Dynamic Threshold Method for Isolation of Worm Hole Attack in Wireless Sensor Networks

Surinder Singh[1], Hardeep Singh Saini[2]
[1]Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India.

[2]Professor, Indo Global College Of Engineering, Abhipur, Punjab, India

Abstract:
The moveable ad hoc networks are untrustworthy and susceptible to any intrusion because of their wireless interaction approach. Therefore the information from these networks can be stolen very easily just by introducing the attacker nodes in the system. The straight route extent is calculated with the help of hop count metric. For this purpose, routing protocols are planned. From a number of attacks, the wormhole attack is considered to be the hazardous one. This intrusion is commenced with the help of couple attacker nodes. These nodes make a channel by placing some sensor nodes between transmitter and receiver. The accessible system regards the wormhole intrusions in the absence of intermediary sensor nodes amid target. This mechanism is significant for the areas where the route distance amid transmitter and receiver is two hops merely. This mechanism is not suitable for those scenarios where multi hops are presented amid transmitter and receiver. In the projected study, a new technique is implemented for the recognition and separation of attacker sensor nodes from the network. The wormhole intrusions are triggered with the help of these attacker nodes in the network. The projected scheme is utilized in NS2 and it is depicted by the reproduction outcomes that the projected scheme shows better performance in comparison with existing approaches.

Keywords:
Wormhole, Delay per hop, attacker, MANETs

I. Introduction

A wormhole attack is generally termed as a hard to detect a problem, though it is easily lodged in any wireless adhoc network. An attacker can simply launch a malicious wormhole attack without even having or compromising information about the network or any legal nodes. Most of the prevailing solutions involve special hardware devices or count on making solid postulations to discover vortex wormhole attacks that limit their usability.

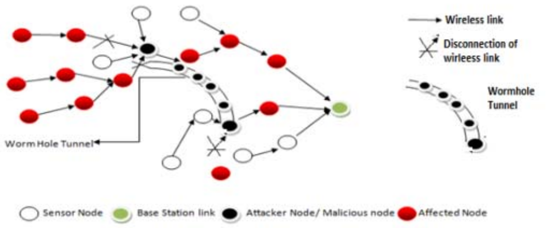

Figure 1: Wormhole Attack In A Wireless Sensor Network.

There are various types of colors circle in figure 1. The white circle is the sensor node not affected by the attack, whereas the red circles are affected nodes by an attacker node. The tiny back circles are the wormhole nodes which created the wormhole tunnel in between the sensor network area. The straight arrow indicates the wireless link, the cross arrow indicates the disconnection of the wireless link and tunnel of the tinny black circle indicates the wormhole tunnel. A one or more malicious node (attacker node) and tunnel between them is created. It creates a shorter path between sensor nodes than the original one which results in confuse routing mechanisms. The delays in processing and queuing processes at each partaking node are also considered while calculating the RTTs between neighbors. As a result of advances in wireless communication, adhoc wireless networks platforms have been reported to gain popularity, regardless of the type of scenario used, particularly when configuring a network infrastructure involves very high costs or is intolerable. The open design of the grids makes them endangered from numerous attacks. These attacks might result in message altering. A message may also behave like another message or the speed of routing may also increase as a result of these attacks (Hu and Perrig, 2004)[1]. Detection and recovery from such attacks often become more challenging as compare to their reinforced complements, as various multi hop wireless surroundings are resource constrained (Khalil et al. 2005)[2]. An example of attack mentioned above is a wormhole attack, that was first stated concerning ad hoc webs (Hu et al., 2006; Wang et al., 2006; Capkun et al., 2003)[3][4]. In it, a

Manuscript received May 5, 2024
Manuscript revised May 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.5.14

mischievous node in the network nets packets from one position and tunnels to some other mischievous node at a remote point, which replays them locally. The tunnel may be launched in a variety of alternative ways as through an out-of-band hidden channel in the form of wired link etc., packet encapsulation, or high-power transmission. This causes the packets (which are tunneled)to arrive before or with a smaller hops count than packets transmitted over standard multi-hop routes. A misapprehension that the two endpoints of the tunnel are nearby taken place as a result. If a wormhole tunnel is to be used for forwarding all the packets, it may be beneficial. Conversely, it is manipulated by violent nodes to weaken the proper functioning of adhoc routing procedures, in its malevolent manifestation. The two mischievous tunnel endpoints can use it to transmit directing movement to fascinate paths through them. Then, they can propel various attacks against the data traffic streaming on the wormhole, for instance, selective declining of the data packets. The wormhole attack can avert two nodes from discerning genuine paths to more than two hops and, therefore, interrupt network functionality. Moreover, this can influence data aggregation and clustering protocols and location-based wireless security systems. Importantly, it should be kept in mind that a wormhole attack can instigate even if any cryptographic keys are not opened. Moreover, any sincere node of the network is not changed (Hu et al., 2006; Wang et al., 2006)[3][5]. During a wormhole attack, our procedure will protect the Dynamic Source Routing in ad hoc grids by calculating the RTT between the nodes, which participate in the path. This procedure also calculates the handling times, which are intricate in all participating nodes while handling path request and path reply packets. Our operating principle differs existing ones (Tran et al., 2007; Alshamrani, 2011)[6][7] by considering the handling time and multi-rate transmission. Detecting a wormhole attack accurately by methods defined for wired networks are not possible in a wireless environment because they presume that the rate of transmission between nodes is constant. The RTT will differ by a considerable amount between the nodes if the links are faster or slower. Thus it cannot be exclaimed that this difference in RTT is due to wormhole or transmission rate.

