Retraction Notice

Title of retracted article:	**Isolating Wormhole Attack in Wireless Sensor Networks**
Author(s):	L. Thanga Mariappan*, K. Rubasoundar
* Corresponding author:	Email: thangamariappanme@gmail.com
Journal:	Circuits and Systems (CS)
Year:	2016
Volume:	7
Number:	8
Pages (from - to):	2036 - 2046
DOI (to PDF):	http://dx.doi.org/10.4236/cs.2016.78177
Paper ID at SCIRP:	67793
Article page:	http://www.scirp.org/journal/PaperInformation.aspx?PaperID=67793
Retraction date:	2018-08-06

Retraction initiative (multiple responses allowed; mark with **X**):

☐ All authors
X Some of the authors:
☐ Editor with hints from
- ○ Journal owner (publisher)
- ○ Institution:
- ○ Reader:
- ○ Other:

Date initiative is launched: 2018-07-31

Retraction type (multiple responses allowed):

☐ Unreliable findings
- ○ Lab error
- ○ Inconsistent data
- ○ Analytical error
- ○ Biased interpretation
- ○ Other:

☐ Irreproducible results
☐ Failure to disclose a major competing interest likely to influence interpretations or recommendations
☐ Unethical research

☐ Fraud
- ○ Data fabrication
- ○ Fake publication
- ○ Other:

☐ Plagiarism
- ☐ Self plagiarism
- ☐ Overlap
- ☐ Redundant publication *

☐ Copyright infringement
- ☐ Other legal concern:

☐ Editorial reasons
- ○ Handling error
- ○ Unreliable review(s)
- ○ Decision error
- ○ Other:

X Other: CS does not meet author's publication requirements

Results of publication (only one response allowed):

X are still valid.
☐ were found to be overall invalid.

Author's conduct (only one response allowed):

☐ honest error
☐ academic misconduct
X none (not applicable in this case – e.g. in case of editorial reasons)

* Also called duplicate or repetitive publication. Definition: "Publishing or attempting to publish substantially the same work more than once."

History
Expression of Concern:
☐ yes, date: yyyy-mm-dd
X no

Correction:
☐ yes, date: yyyy-mm-dd
X no

Comment:
Circuits and Systems (CS) does not meet author's publication requirements.

This article has been retracted to straighten the academic record. In making this decision the Editorial Board follows COPE's Retraction Guidelines. Aim is to promote the circulation of scientific research by offering an ideal research publication platform with due consideration of internationally accepted standards on publication ethics. The Editorial Board would like to extend its sincere apologies for any inconvenience this retraction may have caused.

Circuits and Systems, 2016, 7, 2036-2046
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78177

Isolating Wormhole Attack in Wireless Sensor Networks

L. Thanga Mariappan, K. Rubasoundar

Department of Information Technology, Sree Sowdambika College of Engineering, Aruppukottai, India
Email: thangamariappanme@gmail.com

Received 18 April 2016; accepted 26 April 2016; published 29 June 2016

Abstract

Wireless sensor networks (WSNs) are inclined to pretenders or challenger as they are persistently positioning the nodes in regular environments. The assailants can straightforwardly obtain unenthusiastically decisive information and in addition it accomplishes a number of malfunctions also. There are a number of precarious attacks and critical distortion in wireless sensor network. One of the widely held and unadorned attacks in wireless sensor networks is wormhole attack. This paper scrutinizes the developmental action of wormhole attack in wsn and studies the enactment of prior strategies of guarding mechanism available and then recommends intelligent based mechanism with the succor of QoS parameters. The contemplation of suggested mechanism is the observation of QoS parameter considerations between succeeding nodes in the network and those nodes obtained parametric assessment value which is compulsory necessitate to relate those values of other succeeding nodes with the support of swarm agents. The manifestation of wormhole attacks is recognized based on the two phase mechanisms. The principal strategy is that relates QoS parameter between succeeding nodes in the network, the nodes which are compromised by wormhole attack nodes are substantially larger than those between two standard nearest neighbor nodes with the assistance of sophisticated swarm agents. The additional strategy for perceiving wormhole attack is depending on the circumstance that accomplishes the enactment of agent nodes within its communication or transmission range by initiation of fresh connection links into the network. This strategy does not care about any unambiguous hardware, has greater performance, least overhead and also does not consume extra power. The proposed mechanism is modeled with an assistance of the AODV routing protocol, exploration and simulations of the proposed mechanism are carried out using the network simulator (ns-2).

Keywords

AODV, Swarm Agents, Wormhole Attacks, Wireless Sensor Networks

How to cite this paper: Mariappan, L.T. and Rubasoundar, K. (2016) Isolating Wormhole Attack in Wireless Sensor Networks. *Circuits and Systems*, **7**, 2036-2046. http://dx.doi.org/10.4236/cs.2016.78177

1. Introduction

Nowadays, Wireless Sensor Networks are getting higher interaction with a wide range of application, most of the areas including military, dweller environments. The establishment of wireless communications is open link and due to lack of infrastructure, the network communication becomes the toughest challenge for the users, in case of critical and emergency need of deployment practices, and the insistent surroundings where the sensor nodes may be positioned having very low contemplation of safety measures, make the sensor nodes prone to a various threads to wireless sensor networks. Wormhole attack is one amongst the most of the cruel attacks for the reason that this wormhole attack does not initiate massive amount of congestion into the wireless sensor network. Wormhole attacks mainly focus on routing because it damages the route and bamboozles the routing protocols to get the knowledge of the route.

