0.7629	0.9122
50	0.7501	0.7523	0.7554	0.9075
60	0.7210	0.7342	0.7468	0.8492
70	0.7054	0.7216	0.7263	0.8363
80	0.6920	0.7056	0.7114	0.7997
90	0.6773	0.6810	0.7029	0.7905
100	0.6410	0.6571	0.6854	0.7647

average MCC value in the 'RHE2WADI' method is 87.33% which is much better than earlier work.

After comparing the results obtained in the 'RHE2WADI' method for performance-based and security-based metrics with state-of-the-art results, it is concluded that the IDS developed in the proposed method is better than all existing methods. The proposed method is different than the already existing methods in term of number of stages used to confirm the presence of attack. In proposed 'RHE2WADI' method, two stages of attack detection are used. The first stage uses 'RSSI' parameter to identify the presence of attack. Second stage which uses 'hop-count' parameter, confirms the attack if same nodes appear in both the detection stages. These two-stage attack identification methods have improved TPR and FPR values tremendously.

5 Conclusion

This paper has explained the design of IDS for wormhole attack detection. The IDS of the proposed method is less complex and uses less overhead; hence, it consumes less energy and it provides less propagation delay. Under performance-based metrics, most of the IDSs proposed in literature fail to get effective results in wormhole attack detection in IoT. When the system in 'RHE2WADI' is implemented using the Cooja simulation software, it is observed that the TPR value is 95.01% which is the highest TPR value for wormhole attack detection in an IoT based network. Even the FPR value is reduced to 11.96%, which is the lowest value compared to all the existing IDSs developed in the IoT network for wormhole attack detection. Energy consumption and propagation delay values of the 'RHE2WADI' method are better compared with state-of-the-art results.

The IDS in the 'RHE2WADI' method has judged using performance-based metrics and security-based metrics. Under performance-based techniques, detection rates, energy consumption and propagation delay are measured. The obtained results are far better than the existing research methods. Whereas, under security-based metrics, accuracy, F1 score and MCC are evaluated. The accuracy is 94.51% which is 7.88% better than the latest research work. For the F1 score, the obtained result is 91.19% which is 10% higher than the latest research work. Also, the result for MCC is 87.33% which is 12.39 % higher than the existing latest research work. From the obtained values in the proposed method, it can be concluded that the implemented system in this paper has given superior results in terms of all the metrics which decide the quality of the IDS.

Authors' contributions SAB and SSS conceived of the presented idea. SAB developed the theory and performed the computations, verified the analytical methods. SSS encouraged SAB to investigate security aspect in IoT and supervised the findings of this work. Both the authors discussed the results and contributed to the final manuscript.

Funding NA.

Availability of data and material The authors confirm that the data supporting the findings of this study are available within the article and its supplementary materials.

Code availability The Code that supports the findings of this study are available from the corresponding author, [SAB] upon reasonable request.

Declarations

Conflicts of interest The Authors (SAB and SSS) declare that there is no conflict of interest.