2. Types Of Wormhole Attack

The four prominent wormhole attacks which are enumerated as under -

2.1 High power communication

2.2 Wormhole channeling by encapsulation

2.3 Wormhole channeling by out of band frequency

2.4 Using packet relay

2.1. High Power Communication Mode

The attacker creates a wormhole just by sending a single malicious node even without the help of conspiring node. On receipt of a route request by a malicious node, it is further broadcast to high power as related to the normal node. Any other node receiving this further redirects it towards the destination. By this, the interjection of nasty node gets established to the main route.

2.2. Wormhole Channeling by Encapsulation

A far distant two or more malicious nodes generates a tunnel between the authorized path create a false illusion that they are the shortest route. This occurs while traversing each node by not increasing the hop count. As a result of encapsulation, the attack is launched amid source and destination.

2.3. Wormhole channeling by out of band frequency

A wormhole channel is created by an out of bound frequency bandwidth among the malicious nodes. Specialized hardware is a must in this type of attack which makes it more difficult as compared to encapsulation mode.

2.4. Using Packet Relay

Even one malicious node can make far away nodes believe that they are neighbors of each other, so we can imagine how long the list of this type virtual neighbors can grow if there is a group of malicious nodes.

3. Related Work

Perkins et al., (2003) [8] proposed a protocol for sensor and Ad hoc networks and that protocol was known as AODV routing protocol. In this protocol, path from node to node is made only when, there is a need to transfer data packets. Discovery and maintenance of the path are the two main operations in this protocol. To find and maintain the paths, Route Reply (RREP), Request (RREQ) and Error (RERR) messages are used. In route discovery, the source node transmits a RREQ packet in the grid, whenever it does not have a path to the destination node and requires one. The source IP address, destination IP address, source sequence number, destination sequence number, request ID and steps count are stored in a RREQ packet. The node will process the route request if and only if, the source address of the request is different from that of former request. The number of destination sequence for the table is then compared with the destination in routing table if the address is present and destination number is increased by 1 and route request is sent if destination is not reachable through that path. Therefore, route freshness is mentioned by the destination number. Whenever a link is broken in an active route, it is notified by the node by sending a RERR message to the source node.

Capkun et al. (2003) [4] stated a wormhole detection method which would not require any synchronization of a dock by using MAD (Mutual Authentication with Distance Bounding). According to this, a node could find an approximate distance by sending one bit to another node, and another node has to respond instantly and using this estimated time of the shoot, the node can also find out that if the other node is its neighbor or not. In this method, special hardware is used that can control the transceiver of the other node, so that there must be no time delay because of processing the message.

Khalil et al. (2005) [2] proposed a simple procedure called LITEWORP. It detects and somehow reduces the effects of wormhole attacks in fixed ad hoc and sensor networks. This measure isolates the nasty node from the grid by providing a countermeasure to it. Wormhole nodes are detected by monitoring the control traffic two step discovery of neighbor is secured. In this procedure, no special hardware is used. Here, negligible bandwidth is over headed so size of the packet is not increased. Wormhole is properly detected and isolated to prevent the nodes to become victim due to false alarms, which the natural collisions and nasty framing does.

Hu et al. (2006) [3] presented that perception of the physical and progressive packet will help in detecting wormhole attacks in wireless networks. It is stated here that, all nodes need to have their lightly synchronized and each node should correctly know its address. The physical strings confirm that the gap in source and receiver should be in certain limits. The maximum travel distance is restricted because the sequential or we can say progressive strings confirms that there must be an upper bound on the lifetime of all packets. Also, all the nodes require to have their clocks tightly synchronized and the time delay in processing of the packets is insignificant. Both the physical and sequential strings need to send verified data to guard the string which in turn, adds the significant overheads of communication. Also, in Merkle (1980), an authentication scheme which was based on hash trees was used, so a great amount of storage is needed at each node.

Khabbazian et al. (2006)[9] postulated two assumptions, the first one being to assume that in a network, there are a lot of dispersed nodes and the second assumption is that the distance between the two nodes is lesser than or equal to the communication range. It also shielded a packet step count by using a botch chain so that the attackers cannot reduce the step count. The work was divided at different levels to examine the position and distance between two genuine nodes. It also helped us to give information about the number of steps between the two genuine nodes. The results show the way to measure the effects of wormhole by using this analytic model. However, this method is not good if the attackers do not care about dropping packets to disturb the network traffic but only analyze the network.