The wormhole attacks in wireless sensor networks build a tunnel with the assistance of the malicious nodes and it eavesdrops the encapsulated packets from one network position to a some other location in the same network that is a node which is distant from the deployed position or to another network and retransmitted data to build a phony neighbor relations with the original genuine nodes in the wireless sensor network, and as a result, it damages the routing strategies completely and deteriorates the security techniques in the routing methodologies [1] [2]. Supposing in a network, there are two or more wormhole malicious nodes that may present, lead to the data loss by the phony neighbor relations and get incoherent from the original network, because there may be a possibility of data drops which are proportional to the data transmitted, which nearly one out of two packets get drops because of a phony neighbor relations. Therefore the additional concentration is required to smell the existence of wormhole attack in the network and also keep on focus for preventing such a type of crucial attacks from the network [3]. A variety of techniques are available that have been taken into account and examined, in association with wormhole attacks in wireless sensor networks. The existing strategies mainly concentrate on predicting the occurrence of a wormhole attack in the wireless sensor network and also try to eradicate such type of attacks from the network, but still no other strategies that completely flush out the occurrence of wormhole attacks. Here we recommend a mechanism for smelling the presence of wormhole attack based on the QoS parameter. Here we consider the transmission time and with the assistance of neighbor relation nodes and the routing table information, we can easily detect and spot out the prevalence of wormhole attacks with the support of swarm intelligence network and routing protocol (AODV). Here the time of transmission (QoS Parameter) is considered and trained to swarm network which periodically monitors the network, whether any additional node is introduced in the network within an unambiguous range and a bureaucrat node monitors the each and every swarm node in the network within its radius up to which its signal reaches [4]. This method helps to predict and segregate the occurrence of a wormhole attack at the instant of route setup process with the calculating time of data exchange between two successive neighboring nodes from all the way through the route which has been already connected with the neighboring nodes. It is taken into account that there are two traces for finding the occurrence of worm attacks. The first strategy is that communication time between two successive nodes which have been compromised by the intruder that is from the malicious or wormhole node is drastically greater than the communication time between two legitimate or unaffected adjacent nodes. Then next step is that wormhole links that build two or more new edges and result in increasing the number of neighbors surrounding the malicious nodes. The proposed mechanism does not require any specialized hardware to find out the presence of wormhole attack, the synchronous monitoring is not required and also the computational overhead is considerably very low and because it should not use more power for finding the presence attack, hence it will manipulate the time to live of the nodes in the networks.

2. Wormhole Attacks

The wormhole attacks that mean a malicious node that construct a tunnel and frontward the data packets acknowledged from one terminal of the network connection and replay the similar packets in a remote spot of the network itself or else to an additional network which may be near or remote location. The tunnel is able to be built by means of different methodologies, such as through a wired connection, the data packets are encapsulated within it, or the messages are broadcasted. The tunnel that creates the sagacity or building a virtual mean that the passage linking the nodes are in very close proximity to it, and as well as by persuading tunneled data packets arrive at destination node very promptly otherwise it demonstrates that a smaller amount of hops measured up to the messages that will arrive at the target through the usual path. This tolerates the intruders to con-

front the precise progression of the routing protocol, by monitoring different path in the network. Later than that, the challengers carry out a data transfer examination or it plunges data packet due to congestion. In a wireless sensor network the wormhole attacks that mainly intent on the attacks commonly in the network layer and the three-tunnel building for the wormhole attack strategies that follows:

1) In the network layer it tunnels the packet over the routing protocol.

2) Encompassing the limited area of communication of the tunnel with the assistance of more supremacy transmitters.

3) Building the tunnel through wired infrastructure.

Wormhole tunnel creates possible to the quantity of bouts in against to generation of keys and the routing protocols. The challengers try to get the governing process of the connection and at once the monitoring process gets weakens and the control switched to the challengers, they know how doing any kind of maneuver easily to dislocate the route in the network. In common wormhole attack can sway the routing strategies in other words the routing protocols and data aggregation, and wireless safety measures techniques depends on the positioning. The challengers responsible for wormhole attack will not generate any isolated packets; they simply replay the prior packets which are forwarded on the route arrived from the untrusted network, and it deviates or diverts some cryptographic techniques. The Challengers or attackers are needed not to worry about the routing protocols, routing strategies or cryptographic techniques for creating the wormhole tunnel. After the creation of Wormhole links between the nodes that gives toughest challenge to cryptographic technique to detect and prevent the wormhole attack. As a consideration that it is very important that sentry the nodes of wireless sensor network from the wormhole attacks successfully.