References

1. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Network, 32*, 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future2013.01.010
3. Pishva, D. (2017). Internet of Things: Security and privacy issues and possible solution. In *2017 19th international conference on advanced communication technology (ICACT)*. IEEE. https://doi.org/10.23919/ICACT.2017.7890229
4. Deshmukh, S., & Sonavane, S. S. (2017). Security protocols for Internet of Things: A survey. In *2017 international conference on Nextgen electronic technologies: Silicon to software (ICNETS2).* IEEE. https://doi.org/10.1109/ICNETS2.2017.8067900
5. Pongle, P., & Chavan, G. (2015) A survey: Attacks on RPL and 6LoWPAN in IoT. In *2015 international conference on pervasive computing (ICPC).* IEEE. https://doi.org/10.1109/PERVASIVE.2015.708703
6. Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. *Procedia Manufacturing, 32*, 840–847. https://doi.org/10.1016/J.Promfg.2019.02.292
7. Kothmayr, T., Hu, W., Schmitt, C., Bruenig, M., & Carle, G. (2011). Securing the internet of things with DTLS. In *Proceedings of the 9th ACM, conference on embedded networked sensor systems* (pp. 345–346). ACM.
8. Raza, S., Duquennoy, S., Chung, A., Yazar, D., Voigt, T., & Roedig, U. (2011). Securing communication in 6LoWPAN with compressed IPsec. In *2011 international conference on distributed computing in sensor systems and workshops (DCOSS).* IEEE. https://doi.org/10.1109/DCOSS.2011.5982177
9. Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2012). Secure communication for the Internet of Things—A comparison of link layer security and IPsec for 6LoWPAN. In *Security and communication networks*. Wiley Online Library. https://doi.org/10.1002/sec.406
10. IETF, RPL. *Routing over low power and lossy networks*. Accessed on August 2018.
11. Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). *Pv6 over low power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals*. IETF, RFC 4919. https://doi.org/10.17487/RFC4919
12. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Network, 20*(8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7
13. Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
14. Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2014). *Smart, nest thermostat: A smart spy in your home*. Black Hat USA.
15. Trappe, W., Howard, R., & Moore, R. S. (2015). Low-energy security: Limits and opportunities in the Internet of things. *IEEE Security, Privacy, 13*, 14–21. https://doi.org/10.1109/MSP.2015.7
16. El-hajj, M., Chamoun, M., Fadlallah, A., & Serhrouchni, A. (2017). Analysis of authentication techniques in Internet of Things (IoT), In *Proceedings of the 2017 1st cyber security in networking conference (CSNet)*, Rio de Janeiro, Brazil, October 18–20, 2017 (pp. 1–3). https://doi.org/10.1109/CSNET.2017.8242006
17. Shang, W., Yu, Y., Droms, R., & Zhang, L. *Challenges in IoT networking via TCP/IP architecture*. Technical Report 04, NDN, Technical Report NDN-0038; Named Data Networking. http://nameddata.net/techreports.html
18. Azer, M., El-Kassas, S., & El-Soudani, M. (2009). A full image of the wormhole attacks towards introducing complex wormhole attacks, in wireless ad hoc networks. *International Journal of Computer Science and Information Security, 1*(1).
19. Deshmukh-Bhosale, S., & Sonavane, S. S. (2018). Wormhole attack detection in Internet of Things. *International Journal of Engineering & Technology, 7*(2), 749–751. https://doi.org/10.14419/ijet.v7i2.33.15488