Qian et al. (2007)[10]focuses upon analyzing the routing statistics named as SAM. They say that suspicious links can be excluded whose frequencies are much higher than expected. It can be done in favor of more different pathways by analyzing the group of multipath roads at the base station. The approaches presented here provides us the flexibility when a wormhole changes the path formation which allows much easier allowance to multi-sink scenarios as detection state is indirectly shared. However, extra overheads might reduce it if multi path routing is not required by the application.

Tran et al. (2007) [6], states that TTM detects wormhole attacks TTM on AODV routing method, which is the closest work to the one presented in this paper. RTT can be calculated by subtracting the values of forwarding and receiving times that is calculated between two preceding nodes throughout the path. The sending time is stored as the sender produces the RREQ. The node retransmits the RREQ after processing it as soon as it receives RREQ and then it records its sending time also and so reaches the destination. And then, the RREP produced by the destination is received by each node. At that point, every hub figures its RTT with the goal and appends it to the extra part in RREP which is as of now made by the goal. At the point when the source hub gets the RREP, it triggers the distinguishing procedure to check if the set up path is substantial or not. The source hub will ascertain RTTs between each two progressive hubs along the way dependent on RTT values in the extensional piece of RREP. The creators trusted that if the contrast between the RTTs of progressive hubs is higher than the limit (which they expected 45 s dependent on reproducetion results) esteem at that point there is a wormhole. The handling time which is required for each node is also discussed here, which may change the value of RTT and they proposed a mechanism that measures the RTT several times and then calculates the average value of RTT between two nodes as the authors believes that wormhole can be better detected by considering this average value of RTT. But in actual practice, there is a difference in transmission times because of crowding in the network and also, there is a difference in handling time at different time intervals. Because of these reasons, the average value of

RTT is unable to give better results than calculating single values of RTT.

Znaidi et al. (2008) [11] acquainted another calculation with identifying a wormhole assault by registering some particular coefficients for every hub's neighbors. They accept that every hub gets the rundown of one and two-bounce neighbors. Every hub will send a HELLO message including its character; accordingly every hub which hears the HELLO message must add this hub to its neighboring rundown and afterward send an answer message to the sender of the HELLO message. After this, each node has the neighbor list of its side nodes and the last thing that is going to happen after sharing the neighbor list is the comparison of the received list with its neighbor list and if the other node is having at minimum one node as a common neighbor, then only the node shall be considered as a regular node else, it will be considered as a doubtful node and so, it will be put in the red list and then the former node will broadcast a message that the latter node is a doubtful node and all nodes will receive this attentive message. Then, all nodes will be aware of any suspicious node and the malicious node will be deleted by a node, for which it has received the alert message. So, the result shows that this algorithm efficiently detects the presence of a wormhole.

Dong et al. (2009)[12]proposed a scheme which is based on topological analysis of a wormhole and by watching the unavoidable topology deviations presented by wormholes. Creators labeled the wormholes as indicated by their effect on the system and gave a topological methodology. This methodology exclusively depends on topological data of the system and identifies wormholes by identifying non-isolating circles (sets). They officially demonstrated the rightness of this structure by broadening the constant geometric fields into discrete fields.

Garcia and Robert (2009)[13] presented an adjustment in the Split Multipart Routing (SMR) method (Qian et al., 2007) while proposing a new routing protocol. This new method allows transitional hubs to forward rehashed duplicates of a RREQ message, as long as their jump checks are not bigger than the bounce tallies of effectively gotten duplicates. The destination ought to get various duplicates of the RREQ message. In this manner, the destination ought to have the capacity to make a rundown of accessible paths from the source; this data gives a fractional perspective on the system that would be utilized by the WIM-DSR convention in the revelation of conceivable wormhole assaults. In this convention, the destination picks a path and communicates it towards the source. There should be the retransmission of just a single duplicate of RREQ message by transitional nodes and validation of the information should be allowed to transitional nodes.

Su (2010) [14] proposed a steering convention named WARP which will shield the ad hoc systems during the wormhole assaults. AODV steering convention type is altered by taking link disjoint multi-way directing among source and destination. Here, every hub records every bit of it in neighbor's irregularity esteems (number of times it shapes a way from various source to goal). Because of the wormhole hub's incredible capacity to get directing ways, if the event of one connection surpasses the edge esteem, the two closures of this connection might be wormhole hubs. In the event that oddity estimations of a hub surpass limit esteem, at that point all route forming requests which contain that node in the path will be discarded by its neighbors.

Yu et al. (2010)[15] suggested securing ad hoc networks by Reputation Evaluation based Routing Security Scheme. They considered functions of participating nodes to study the hierarchical ad hoc networks. The connection is worked by the conduct and relationship of the hub. They picked generally secure hubs by notoriety assessment in steering and refresh the notoriety through hubs relationship. This paper guarantees that the AODV directing convention can be used to secure any routing security.

