Energy Aware Secured Routing against Wormhole Attack in WSN

Vignesh Saravanan K
Department of Computer Science and Engineering,
Ramco Institute of Technology
Rajapalayam, India

Narmadha S
Department of Computer Science and Engineering,
Ramco Institute of Technology
Rajapalayam, India

Vijayalakshmi K
Department of Computer Science and Engineering,
Ramco Institute of Technology
Rajapalayam, India

***Abstract*—A wireless sensor network(WSN) is a network consists of autonomous sensor devices that are mainly used to monitor physical and environmental condition like temperature pressure etc. The WSN is made of hundreds and thousands of detection station known as nodes, where every node consists of one or additional sensors. The WSN are also the networks that is for to communicate by sensing the behavioral changes and also the sensing node can collect the info and it'll get processed. There are some organizations that are having important necessity of wireless networks in organizations like military, ecology and health.**

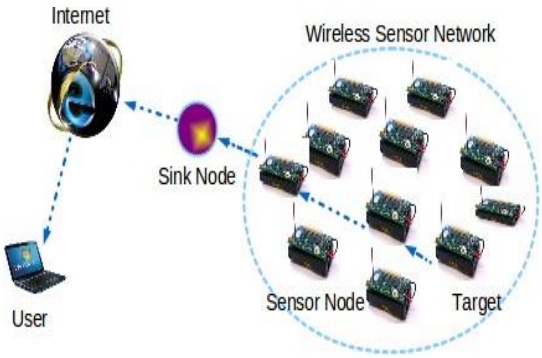
The WSN have to be compelled to be secured from network attacks particularly at unfriendly things as a result of information will simply be attacked by the attackers. There are varied forms of attacks targeting totally different network layers. One form of attack may be a wormhole attack that's harmful and simply deployed attack that targets the routing layer. There are different attacks they're depression(sinkhole) attack and greeting(hello) flood attack. These drawbacks will build WSN totally different from different networks. The projected live is applied to the ad- hoc on-demand distance vector routing protocol and simulation of the attacks are worn out the NS2 simulator. By simulating, the performance of the network are often monitored and done once the hole tunnel is of minimum of 4 hops or additional long.

***Keywords*—Routing, AODV, Wormhole Attack, Hop Count**

I. INTRODUCTION

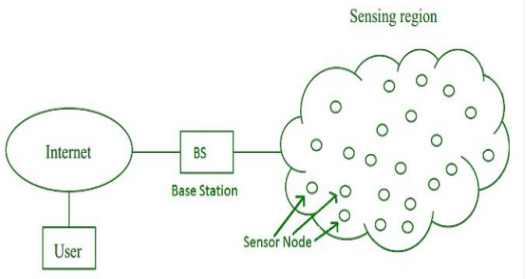
A WSN consists of sensor devices that are mainly used for to measure accustomed monitor physical and environmental conditions like temperature, humidity, pressure etc. Fig. 1 represents the design of a WSN. The WSN is made of a hundred and thousands of detection stations referred to as nodes, where every node connects to sensors. Every WSN consists of a radio transceiver, associate degree internal/external antenna, a microcontroller and electric battery. Constructing a wireless sensor network (WSN) has become vital altogether places. Small sensor devices will perform multiple tasks like processing, sensing and human action with different devices within the wired network. A Wireless sensor network is employed for easier system style and observance the device in wireless network. Several sensors are deployed in numerous places; therefore they have security for transferring knowledge through the network. Victimization some technologies and economical techniques we are able to produce a secure knowledge transfer theme in WSN. Wireless sensor network security arrange should have effective key distribution among all completely different nodes in same network.