3. Related Work

In the wormhole attack, the challenger gets hold of the information from one end or at a specific position in a network, tunnels that data to some other position in the network itself or sometimes which is too distant away from the same network or to different or independent network, and later on it begins replays those messages in it [5]. To take care for the messages or data or nodes or links in a network from wormhole attacks, some strategies have to be built and designed with the hardware design and signal indulgence strategies. The information bits are relocated with connecting the nodes in the network and are revised using some exceptional strategies that information is known to the specific location and it is shared with the neighbor, which are very confront to wormholes [6]. Another plausible technique [7] is to include all deterrence strategies into systems. It also affords the high degree of confront for the challengers to adjust with untrust worthy nodes, those nodes deal with a software only approach. More often than that not all the strategies that follows common security techniques proposed so for detecting and averting the wormhole attack with routing protocols are a smaller amount of existence to wormhole attacks. Despite the fact that, the wormhole attacks that gives toughest challenge to the network against network security, but the abolition of wormhole attack from the network is very complicated for the researchers.

Processes implemented to isolate the data packets arriving or moving from distant locations than a radio transmission circle or communication range referred as packet leashes [8]. The existence of wormhole attack can be observed by parametric values by a physical metric, such as data packet delay occasion or physical locality of the node. It isolates the occurrence of wormhole attacks by limiting the maximum distance of broadcasting the information, using either by synchronization of points with respect to time or data positioning. This packet leash that gives security to the packet has a next top hop on its subsistence. When a node forwards a data packet to the target node or end node, the forwarded data packet encompasses of time which it how long the packet travels in the network, and the target node poise this obtain value to the threshold value. It requires that the clocks to be synchronized continuously this is the disadvantage of this process [9]. The Packet leash respect to geographical that gives the assurance that the data transferred between sender and receiver are in limited mode that is within a predictable remoteness. The data packets include the position of the data forwarder and the instances in which it forwarded. When the data packet reaches the target node, the target or receiving or destination node computes the distance between the data forwarder and a data receiver [10]. Location of the data packets and clock synchronization is used to authenticate the performance of a neighbor node. The shortcoming of this strategy is that, every node must be recognizable by its position and the nodes in the same network, which are in close proximity to it must have clocks synchronized. For the reason that synchronization of clock is challenging the resources

and as a result packet leashes have constrained usability in wireless sensor networks [11].

A methodology [12] was designed based on packet leashes, however, in that strategy, it contracts with node to node position information; all nodes in the network attached to its arrangement and the packet life duration, and defends this information with a verification technique. The receiving target node of the data packet authenticates the nodes synchronize the transmission range of the transformation of the packet and its momentum. A small shortcoming of this strategy is that the end node is mislaid to perform all verification. Same as like geological packet leashes, this approach is better for detecting and preventing the wormhole attack.

Another approach called SECTOR [13] in that dedicated hardware were used which make possible rapid transfer of data packets without the assistance of CPU, as to diminish all feasible dispensation delays. This strategy exploits a remoteness-routing algorithm to compute the remoteness between the source and destination. It can be used to segregate wormhole attacks in the network without necessitates clock synchronization or spotting information. To segregate wormhole node [14] have to compute Round Trip Time of a data packet and its acknowledgement from the receiver, computes the remoteness between the target nodes relates to this duration of packet life time or travel time, and an approximation whether the practically estimated remoteness is within the maximum feasible radio transmission range. To validate remoteness between the source and destination nodes, nodes in the network forwards a hello test message to the neighbor nodes in the network, and waits for an acknowledgement. A final target node instantaneously replies an acknowledgment reply to the receiver. An additional strategy for preventing wormhole attacks, closely related to temporal packet leashes strategy, is based on the data travel duration or packet lifetime of each packet in the network. Wormhole attacks are not yet completely flushed out from the network and there is feasible for the reason that a challenger can create more than one distant remote nodes recognize that node as nearest node [15].

In our projected technique the revealing of wormhole attacks that will not depend on any type extraordinary hardware and superfluous information. The projected technique focuses only on the Round Trip Time of route entreaty and retorts of data packets and the numbers nearest nodes of the suspected nodes. This technique is expounded in detail in the following section.

4. Proposed Mechanism

In this section, concentrate on the detection of the wormhole is discussed in detail.

4.1. The System Design and Considerations

Prior to starting approaching with this technique in ornately, devise the backgrounds and constructing a quantity of contemplation should be clearly explained. Let we taken into an account that the total quantity of nodes implemented in the network attain the analogous nature of hardware and software provisions, proportioned (node in the network be able connect with a nearest node in the network if and only if the same node to communicate them in vice versa), and stagnant (nodes that are deployed in the network that remains stable that is the pedestrian movement is set to zero based on ITU-T recommendation roam after deployment). The total numbers of nodes present in the network are distinctively characterized. To identify the existence of a wormhole attack in the network is based on the Round Trip Time of the message between two succeeding nodes and their nearest number of neighbors. At this stage the postulation is to facilitate the pretender a node enhances the link between the number of neighbor nodes within the contentious area, confiscate the path and intensifications the Round Trip Time value between succeeding nodes. This proposed technique comprises of three junctures. The preliminary step is to build the routing table which contains the information about the list of nearest nodes for every single node and the ensuing step is to define the itinerary between sources to the destination node. Later on that it takes certain critical action to envisage the locus of wormhole link. By the side of initial implementation the nodes, the wireless sensor network participates in a process of searching nearest neighbor route and this output of this stage illustrates extensive information's of the nearest node in the network, sensor node and transmission path. Afterwards, the sensor network accomplishes a correct and optimized routing protocol therefore the source nodes are ready and are able to frontward messages to their accurate target location. For this similar kind of process, have need of discovering the performance of the routing protocol potentials. For the reason that node in the network is accomplished in cooperation of send and receive operations, this process must be educated to intelligent proxy nodes with routing information thus observing node that is data packet transfers exactly to supplementary nodes.