Prasannajit et al. (2010)[16] have introduced an algorithm WRTTGDD, which will calculate the physical distance and RTT. There are two stages of operating this algorithm that is :utilizing a stage checking system and RTT between each progressive hub. At that point, each hub should gather the arrangement of jump checks of its neighbor hubs. Furthermore, the Dijkstra calculation is utilized by every hub to locate the smallest path for each pair dependent on the RTTs and jump tally. Additionally, through multidimensional scaling (MDS), a nearby guide will be recreated. At that point, twists in nearby maps will be recognized by the utilization of a diameter feature (jump tallying). Further, the largest RTT has a place with the fake connection that is made by the assailants, in light of the fact that in an ordinary system without wormholes, the creators guarantee that all the RTTs are almost the equivalent. This technique identifies the wormhole assaults since it gives each hub has huge data about the hubs that can impart legitimately. In spite of the fact that this calculation can recognize wormhole assaults, it isn't expressed how to separate pernicious hubs to dodge future wormhole assault.

Kim et al. (2011)[17] have examined the materialness of existing WSN steering conventions (BVR, MINT GRAB, and ZBR) to military sensor grids through reenactment contemplate in regards to the four execution measurements, for example, bundle conveyance proportion, normal start to finish delay, control parcel overhead and the normal measure of vitality utilization. This work managed just the system lifetime and vitality utilization not identified with the security.

Gandhi et al., (2012)[18] expressed that the execution of the three directing conventions, for example, AOD, DSDV, and ZRP is dissected with differing portable hubs without assault. Execution measurements are normal start to finish Delay, normal jitter, normal throughput, Normalized Routing Load (NRL) and Packet Delivery Fraction (PDF). The reproduction was done in NS2 test system. At long last, it reasons that AODV has preferable execution over DSDV and ZRP.

Goyal et al., (2012) [19] examined and embraced the reenactment based investigation of Ad-hoc Routing Protocols in a remote sensor arrange. This work managed examination of four steering conventions AODV DYMO, OLSR, and IERP, which is finished by utilizing an irregular waypoint portability show and changing the versatility of the hubs utilizing QualNet 5.0.2 test system. The measurements utilized for execution assessment are Average Jitter, Throughput, End-to-End delay, Signals got with mistakes, Average Queue Length and all out parcels got at the collector end.

Ahuja et al. (2013) [20] proposed that the execution of AODV and DSR directing convention under wormhole assault have been assessed. Execution parameters are Average End-to-End Delay, Throughput, and Packet Delivery Ratio (PDR), and reproduction was done in qualnet test system 5.0.

Paul et al. (2014) [21] have displayed as it were, the place steering convention AODV, AOMDV, DSR, and DSDV been broke down by contrasting the diverse execution measurements, for example, Packet conveyance proportion (PDR), Loss Packet Ratio (LPR), and normal start to finish delay with changing respite time and number of hub under TCP and CBR association by means of system test system NS2.35 for remote sensor systems.

4. Packet Transmission Time-Based Technique for Detection Of Worm Hole Attack

The PTT technique detects based on Round trip time. RTT can be calculated between two successive nodes within the route. Every node in the network will calculate the RTT and send back the values of RTT to the sender node. The sender node will store all the values of every possible route within the network and also identify the wormhole tunnel by calculating the RTT of all possible route. The value of RTT for wormhole node will be considerably higher than other RTT values of neighbor's network node as in Tran et al. (2007)[6] A wireless sensor network with eight nodes as shown in figure 1.

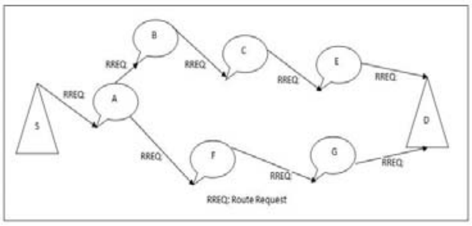

Figure 2: Route Request In Wireless Sensor Network

Every node in the network saves the time while sending an RREQ (Route Reply Request) to its neighbor node. As shown in figure 2 the S node will save the RREQ time while sending the data to a node. Similarly, the A node the value of RREQ time of A node while sending the data to the B node.

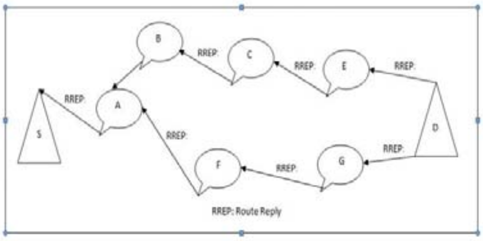

Figure 3: Route Reply In Wireless Sensor Network

Every node in the network received the route reply from the destination node. Figure 3 shows that the D node sending the RREP to the E node while sending the data. Similarly, the E node sends the RREP to the C node while sending the data. By subtracting the RREQ time from RREP time, we will get the RTT. We take an example of Route

S → A → B → C → E → D

The RREP Values for an above route are TS(RREP), TA(RREP), TB(RREP), TC(RREP), TE(RREP) and TD(RREP).