20. Perazzo, P., Vallati, C., Varano, D., Anastasi, G., & Dini, G. (2018). Implementation of a wormhole attack against a RPL network: Challenges and effects. In *14th annual conference on wireless on-demand network systems and services (WONS)*. IEEE. https://doi.org/10.23919/WONS.2018.8311669
21. Ansam Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*, 20. https://doi.org/10.1186/s42400-019-0038-7
22. Zarpelao, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications, 84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009
23. Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing, 72*, 79–89. https://doi.org/10.1016/j.asoc.2018.05.049
24. Moustafa, N., Turnbull, B., & Choo, K. R. (2019). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2871719
25. Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). *IPv6 over low power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals*. IETF, RFC 4919. https://doi.org/10.17487/RFC4919
26. Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). Denial-of-service detection in 6LoWPAN based Internet of Things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE. https://doi.org/10.1109/WiMOB.2013.6673419
27. Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., & Spirito, M. A. (2013). DEMO: An IDS framework for Internet of Things empowered by 6LoWPAN. *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*. https://doi.org/10.1145/2508859.2512494
28. Dvir, A., Holczer, T., & Buttyan, L. (2011). VeRA—Version number and rank authentication in RPL. In *2011 IEEE eighth international conference on mobile ad-hoc and sensor systems*. IEEE. https://doi.org/10.1109/MASS.2011.76
29. Perrey, H., Landsmann, M., Ugus, O., Schmidt, T. C., & Wählisch, M. (2013). TRAIL: Topology authentication in RPL. In *Proceeding EWSN '16 proceedings of the 2016 international conference on embedded wireless systems and networks* (pp. 59–64). arXiv:1312.0984v2
30. Le, A., Loo, J., Luo, Y., & Lasebae, A. (2014). The impacts of internal threats towards routing protocol for low power and Lossy network performance. In *2013 IEEE symposium on computers and communications (ISCC)*. IEEE. https://doi.org/10.1109/ISCC.2013.6755045.
31. Wallgren, L., Raza, S., & Voigt, T. (2013). Routing attacks and countermeasures in the RPL-based Internet of Things. *International Journal of Distributed Sensor Networks, 9*(8), 794326. https://doi.org/10.1155/2013/794326
32. Perazzo, P., Vallati, C., Arena, A., Anastasi, G., & Dini, G. (2017). An implementation and evaluation of the security features of RPL. In A. Puliafito, D. Bruneo, S. Distefano, & F. Longo (Eds.), *Ad-hoc, mobile, and wireless networks. ADHOCNOW 2017. Lecture Notes in Computer Science.* (Vol. 10517). Springer. https://doi.org/10.1007/978-3-319-67910-5_6
33. Mayzaud, A., Sehgal, A., Badonnel, R., Chrisment, I., & Schönwälder, J. (2014). A study of RPL DODAG version attacks. In *8th IFIP international conference on autonomous infrastructure, management and security* (AIMS), Brno, Czech Republic (pp. 92–104). https://doi.org/10.1007/978-3-662-43862-6_12
34. Perkins, C., & Das, S. (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing*. Network Working Group.
35. Xin, H.-M., & Yang, K. (2015). Routing protocols analysis for Internet of Things. In *2015 2nd international conference on information science and control engineering*. https://doi.org/10.1109/ICISCE.2015.104
36. Sharma, R., & Sharma, P. (2016). Detection and prevention of wormhole attack in MANETs: A review. *International Journal of Science, Engineering and Technology Research (IJSETR), 5*(5).
37. Gupta, S., Kar, S., & Dharmaraja, S. (2011). WHOP: Wormhole attack detection protocol using hound packet. in *Proceedings of IEEE international conference on innovations in information technology* (pp. 226–231). https://doi.org/10.1109/INNOVATIONS.2011.5893822
38. Khan, F. I., Shon, T., Lee, T., & Kim, K. (2013). Wormhole attack prevention mechanism for RPL based LLN network. In *Proceedings of fifth international conference on ubiquitous and future networks* (pp. 149–154). IEEE. https://doi.org/10.1109/ICUFN.2013.6614801
39. Ji, S., Chen, T., Zhong, S., & Kak, S. (2014). DAWN: Defending against wormhole attacks in wireless network coding systems. In *Proceedings of IEEE INFOCOM* (pp. 664–672). https://doi.org/10.1109/INFOCOM.2014.6847992