Figure 1: Illustration of a WSN



The sensor nodes collect the data and send to the base station for processing and then it sent to the user via a wireless medium. A WSN has numerous applications in many fields. They are deployed in many places. A WSN is used in these applications to monitor the maintenance, improve the productivity and enhance the security and safety. For wide deployment, it is required that the sensors should be made smaller and inexpensive. There are also many methods being proposed to secure the network from different kinds of attacks. Fig. 2 shows the applications of WSN's in numerous fields. They are deployed in many places and the sensors have a capability to give a warning at emergency situations.

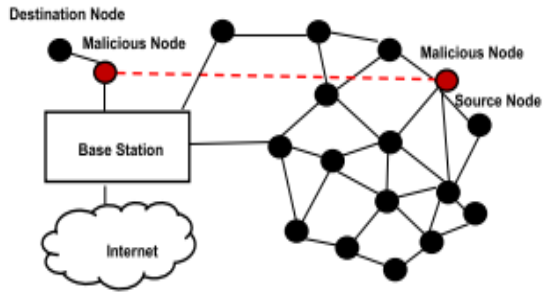
Figure 2: Actual image of a WSN with multi-hop communications



There are many types of attacks targets routing protocol in WSNs referred routing attack. The wormhole attack is a grave attack. Fig. 3 shows Two attackers locate themselves as two conniving sensor node tunnel control and data packets between each other with intention of creating

shortcut in WSN. The first malicious sensor eavesdrops on first location to receive the control and tunnel packets to second malicious sensor, then second malicious sensor forwards the received packets to intended destination. Alternatively, the malicious sensor captures the packets within a certain area and send them to remotely placed sensor. The wormhole attack effortlessly started by intruder without need of understanding the networks or applying cryptographic techniques. They affect the network by changing or drop send packets or collecting packets with goal traffic examination/encryption breaking. The influence system powerless in discovering the routes that are longer than 2 hops thus the result in false network topology. This works contributes secure WSN against wormhole attack by proposing an energy preserving secure measure.

Figure 3: Wormhole attack in wireless sensor network.



II. LITERATURE REVIEW

WATEEN A. ALIADY AND SAAD A. AL-AHMADI et al (2019) proposed that there are various varieties of attacks targeting different network layers. One kind is a wormhole attack that's harmful and easily deployed attack that only targets the routing layer. In this paper, a proposed energy preserving secure measure based on the network connectivity main aims to detect the wormhole attack. The proposed measure is applied to the ad-hoc on-demand distance vector routing protocol and therefore experiment is tested victimization Network Simulator 3. The results state that the detection accuracy is 100 percent when the wormhole tunnel is of four hops or more in length [1].

Z. Qian and Y. J. Wang et al. (2014) proposes that Wireless Sensor Networks (WSNs) have gained increasing interest within research communities for its major role in wide number of applications. It makes life more convenient, safe and easy. Moreover, it is adapted in variant areas e.g., health, environment, traffic, surveillance and industry. It also lacks infrastructure and is composed of sensor nodes that can communicate directly through a transceiver [2].

C.Guy et al. (2006) proposes that WSN composed of sensors that can sense their surrounding environment, to deliver the information to a base station that has a connection to the Internet. the base station has more computational and storage abilities than sensors. The sensed information is sent through the base station to be received for those of interest.For example, habitat and environment monitoring is of interest to scientists and researchers interested in natural sciences [3].

F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci et al.(2002) proposed that a sensor is composed of a sensing unit to sense the environment, a processing unit, storage, a transceiver unit to communicate, a power unit used for power supply. There are optional units in a sensor which are: location finding system to determine the sensor's location, a power generator, and a mobilizer that is needed to move sensor nodes when required to carry out a specific task [4].

G. Serpen, J. Li, and L. Lu et al. (2013) proposed that in pursuance to implement, there are some challenges that are required to be solved. The major challenge in adapting this type of network is preserving energy because sensors have limited life time. Furthermore, sensors have limited storage space and restricted computational ability and thus making defense against security attacks more challenging [5].