The RREQ Values for an above route are TS(RREQ), TA(RREQ), TB(RREQ), TC(RREQ), TE(RREQ) and TD(RREQ).

Then the RTT values between S, A, B, C,E, and D will be:

RTT(S, D) =TS (RREQ)-TS (RREP)

RTT (A, D) =TA (RREQ)-TA (RREP)

RTT (B, D) =TB (RREQ)-TB (RREP)

RTT(C, D) =TC (RREQ)-TD (RREP)

RTT (E, D) =TE (RREQ)-TE (RREP)

And the RTT values between two successive nodes along with the path will be:

RTT(S, A) =RTT(S, D)-RTT (A, D)

RTT (A, B) =RTT (A, D)-RTT (B, D)

RTT (B, C) =RTT (B, D)-RTT(C, D)

RTT(C, E) =RTT(C, D)-RTT (E, D)

RTT (E, D) =RTT (E, D)-RTT (E, D)

The nodes having greater values of RTT considered to as wormhole node as per Packet Transmission Time-Based Technique

Let us assume the values and it will be shown on following table 1 and values of RTT with Destination

Table 1: Rtt With Destination

Node	TN(RREQ)	TN(RREP)	RTT(N, D)
S	0	34	34
A	0.5	30.5	30
B	3.5	23.5	20
C	8.5	16.5	8
E	10.5	14.5	4

Table 2:Rtt Between Intermediate Nodes

RTT(S, A)	4
RTT(A, B)	10
RTT(B, C)	12
RTT(C, E)	4
RTT(E, D)	4

Under normal situation RTT(S, A), RTT(A, B), RTT(B, C), RTT(C, E) and RTT (E, D) are similar but if there is wormhole link between and any node then nodes having wormhole attack have more value than other. As shown in above table 2 there is a wormhole link between nodes A, B and C. Hence the values of RTT in table 2 for this node are larger values than other nodes.

Table 3: Round Trip Time

RTT(S, A)	5
RTT(A, B)	11
RTT(B, C)	14
RTT(C, E)	5
RTT(E, D)	6

Table 3 shows the round trip time for successive nodes. The RTT (A, B) and RTT (B, C) have the larger values than RTT(S, A), RTT(C, E) and RTT (E, D). So there is a wormhole link between node A, B, and C.

5. Proposed Methodology

The technique starts with many steps. When the route is formed from Node S to D, the source node S is capable of computing the RTT between all intermediate nodes and also it can compute the handling time for each node. In this technique ,the time of each node (TN (RREQr), TN (RREQf), TN (RREPr) and TN (RREPf)) can be forwarded to the source in addition to route reply packet. The main important advantage of this technique is that the time of a node can be seen and stored by its neighboring nodes and they can also forward the same request packet. The neighboring nodes of a node note the forwarding time of that node so that, the chances of altering the request forwarding time by the attacker node be less and an illusion that the delay is due to the handling and queuing time may not be created. The following steps can be used for RTT calculation in this technique.

5.1. Mathematical Analysis

Here, actual RTT among participating nodes and destination will be discussed. After the calculation of actual RTT the processing time calculation will be discussed. Let us assume the route from S node to D node. Table 3 shows the calculation of ARTT with participating node and destination. The process starts with generation and record of TS (RREQr), TS (RREQf), TS (RREPr) and TS (RREPf) times. These timing values will be generated and recorded for the S node. The S node record RREQf that is pathrequest forwarding time of a packet, RREQr (Route request receiving time of Packet) transmitted from node S to destination node. Similarly, it can record the RREPf (Route reply forwarding time of Packet) and, RREPr (Route reply receiving time of Packet) to the destination node. The Actual RTT can be calculated by subtracting the Value of TS (RRPRf) from TS (RREQr). It gives the values of ARTT (SD) that is from the S node to the destination. The above process can also be done for the other nodes like A, B, C and E. The values of all time generation and recording will be given in table 3. The processing time for node S can be calculated by subtracting the Value of TS (RREQr) from TS (RREQf). It gives the values of the Processing time of the packet at S node. The details of processing time calculations will be given in table 4.The ARTT between an intermediate node for example from node S to A can be calculated by subtracting the Value of ARTT(AD) from ARTT(SD). The details of the ARTT of all intermediate nodes can be given in table 4

5.2. Working of Proposed Technique

As discussed in the previous section, Let us assume the route from S node to D node. The S node broadcasts a route request RREQ and also source node receives the route reply. All the neighboring nodes receive that request packet and rebroad cast it until it reaches the destination D. Then D prepares a reply packet and forwards

It back to the same route from which it received the request. D replies to all the requests received from different routes after fulfilling in all there requirements mentioned in this method. Table 4 shows the calculation of ARTT with participating node and destination. The process starts with generation and record of assumed values TS (RREQr), TS (RREQf), TS (RREPr) and TS (RREPf) times. These timing values will be generated and recorded for S node after the calculation of RTT of al lthe participating nodes with the destination, the source node S calculates the RTT between the intermediate nodes,

As shown in Table 5. The processing time calculations for all node will be shown in table no 8. The ARTT values of the intermediate node will be shown in table no 6. Table6 presents the expected and calculated RTTs of all the intermediate nodes.