4.2. Construction of Neighbor Node List

After making all preliminary phases this step is the initial deployment stage, all nodes in the network broadcast the Route Entreaty to Nearest Node (RENN) message. Riposte to RENN from the delivery node concede to the REQN as a Reply from a neighbor (REPN) message. Based on the REPN messages, the node which sends the RENN build the itinerary and sum the total number of nearest nodes (NeN).

4.3. Determination of Route

At this moment, the practices that preceding point that is the source node having an authority for building the itinerary which comprises the hierarchical routing tree to the further nodes in the network or sensor field. The source node on the Route Entreaty (RoEn) message to the nearest nodes excludes the period of its forwarding (Destination) DReq. The transitional node also frontwards the RoEn message and saves DReq of its transfer duration. At the time of the RoEn message reaches the target node, it propels route riposte message (RoRi) with the restraint path. When the transitional node gets the RoRi message, it saves the duration of receiving RoRi DRep. The consideration is based on the Round Trip Time of the route entreaty and riposte.

The Round Trip Time can be calculated as

$$\mathrm{RTT} = \mathrm{DRep} - \mathrm{DReq}\ . \tag{1}$$

All transitional nodes load this information and later on frontward it back to the source itself.

4.4. Detection of Wormhole Attack

In this juncture, the transmitter computes the Round Trip Time of entire nodes in the path that is intermediary, also itself and the final target. It computes the Round Trip Time of succeeding nodes and relates the assessment to examine the presence of wormhole node in the network or not. This must be educated to intelligence agent node. If the nodes in the network are unrestricted from attack, then the computed assessment of Round Trip Time is approximately the same. If the Round Trip Time assessment diverges exceedingly when related to other succeeding nodes in the network, it can be virtually as a wormhole attack between this connection of node or network.

The ensuing revealing strategy depends on the circumstance that by making known to the fresh network acquaintances into the network graph, the antagonist helping hand up for an increasing number of neighbor nodes within its communication area or range. Thus, it needs to test the number of nearest nodes (NeN) of these two adjacent nodes.

The following equation evaluates he mediocre number of nearest node mn. It is verging on as

$$\mathrm{mn} = (\mathrm{Nno} - 1)\pi(\mathrm{tr})^2 / \mathrm{TrA} \tag{2}$$

where TrA is the communication range of the sensor nodes, Nno is the total number of nodes in the network, which are in between transmission region and tr is the corporate transmission circle. For case in point, if the Round Trip Time assessment between the nodes Beg to Tar is substantially higher when compared with other connection, it prerequisites to evaluate the assessment of number of nearest for Init and Nex. If also the NeN assessment for Beg and Tar is higher than the mediocre nearest number of nodes mn, there is a qualm that may be a fortuitous of wormhole connection in between nodes Beg and Tar. In this consideration the strategy can pinpoint the existence and locus of the wormhole attack.

4.5. Calculation of RTT

In this division, the meticulous computation of the Round Trip Time is enlightened. The assessment of Round Trip Time is deliberate as the periodic interval variance between RoEn of the initiator and RoRi of the destination. In the course of route operation technique, the interval of forwarding RoEn and receiving RoRi is demonstrated in **Figure 1**. Like this case, every single node in the network will curtail the duration of packet travel that is they frontward RoEn and the period at which they receive RoRi from the endpoint to estimate the Round Trip Time.

Given all Round Trip Time assessment between nearest neighbor nodes in the path and the destination, Round Trip Time between two succeeding nodes, Init and Nex can be evaluated as follows:

$$RTT_{Init,Nex} = RTT_{Init} - RTT_{Nex} \quad (3)$$

where RTT_{Init} is the Round Trip Time between the starting intermediate node (Init) and the target node(Tar), RTT_{Nex} is the Round Trip Time of node (Nex) and the target node(Tar).

For consideration, the path from starting place node (S) to the final target node (R) get ahead of through different nodes here, **Figure 2** elucidates passes via the nodes A, and B therefore which routing path includes:

$$Beg \rightarrow Init \rightarrow Nex \rightarrow Tar$$

And the Round Trip Time assessment between two succeeding nodes lengthwise the path will be expressed with the assistance of an Equation (3):

$$RTT_{Beg,Init} = RTT_{Beg} - RTT_{Init}$$

$$RTT_{Init,Nex} = RTT_{Init} - RTT_{Nex}$$

$$RTT_{Nex,Tar} = RTT_{Nex} - RTT_{Tar}.$$

Under customary circumstances, $RTT_{Beg,Init}$, $RTT_{Init,Nex,}$ $RTT_{Nex,Tar}$ are analogous assessment in communication circle. If there is a wormhole connection between the nodes connected in shortest path, the RTT value may significantly shows better variance than other succeeding Round Trip Time assessment and anticipated that there may be a possibility of existence of a wormhole connection between these two nodes.