I.Tomic and J. A. McCann at el. (2017) proposed that the security is a priority in wide applicationse.g., responding to emergency as in natural disasters, military and in safety critical operations. If communication is damaged catastrophes might happen without the rescue team's knowledge. There are many types of security attacks that target routing protocols in WSNs referred to as routing attack e.g., Sybil, wormholes and spoofing attacks [6].

S. Bhagat and T. Panse et al. (2015) proposed that wormhole attack is described as generating untrusted shortcut through the network. This is formed when two intruder sensors have a higher transmission range ability than normal sensors. They can form direct communication between them which is equal to the length of the distance between them. Also, they can communicate with the rest of the normal sensors using the normal sensor's standard transmission range. Alternatively, the malicious sensor has the capability to capture the packets within a certain area and send them to other remotely placed sensors. Because packets generated by malicious sensors are received earlier than packets generated by normal sensors, the destination sensor will drop the normal packets [7].

G. Farjamnia, Y. Gasimov and C. S. Hong et al. proposed that the major problem of the wormhole attack is that it can be effortlessly started by the intruder without the need of understanding the network or applying cryptographic techniques the generated wormhole tunnel by two intruder sensors. They use this tunnel to not allow any legitimate sensor to receive the transmitted packets. This way they ensure that their packets will be received earlier. Therefore, they can control the transmitted packets by either altering or dropping them [8].

Y.-C Hu, A. Perrig, and D. B. Johnson et al. (2019) proposed that wormhole attack is among the most extreme routing attacks, which can be implemented easily however hard to detect. This attack is launched regardless if the host is being compromised or not, though the network assures authenticity and confidentiality. They'll have a affect on network by changing or dropping the sent packets or simply by collecting a substantial number of packets with the goal of traffic examination or coding breaking. It will influence the system to create it powerless in discovering routes that are

longer than two hops therefore this may lead in giving a false network topology [9].

L.Ahmed et al. (2014) focus is to secure the energy efficient Cross-Layer Medium Access Control (CL-MAC) protocol in WSNs. The CL-MAC is made of two neighboring layers. The MAC layer and network layer that trade control packets to locate the shortest route to the base station with the goal that every node having a place with the same path must be prepared for routing packets. Other nodes which are neighbors and do not have a place with the path need to go to a sleeping phase, turn off their transceiver, from the starting point to the finish of the routing procedure. The attack can take place as in the following scenario, a malicious node tunnels a Request To Send (RTS) packet that is sent from one zone to a zone in the distance, to put all nodes in this remote zone into sleep mode. The paper proposed a solution that differentiates between the passive and active wormhole attacks as it gives each a different solution. In the passive attack which is when packets are not modified, the RTT is calculated. This is calculated in the network layer by route request and route reply messages. In addition to this, it is calculated in the MAC layer while sending hello messages periodically to build neighbors list. In the active attack, the communication is protected by adding a flag variable to specify if the receiver is suitable. The limitation for this method is that it consumes more energy if the wormhole node is remotely located from the sink [10].

Amish and Vaghela et al. (2016) propose security against wormhole attack in Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV) that is an extension to Ad-hoc On-demand Distance Vector routing protocol (AODV). The paper mentions that two sensors to communicate, the sender, investigates if there is a path to the destination in its own routing table. If a route is not presented it broadcasts a RREQ packet to its neighbors, as the neighbors in turn check for a route or forward the RREQ until the destination is discovered. Afterwards, the destination generates a Route Reply (RREP) packet to the source follows the exact route for the received RREQ. For every received RREQ in the destination a route is generate and save in the routing table of the source. The method calculates the RTT for each generated route by noticing the time when the sender sends RREQ and it receives RREP. It divides each RTT by corresponding hopcount and the average value is a threshold value. If the RTT is less than threshold and number of hops are two, then a wormhole exists. This solution is able to detect most wormholes with a high throughput and delivery ratio [11].