40. Arai, M. (2015). Reliability improvement of multi-path routing for wireless sensor networks and its application to wormhole attack avoidance. In *Proceedings of ubiquitous intelligence and computing and 2015 IEEE 12th international conference on autonomic and trusted computing and 2015 IEEE 15th international conference on scalable computing and communications and its associated workshops* (pp. 533–536). https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.108
41. Acharjee, T., Borah, P., & Roy, S. (2015). A new hybrid algorithm to eliminate wormhole attack in wireless mesh networks. In *Proceedings of IEEE international conference on computational intelligence and communication networks (CICN)* (Vol. 157, pp. 997–1002). https://doi.org/10.1109/CICN.2015.198
42. Zheng, J. H., Qian, H. Y., & Wang, L. (2015). Defense technology of wormhole attacks based on node connectivity. In *2015 IEEE international conference on smart city/SocialCom/SustainCom together with DataCom 2015 and SC2 2015*. https://doi.org/10.1109/SmartCity.2015.107
43. Sharma, M. K., & Joshi, B. K. (2016). A mitigation technique for high transmission power based wormhole attack in wireless sensor networks. In *IEEE proceedings of international conference on ICT in business industry & government* (pp. 1–6). https://doi.org/10.1109/ICTBIG.2016.7892698
44. Lai, G. H. (2016). Detection of wormhole attacks on IPv6 mobility-based wireless sensor network. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 274. https://doi.org/10.1186/s13638-016-0776-0
45. Bendjima, M., & Feham, M. (2016). Wormhole attack detection in wireless sensor networks. In *Proceedings of IEEE SAI computing conference* (pp. 1319–1326). https://doi.org/10.1109/SAI.2016.7556151
46. Patel, M., & Aggarwal, A. (2016). Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information. *International Journal on AdHoc Networking Systems (IJANS), 6*(1), 1–10. https://doi.org/10.5121/ijans.2016.6101
47. Johnson, M. O., Siddiqui, A., & Karami, A. (2017). A wormhole attack detection and prevention technique in wireless sensor networks. *International Journal of Computer Applications, 174*(4), 1–8. https://doi.org/10.5120/ijca2017915376
48. Tiruvakadu, D. S. K., & Pallapa, V. (2018). Confirmation of wormhole attack in MANETs using honeypot. *Computers & Security, 76*(32–49), 158. https://doi.org/10.1016/J.COSE.2018.02.004
49. Qazi, S., Raad, R., Mu, Y., & Susilo, W. (2018). Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks. *Journal of Information Security and Applications, 39*, 31–40. https://doi.org/10.1016/j.jisa.2018.01.005
50. Luo, X., Chen, Y., Li, M., Luo, Q., Xue, K., Liu, S., & Chen, L. (2019). CREDND: A novel secure neighbor discovery algorithm for wormhole attack. *IEEE Access, 7*, 18194–18205. https://doi.org/10.1109/ACCESS.2019.2894637
51. Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). Detection of security attack in IoT using received signal strength indicator. *Helix, 9*(3), 5042–5045. https://doi.org/10.29042/2019-5042-5045
52. Li, X., Shi, H., & Shang, Y. (2005). A sorted RSSI quantization based algorithm for sensor network localization. In *11th international conference on parallel and distributed systems (ICPADS'05)*. IEEE. https://doi.org/10.1109/ICPADS.2005.53
53. Lee, T.-H., Xie, X.-S., & Chang, L.-H. (2014). RSSI-based IPv6 routing metrics for RPL in low power and Lossy networks. In *IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE. https://doi.org/10.1109/SMC.2014.6974164
54. Shojaifar, A. (2015). *A thesis on evaluation and Improvement of the RSSI-based localization algorithm*. Faculty of Computing Blekinge Institute of Technology SE-371 79 Karlskrona Sweden.
55. Osterlind, F. (2006). *A sensor network simulator for the Contiki OS*. Swedish Institute of Computer Science (SICS), Technical Report T2006-05.
56. Eriksson, J., Österlind, F., Finne, N., & Tsiftes, N. (2009). COOJA/MSPSim: Interoperability testing for wireless sensor networks. In *2nd international conference on simulation tools and techniques*, Rome, Italy (p. 7). https://doi.org/10.1145/1537614.1537650
57. https://www.fierceelectronics.com/iot-wireless/mica-commercialization-microsensor-motes. Accessed on July 2018.
58. http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/Tmote-sky-datasheet.pdf. Accessed on July 2018.
59. Dunkels, A., Eriksson, J., Finne, N., & Tsiftes, N. (2011). *Powertrace: Network level power profiling for low-power wireless networks*. SICS Technical Report T2011:05, ISSN 1100-3154.

60. Shahid, R., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks, 11*(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Dr. Mrs. Snehal A. Bhosale completed her Ph.D. at SPPU, Pune, Maharashtra, India. She is working as Asst. Professor, E&TC Dept, RMDSSOE, Pune. She has published more than 30 research papers in national and international journals. She has also published two patents on her research work. She has received best paper awards twice in International Conferences. She has more than 18 years of experience in the field of education. To fulfill the work of PhD, Mrs. Bhosale with her guide has developed an Intrusion Detection System (IDS), using the Contiki OS and the Cooja Simulator. They obtained optimum results based on throughput, delay and attack detection in terms of positive and negative attack detection. Her research areas are Wireless Communication, Wireless Sensor Network, Internet of Things and Data Analytics.

Dr. S. S. Sonavane Pro-Vice Chancellor, Vijaybhoomi University, Karjat, Navi Mumbai, Maharashtra, India. He has 20 years of experience in the field of education and has served in many well-known organizations. He is a successful academician and has published 2 books internationally (Austria and Germany). He had more than 75 International and National publications on his name in reputed peer Reviewed Journals. He has published more than 5 patents on his name. He is a registered Ph.D. guide in SPPU, Pune. He is also a reviewer of many Electronics International Journals including IEEE Sensor Journal and IEEE Communication Letters. He had successfully completed two Research Projects funded by University of Pune. His Research areas are Wireless Sensor Network and Internet of Things.