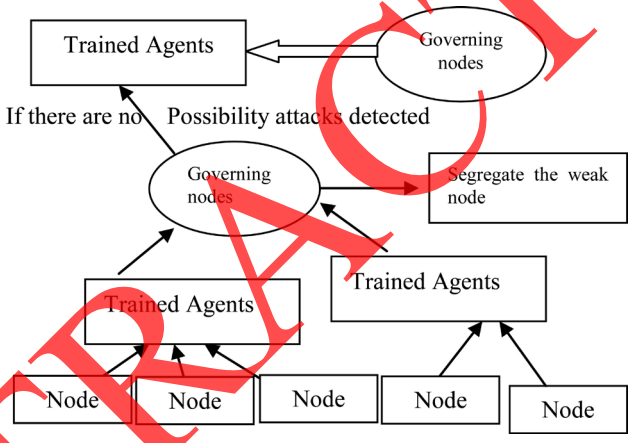

Figure 1. Basic strcutural illustration to perceive wormhole.

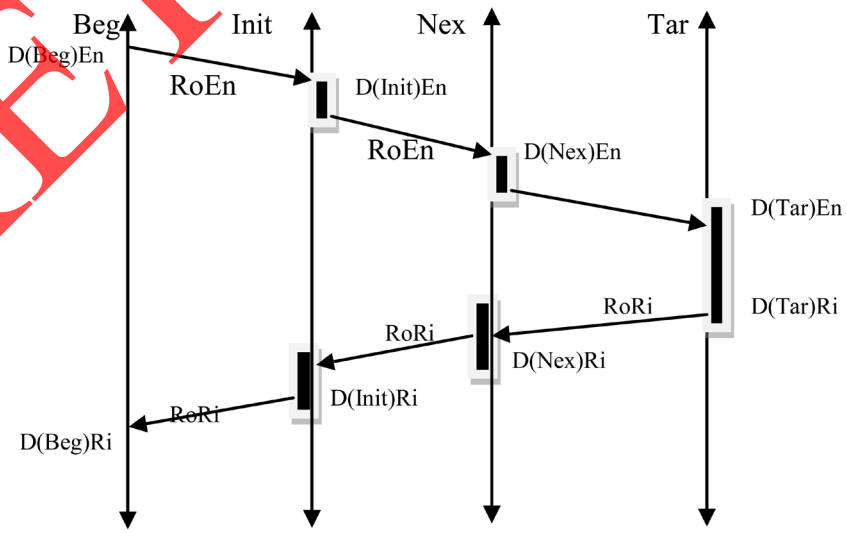

Figure 2. Time for RoEn forward and RoRi accept.

4.6. Swarm Scrutinization

In this section we propose some security related strategies will be rummage-sale, an independent node that is decentralized agent will act as a swarm agent it should be educated with the quality of service parameters, In our experimental setup we considered these agents will act as access points and educated with Round Trip Time concept, and it governs the nodes existent in the wireless sensor network.

For a duration these Security Agents SA will automatically change the QoS parameters randomly as it trained and it should be share the information gathered with legitimate nodes through key exchange algorithm. And after that an another node will act as a centralized node Security officer node (SON) is used at this time to govern the security Agents. There may be a possibility of compromising the security agents by the intruders. So safeguarding the network again by adding extra measure for SON is used to govern the SA.

4.7. Prevention by Path Selection Algorithm

The defenseless nodes can be simply perceived by the prior strategies after discovering the wormhole attack, we should lump the conduit through which the attack exists, for that consideration we used path selection algorithm for that precise challenging node.

1) For the duration of the time interval k, a frequency bandwidth demand bd arrives between successive nodes.
2) Execute the obtainable frequency bandwidth approximation algorithm connection with no bandwidth estimation available.
3) Calculate the finest route using the shortest as well as an optimized path algorithm with loads as evaluated in step two.
4) Acquire the accessible frequency bandwidth N on the bottleneck connection of the traveling link that is the path or route.
5) If bd > (N ∗ threshold), throw away this path and come back to step 3. Or else, footpath is nominated for the request.
6) If there exists no path, request is rejected and the network gets congested.

At last the wormhole attack will be isolated from the wireless sensor network.

5. Simulation and Results

In this fragment, the recitation of the designed technique is appraised using a simulator tool (ns2). In this experiment, the network structure includes 40 homogenous nodes deployed indiscriminately in a field of thousand square meters and the diffusion range of signal are defined for around 250 meters. All the nodes are stagnant and the backdrop congestion is spawned indiscriminately by a random initiator provided by network simulator. The CBR acquaintance with the data rate of 4 packets is formed and the range of the data transfer is 512 bytes. In the design model, more than one wormhole nodes are introduced.