M. Imran et al (2015) proposed that the round-trip time is the time it takes for the packet to be sent and for the acknowledgment to be received. The work is based on RTT for detecting this attack. The paper presented the detection rate for their method, which is the basic parameter to specify the effectiveness of the proposed method. The limitation for this method is that all sensors in the network must have a tightly synchronized clock but it is a difficult and expensive task to implement synchronized clocks [12].

Rai et al. (2012) propose a method of identification in mobile ad-hoc networks. The method is based on the calculation of delay and hop count for several paths chosen randomly. First, one of the nodes in the path was chosen to transmit a packet. Then, a timer was started to measure delay and hop count. The process was repeated and on each iteration the route information associated with its hop count and delay was stored. If the same route appears to have less delay in comparison to other routes, then a certain node is malicious. To detect it, the node that is not encountered previously is found [13].

Sookhak et al. (2015) propose a method that starts as the sender generates a pairwise key using hash function for both public and private keys. The goal is to send a beacon packet containing location, nodes' ID and destination to its neighbors to generate neighborhood table. In addition, the beacon packet contains a list of private keys to detect malicious nodes. Then, select the best neighbor that is the closest to the destination and must have at least one private key matrix similar to a private key matrix in the sender's neighborhood table. After that, generate a shared key using the private key to assure the sender of the trustworthiness of the received neighbor. The final step happens in the destination, which is to double check by calculating the distance through path and its relationship with number of hops and transmission range for sensor nodes. The proposed method can detect wormhole attacks with a high accuracy but in a dense environment it is a memory drainage method because this means a large neighborhood table needs to be stored [14].

Chen et al. (2014) proposed an identification technique based on mobile beacon. The existing paper focuses to detect wormhole and localize them based on the network model assumption of having a mobile beacon node that has GPS, static beacon that are fixed in location in advance and static sensors. The drawback in this method is that employment of mobile beacon node is costly and the malicious node can drop the packets or corrupt the packets. The scheme of detecting a wormhole is to check if there are violations. From the packets' side, its uniqueness property which is identified in that the receiving node should receive a packet once, if a duplicate is received then a wormhole is detected. Second, is from the nodes' side, it checks for violation to transmission constraint Property identified by an existing communication between neighboring nodes that are more apart than their transmission range [15].

Jegan and Samundiswary et al. (2016) proposed a mechanism in Zigbee WSNs using IDS. The paper introduced an Energy Efficient Intrusion Detection System (EE-IDS) that detects wormhole attack in an energy efficient manner in Zigbee based WSNs. First, the sink does a topology discovery for all nodes as it broadcasts topology discovery message to nodes that will do measure quality of service e.g., residual energy and queue delay. Then, fill in the topology information table. Then, give an optimal location for watchdog nodes to have less energy consumption and stronger security. Finally, detect wormholes in watchdog nodes by verifying the trustworthiness of nodes and abnormality in packet delivery ratio [16].

Krentz and Wunder et al. (2014) proposed a method that is totally based on the RSSI to avoid hidden wormholes using

channel reciprocity. This paper proposed a Secure Channel Reciprocity-based Wormhole Detection (SCREWED), that has two operations. The first method is called Sampling which is based on sending N pings and pongs between two nodes, that is node A sends N pings to node B, and node B replies with pongs. A timeout for these is added to avoid deadlock such as when certain ping or pong is lost. Those are sent using channel hopping to generate variation in RSSI The second operation is called judgment that is node A sends a judge message to B, so node B shall decide if node A should be dropped or not based on received pongs, and RSSI correlation of node A and B [17].

N. Labraoui, M. Gueroui, and M. Aliouat et al. (2014) proposed it will trigger a wormhole link by two checking ways. The primary is based on the RSSI and the second way is to overcome the primary way drawback that some malicious nodes will fabricate the RSSI. This way rely on the RTT, to calculate the time for a packet to be transmitted between two neighbors. If the time is smaller than the common RTT of all neighbors, then a wormhole link will detect [18].