Table 4: Actual Rtt Among Participating And Destination Nodes

Node	TN(RREQr)	TN(RREQf)	RREQ(sn)	TN(RREPr)	TN(RREPf)	RREP(sn)	ARTT(ND)
S	TS(RREQr)	TS(RREQf)	RREQ(ss)	TS(RREPr)	TS(RREPf)	RREP(ss)	ARTT(SD)=TS(RRPRr)-TS(RREQf)
A	TA(RREQr)	TA(RREQf)	RREQ(sa)	TA(RREPr)	TA(RREPf)	RREP(sa)	ARTT(AD)=TA(RRPRr)-TA(RREQf)
B	TB(RREQr)	TB(RREQf)	RREQ(sb)	TB(RREPr)	TB(RREPf)	RREP(sb)	ARTT(BD)=TB(RRPRr)-TB(RREQf)
C	TC(RREQr)	TC(RREQf)	RREQ(sc)	TC(RREPr)	TC(RREPf)	RREP(sc)	ARTT(CD)=TC(RRPRr)-TC(RREQf)
E	TE(RREQr)	TE(RREQf)	RREQ(se)	TE(RREPr)	TE(RREPf)	RREP(se)	ARTT(ED)=TE(RRPRr)-TE(RREQf)

Table 5: Actual Rtt Among Participating And Destination Nodes

Node	P(t)=RREQ(N)=[TN(RREQf) -TN(RREQr)]	P(t)=RREP(N)=[TN(RREPf) -TN(RREPr)]
S	P(t)=RREQ(S)=[TS(RREQf)-TS(RREQr)]	P(t)=RREP(S)=[TS(RREPf)-TS(RREPr)]
A	P(t)=RREQ(A)=[TA(RREQf)-TA(RREQr)]	P(t)=RREP(A)=[TA(RREPf)-TA(RREPr)]
B	P(t)=RREQ(B)=[TB(RREQf)-TB(RREQr)]	P(t)=RREP(B)=[TB(RREPf)-TB(RREPr)]
C	P(t)=RREQ(C)=[TC(RREQf)-TC(RREQr)]	P(t)=RREP(C)=[TC(RREPf)-TC(RREPr)]
E	P(t)=RREQ(E)=[TE(RREQf)-TE(RREQr)]	P(t)=RREP(E)=[TE(RREPf)-TN(RREPr)]

Table 6: Artt Between Intermediate Nodes

Intermediate Nodes	Actual RTT
ARTT(SA)	ARTT(SD)-ARTT(AD)
ARTT(AB)	ARTT(AD)-ARTT(BD)
ARTT(BC)	ARTT(BD)-ARTT(CD)
ARTT(CE)	ARTT(CD)-ARTT(ED)
ARTT(ED)	ARTT(ED)

Table 7: Notations

Name of Notations	Meaning
TN(RREQr)	Requesting Node N's Receiving time
TN(RREQf)	Requesting Node N's Forwarding time (Noted by Neighbors)
RREQ(sn)	Node N's RREQ packet size at a particular instant
TN(RREPr)	Replying Node N's receiving time
TN(RREPf)	Replying Node N's forwarding time(Noted by Neighbors)
RREP(sn)	Node N's RREP packet size at a particular instant
ARTT(ND)	Actual Round Trip time between Node N to Destination
P(t)	The processing time of a packet
Pd	Transmission delay (0.001ms)
µ	2ms(Limit for RTT between participating nodes
Tt	Transmission time
Ps	Packet Size in bits
Bw	Bandwidth in bps
ERTT(ND)	Expected Round trip time between Node N to Destination

5.3. Steps of Proposed Methodology

The expected RTT can be calculated by using equation (1) to equation (6). The Transmission time of each packet can be calculated by using equation (1).

$$Tt = \frac{Ps}{Bw}\text{-} \qquad (1)$$

The projected communication time of RREQ and RREP packet is calculated by equation (1). The transmission times for 4 neighboring nodes can be easily calculated as mentioned in equations (2) and (3) because each node is forwarding the packet size. Both the transmission times can be added using equation (4).

$$TtNiNi + 1 = \frac{Ps(RREQ)}{Bw}\text{-} \qquad (2)$$

$$TtNi + 1\ Ni = \frac{Ps(RREP)}{Bw}\text{-} \qquad (3)$$

$$ERTTNiNi + 1 = \ TtNiNi + 1 + TtNi + 1\ Ni\text{-} \qquad (4)$$

The Expected RTT can be calculated by adding the transmission time, processing time and propagation delay as shown I equation (5)

$$ERTT = \sum_{i}^{2N-1}[Tt(i) + P(t)i + Pd]\text{-} \qquad (5)$$

The algorithm of this technique simulates the results according to the equation (6). If the difference value of Actual RTT and Expected RTT is less than equal to µ. The node said to wormhole node otherwise no wormhole detected.