At this point, **Table 1** is prerequisite to derived to a supposition that the two assessments, NeN and RTT, as threshold Assessment value. In the initial assessment, The value of NeN is superior than paired times than the middling neighbor number, it may result to intensify in false negative and at the time of NeN smaller than 3/2 times of the middling neighbor number, it is raised to intensification positive value. Hence the threshold assessment of NeN is set to permanent, and the checkout the result shows an adequate area of false positive and negative assessment. After that threshold assessment to cogitate is RTT and it is proportionate to false negative rate. To acquire the adequate rate of false positive and negative, the model simulation is designed 1000 times and get the assessment of 50 ms, which is diminishes both false positive and false negative rateios explained in **Table 2**.

Figure 3 gives the degree of discovery also is subject to on the extent of the wormhole, for the reason that both are proportionate to each other that is supplementary the wormhole distance, then lengthier the communication duration between two counterfeit nearest neighbors and the simpler to perceive. In this case, the revealing rate is 100% when the measurement of the wormhole is larger or equal to five.

Memory overhead: Every node in the network necessities to accumulating a neighbor list in the routing table. It is presumed that the uniqueness of a node is sixteen bits and the size of the neighbor list is mn = (Nno − 1) $\pi (tr)^2/TrA$ entries, thus the routing of neighbor list necessitates more than 20 bytes for the loading process is represented in **Figure 4**. To find out RTT, separate individual node desires 8 * mnr bytes memory, where mnr is the highest number of RREQ arrival to the node at the equivalent time and this value depends on the network

Table 1. Network design model parameters and values.

Parameters	Assessments
Starting energy	Eini 1 J/Node
No. of agent nodes	(N) 3,5,7,10,12,15 times the neighboring nodes of source node
Packet size (K)	1 K
Bandwidth (B)	1 Mbits/s
Traffic load	Random.

Table 2. False alarm rate upper bound.

Observation scale j	4	5	6	7
False alarm rate	0.0137	0.0274	0.1065	0.2054

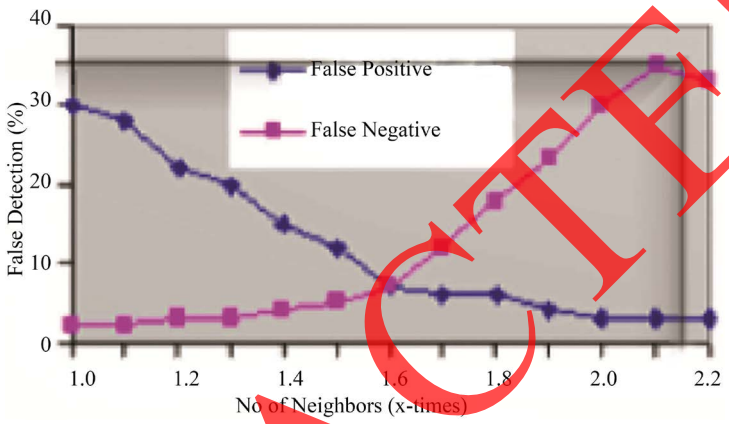

Figure 3. False detection rate vs neighbor rate.

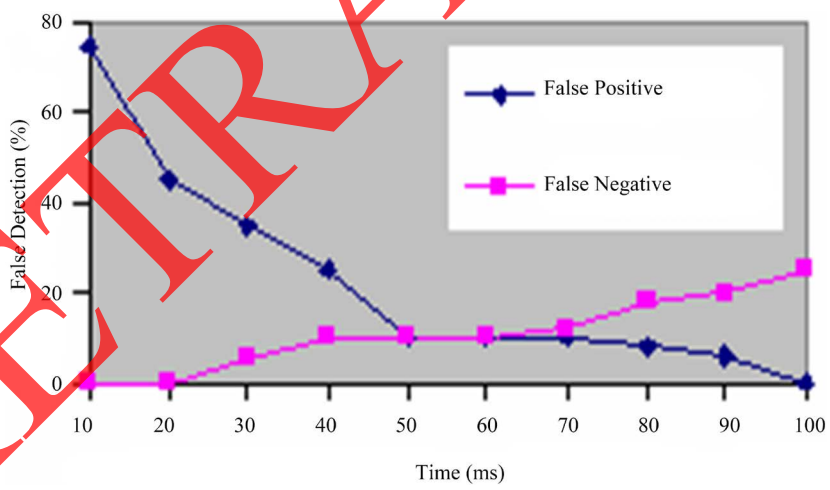

Figure 4. False detection rate vs time threshold.

design and congestion of the network is explained in **Figure 5**. In this condition, set 4 was assigned to *n* and hence respective node requests for 32 bytes of memory to implement the strategy.