$$\text{If } If\ [A(RTTNiNi + 1) - E(RTTNiNi + 1) \leq \mu\ then\ \text{-} \qquad (6)$$

The value of µ can be calculated with the equation number 7 and 8

$$\text{Distance =(a(i+1)-a(i))^2+(a(y+1)-a(y))^2} \quad \text{-(7)}$$

$$\mu = \frac{Distance\ between\ each\ node}{Total\ number\ of\ message\ exchnage} \qquad (8)$$

No Wormhole

Else

Wormhole Detected Ni and Ni + 1

Proposed Flowchart

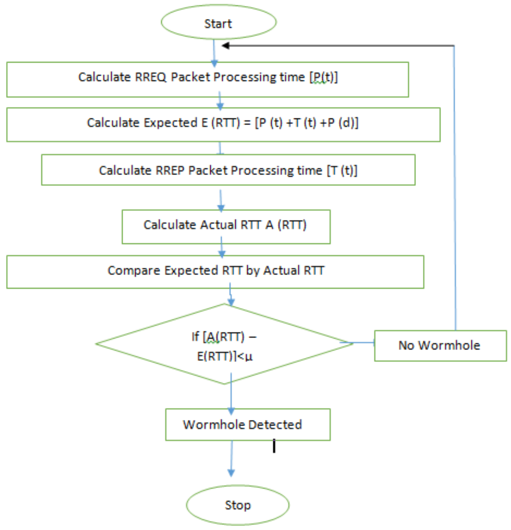
Start
Calculate RREQ Packet Processing time [P(t)]
Calculate Expected E (RTT) = [P (t) +T (t) +P (d)]
Calculate RREP Packet Processing time [T (t)]
Calculate Actual RTT A (RTT)
Compare Expected RTT by Actual RTT
If [A(RTT) – E(RTT)]<µ
No Wormhole
Wormhole Detected
Stop

Figure 4: Proposed Flowchart

6. Result and Discussion

This research work is related to detection and isolation of wormhole attack in wireless sensor networks. The proposed methodology is based on the threshold based delay technique for the detection of isolation of worm hole attack in wireless sensor networks. The proposed methodology detection the malicious nodes accurately from the wireless sensor network. The proposed methodology is implemented in network simulator version 2 and results are analyzed in terms of throughput , packet loss and energy consumption. The table 8 describe the simulation parameters in detail

Table 8: Simulation Parameters

Parameters	Values
Network simulator version	Ns2.2.35
Area	800 * 800 meters
Number of nodes	100
Antenna Type	Omi-directional
Link Layer	LL
Mobility Model	Random
Pause time	0.2 second
Simulation type	100 second

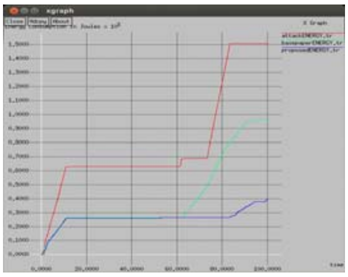

Figure 5: Energy Consumption

As shown in figure 5, the power expenditure of intrusion situation, foundation document situation and projected method situation are evaluated for the presentation scrutiny. It is investigated that the projected set-up involves smallest amount of power utilization in comparison with other approaches

Table 9: Energy Analysis

Time	Attack Scenario	Existing Technique	Proposed Technique
20 second	0.60 joules	0.22 joules	0.20 joules
40 seconds	0.62 joules	0.24 joules	0.22 joules
60 seconds	0.70 joules	0.40 joules	0.24 joules

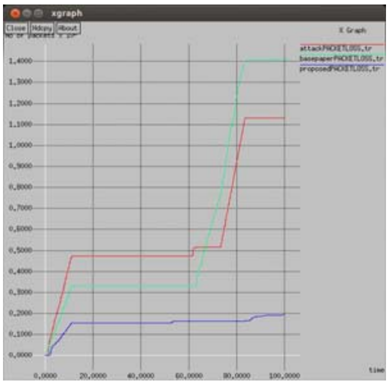

Figure 6: Packet Loss Comparison

As shown in figure 6, the package thrashing of intrusion set-up, foundation document set-up and projected set-up are evaluated for the presentation scrutiny. It is scrutinized that package thrashing of projected practice is fewer in comparison with other techniques.

Table 10: Packet Loss Analysis

Time	Attack Scenario	Existing Technique	Proposed Technique
20 second	0.48 packets	0.32 packets	0.10 packets
40 seconds	0.50 packets	0.34 packets	0.12 packets
60 seconds	1.2 packets	1packets	0.20 packets

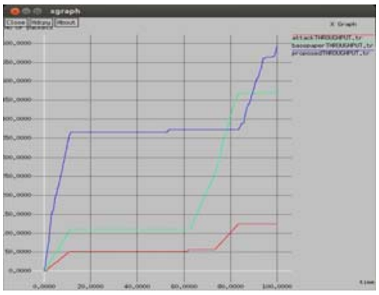

Figure 7: Throughput Comparison

As shown in figure 5, the overall performance of intrusion state, foundation document set-up and projected set-up is evaluated for the presentation scrutiny. It is investigated that overall performance of projected set-up is utmost in comparison with other setups.