Frequency Bandwidth overhead: The frequency bandwidth overhead acquired after implementation of a node for nearest neighbor or optimized route discovery and in the circumstance of wormhole recognition. In all route entreaties in AODV, every node frontward RoEn once and RoRi is progressed by nodes of end to end the conventional route, the size of RoEn is 32 bytes and its RoRi is 20 bytes. But, the simulation necessities the assessment of RTT and adds to the trustworthy route path, and the size of RTT is a 32 bits assessment. The overhead is premeditated as (amount of RREP * span of reputable route) + (amount of RREQ * quantity of node). In the

design model, 40 nodes and space of thousand squares is used so the usual reputable path is 4.57. So ahead of using this strategy the overhead is 1691.48 and later than the overhead increase by 1775.18. So this is illustrated that therefore a unimportant portion of the total bandwidth in excess of the duration of the network for the reason that this overhead occurs only when a fresh itinerary is demanded is shown in **Figure 6**.

Energy consumption: In expressions of power ingestion, the revealing strategies uses smaller power consumption when relates with than prior mechanism, hence the Time to live TTL of nodes in the network greater than the previous strategies. The simulation duration is 1000 s and hence it is enough to 100 J/node for effective network life duration is enlightened in **Figure 7**.

6. Conclusion and Future Enhancement

WSN is an emerging technology, on the other hand, WSN is less prone to various security threats, such as wormhole attacks and fear on intrusion also. This paper offered an intelligence based methodology using swarm intelligence to perceive glitches. In this paper, an investigation of revealing the wormhole attack methodologies is finished and found that to perceive and preclude this attack mainly based on the detailed strength of character of the nearest neighboring information. Most of the discovering methodologies are considered for the nearest neighbor case of the node. The steps for isolating the wormhole attack can be analyzed, designed and

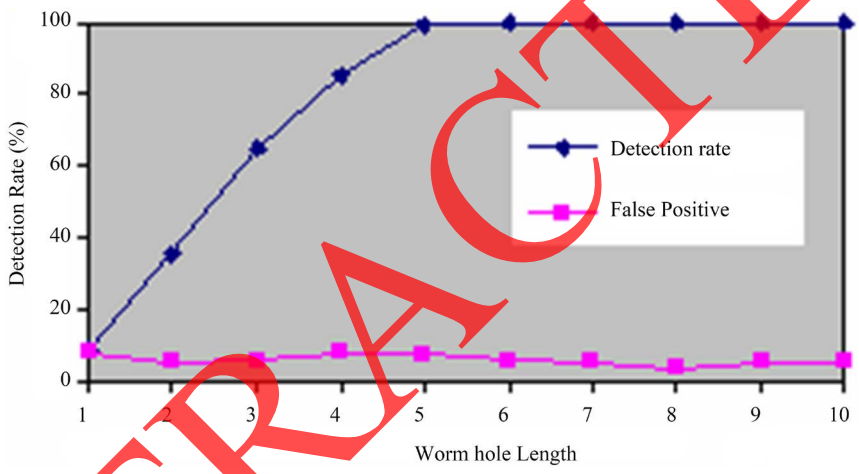

Figure 5. Detection rate.

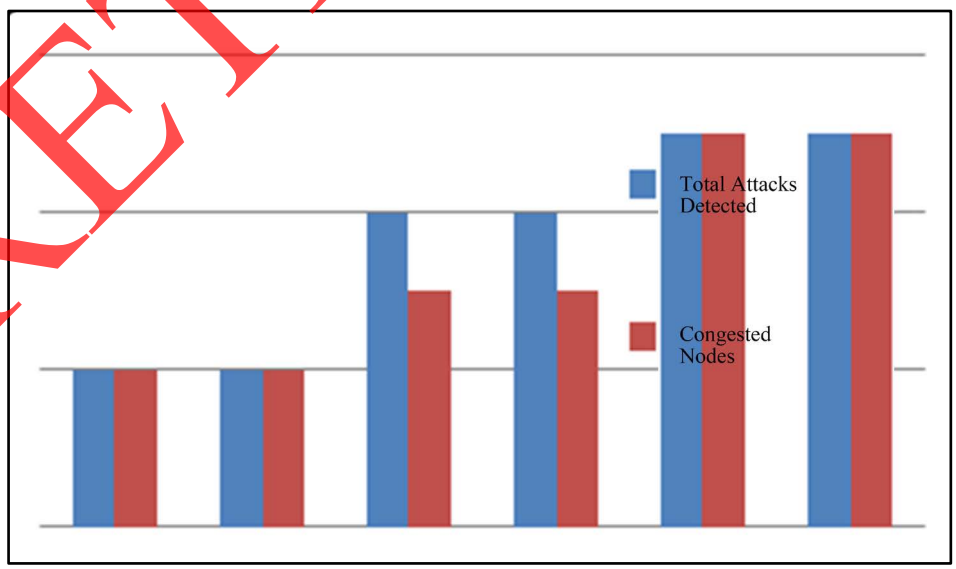

Figure 6. Average detection rate.