Table 11: Throughput Analysis

Time	Attack Scenario	Existing Technique	Proposed Technique
20 second	48 packets	132 packets	210 packets
40 seconds	50 packets	134 packets	212 packets
60 seconds	150 packets	160 packets	220 ckets

7. Conclusion

It is identified that the wireless ad hoc systems are disseminated kind of networks in which sensor nodes can unite or depart the system according to them. No middle regulator is presented in the wireless ad hoc systems. Because of the self reliance character of the system safety, direction finding and service quality are the main problems associated with this system. An active kind of attack named wormhole intrusion may be the reason of the entering of attacker nodes in the system and because of this delay increases. In the presented research, enhanced PTPTT scheme is utilized. For the recognition of attacker sensor nodes, this scheme shows fewer precision and large implementation times. For the recognition of attacker sensor nodes in the presented study, threshold relied approach is implemented. The projected and accessible approaches are applied in NS2 and the reproduction outcomes depict development in power utilization, overall performance, and package thrashing.

References

[1] Y. Hu, A. Perrig, and D.B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”.

[2] I. Khalil, S. Bagchi, and N.B. Shroff, “LITE WORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks,” Proc. Int. Conf. Dependable Syst. Networks, pp.612–621, 2005.

[3] Y. Hu, A. Perrig, and D.B. Johnson, “Wormhole Attacks in Wireless Networks,” vol.24, no.2, pp. 370–380, 2006.

[4] S. Capkun, and J. Hubaux, “SECTOR : Secure Tracking of Node Encounters in Multi-hop Wireless Networks Categories and Subject Descriptors,” vol. 67322, pp.5005. 2003.

[5] W. Wang, and Y. Lu, “Defending against Wormhole Attacks in Mobile Ad Hoc Networks”.

[6] P. Van Tran, L.X. Hung, Y. Lee, S. Lee, and H. Lee, “TTM : An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks,” pp.593–598, 2007.

[7] A.S. Alshamrani, “Workshops of International Conference on Advanced Information Networking and Applications PTT : Packet Travel Time Algorithm in Mobile Ad Hoc Networks,” pp.561–568, 2011.

[8] C.E. Perkins, M. Park, and E.M. Royer, “ Ad-hoc On-Demand Distance Vector Routing,” 2006.

[9] M. Khabbazian, H. Mercier, and V.K. Bhargava, “Wormhole Attack in Wireless Ad Hoc Networks : Analysis and Countermeasure”.

[10] L. Qian, N. Song, and X. Li, “Detection of wormhole attacks in multi-path routed wireless ad hoc networks : A statistical analysis approach”, vol.30, pp.308–330, 2007.

[11] C. Paper, W. Znaidi, and S. Appliqu, “Detecting wormhole attacks in wireless networks using local neighborhood information Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information”, 2008.

[12] D. Dong, M. Li, Y. Liu, and S. Member, “Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks,” vol.19, no.6, pp.1787–1796, 2011.

[14] L. F. Garcia, and J. Robert, “Preventing Layer-3 Wormhole Attacks in Ad-hoc Networks with Multipath DSR,” pp.15–20, 2009.

[15] M.Y. Su, “WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks”, Comput. Secur. , vol.29, no.2, pp.208–224, 2010.

[16] Y. Yu, L. Guo, X. Wang, and C. Liu, “ad hoc networks”, Comput. Networks, vol.54, no.9, pp. 1460–1469, 2010.

[17] Prasannajit, B. Anupama, S. Vindhykumari, K.S.R. Subhashini, and G. Vinitha, “An Approach towards Detection of Wormhole Attack in Sensor Networks,” 2010.

[18] D. Kim, D. Kim, H. Park, and S. Yoo, “Performance Evaluation of Routing Protocols for Wireless Sensor Networks in Military Scenarios”, pp.101–106, 2011.

[19] S.G. Smieee, N.C. Mieee, N. Tada, and S. Trivedi, “Scenario-based Performance Comparison of Reactive”, Proactive & Hybrid Protocols in MANET, pp.0–4, 2012.

[20] A. Goyal, “Simulation and Performance Analysis of Routing Protocols in Wireless Sensor Network using QualNet,” vol. 52, no.2, pp.47–50, 2012.

[21] R. Ahuja, and A.B. Ahuja, “Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack,” pp.699–702, 2013.

[22] B. Paul, K.A. Bhuiyan, K. Fatem, and P. P.Das, “Analysis of AOMDV, AODV, DSR and DSDV Routing Protocols for Wireless Sensor Network”, 2014.