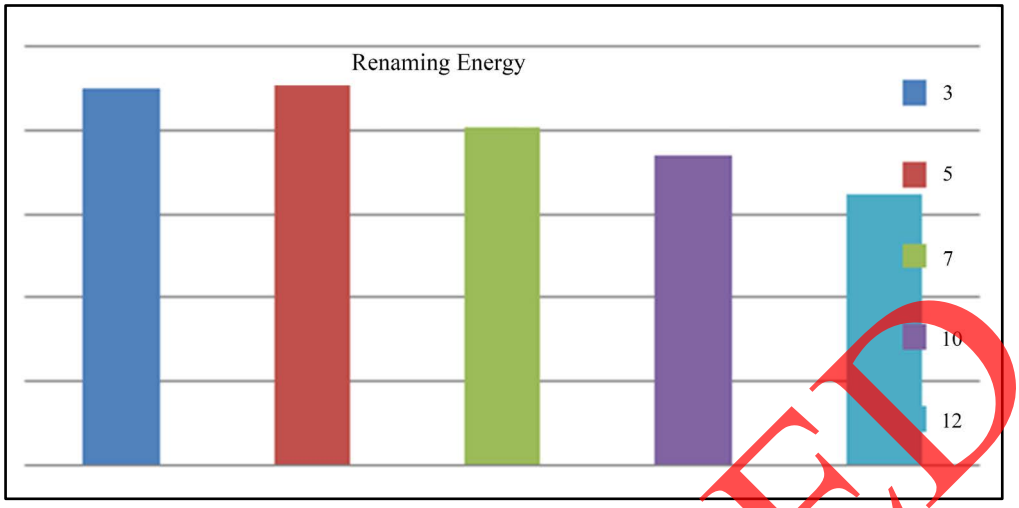

Figure 7. Energy consumption rate.

applied in different layers in the network. For illustration, directional antennas are rummage-sale at the media access layer to assert in contrary to wormhole attacks, and packet leashes strategies are used at a network layer. Since contemporary wormhole detection methods are unsatisfactory, a sensor node will have a lot of phony nearest neighbors below large-scale wormhole attacks. Possessing a number of false, neighbors lead to trouble for many protocols. Some additional determinations are required to brand the perfect neighbor discovery protocols in the detection and isolation of wormhole attacks. So the new mechanism to defend the wormhole attack depends on the Round Trip Time of the routed data packet and the number of neighbor nodes is proposed. The initial deliberations are the Round Trip Time between two succeeding or consecutive nodes and in normal cases and Round Trip Time between two succeeding nodes are closely the same and the next fact is that wormhole nodes may escalate its number of nearest neighbors. The considerable attribute of the proposed technique is that it does not necessitate any precise hardware to spot out the wormhole attacks. This strategy does not necessitate more power consumption than normal and can outspread to other routing protocols than current AODV protocols.

References

[1] Wood, A.D. and Stankovic, J.A. (2013) A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. CRC Press, USA.

[2] Eik, C., Mun, L., Ng, Y., Leckie, C. and Palaniswami, M. (2015) Intrusion Detection for Routing Attacks in Sensor Networks. *International Journal of Distributed Sensor Networks*, **17**, No. 8.

[3] Sankarasubramaniam, A.Y., Sung, W. and Cayiric, E. (2012) A Survey on Wireless Sensor Security. *The Journal of Telecommunications Networking*.

[4] Gupptta, S. (2016) Similar Type Detection in Wireless Sensor Networks. MS Thesis, University of Houstan.

[5] Schonderwoaerd, R., Bruten, J. and Holland, O. (2016) Ant-Like Agents for Load Balancing in Telecommunications Networks. *CM Journal of Information Technology*, **4**, No. 8.

[6] Zhigang, Xi Huei and Xeguang (2012) A Routing Protocol in Wireless Sensor Networks Based on Optimization Technique Ant Colony. *International Conference on Information Application Technology*, University of Canberra, Australia.

[7] Tiranauch, A. (2015) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. In: Wireless/Mobile Networks Security, Chap. 7, Springer.

[8] Aroora, N., Junaeja, D. and Bannsal, S. (2015) An Ant-Based Routing Algorithm for Detecting Attacks in Wireless Sensor Networks. *JCIR*.

[9] Xiao, B. and Yu, B. (2016) Discovering Selective Progressing Attacks in Wireless Sensor Networks. IPDPS, Greece.

[10] Chang, E., Gao, L., Han, S. and Dillon, T. (2013) Taxonomy of Attacks on Wireless Sensor Networks. Springer, London.

[11] Qiaen, D., Chengh, H., Wulfe, W. and Cheng, L. (2016) Energy Balance Routing for Wireless Sensor Networks, Based on Swarm Intelligence. *Second International Symposium on Intelligent Information Technology Application*, USA.

[12] Karlloef, C. and Wangner, D. (2013) Wireless Sensor Network Attacks Secure Routing and Countermeasures. *Proceeding of the IEEE International Workshop on Sensor network Protocols and Applications*, California.

[13] Bahrgav, B. and Wang, W. (2016) Wormholes in Sensor Networks Visualization. ACM Press, New York, NY, USA.

[14] Kar, A. and Kumar, K. (2013) Analysis of Wireless Sensor Network Security. *Journal of Next-Generation Networks* (*JNGN*), **5**, No. 7.

[15] Eberhart Richard, C., Kennedy, J. and Shi, Y. (2015) Swarm Intelligence. Moargan Kaauffmann Publishers, San Francisco.