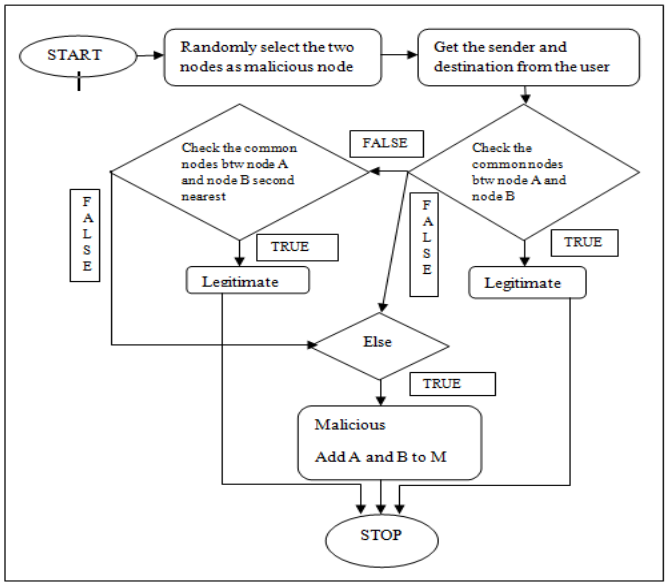
X. Lu, D. Dong and X. Liao et al. (2016) proposed a way for detection that's supported on topologies in WSNs. It is made on investigating the anomalous arrangement conferred by this attack. Each sensor gathers the information of its k-hop neighbors and their subgraph. At that point, it builds associate estimation distance matrix. Next, the matrix of estimation distance is used to construct the subgraph. Then, insert it on a plane by multi dimensional scaling (MDS) amid which each and every sensor will be assigned a virtual position. The fundamental thought of this wormhole discovery approach depends on an essential perception as following. If a node may be a regular sensor, the MDS format fits with the estimation distance however if a node is an intruder, its neighbor's subgraph cannot be simply inserted on a plane [19].

T. Bin, Q. Li, Y.-X. Yang, D. Li, and Y. Xin et al. (2012) The paper with the title ''A ranging based scheme for detecting the wormhole attack in Wireless Sensor Networks'' is formulated on the analysis of statics that can identify hidden wormhole attacks. The paper exanimated the node's timing from sending a packet to other nodes until it gets a response which is called an echo for the message. In different words, every node saves the initial timing T and sends out a HELLO packet for neighbor disclosure. Every sensor that gets a HELLO packet transmits an answer. Every sensor assembles its neighbors table that may incorporate distanced neighbors associated with wormholes and calculate the time of arrive (ToA). A formed list is used as an input to the proposed method. It includes the node's identity and the node's ToA. A decision is made, if there was an increase in density above threshold there would be an intrusion detection investigation. If this is the case, then a wormhole detection is performed based on k-means clustering. The ToA is picked as the measure of dissimilarity. In this paper, k is equivalent to two. Clearly the normal and intruder neighbors will have a total of two groups [20].

III. DESIGN AND IMPLEMENTATION

The step-by-step procedure used to find the wormhole attack in WSN as shown in Fig.. This flow diagram represents the overall flow of the attack detection mechanism. First it is applied between the destination and sensor A, then between sensor A and sensor B, afterwards between the sensor B and sender. Passing the first stage means it is legitimate that is to check if there is a common sensor between the first stage nodes. if it passes the second stage it is legitimate that is to check the common nodes between the nest stage nodes. Passing the third stage it shows that it is malicious that is the else case of above two failed and the nodes are detected to make the new path.

Figure 4 : Flowchart for finding wormhole attack



ROUTING:

The process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network/node to another.

AODV:

Ad-hoc On-demand Distance Vector is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses.

WORMHOLE ATTACK:

Two attackers locate themselves as two conniving sensor node tunnel control and data packets between each other with intention of creating shortcut in WSN.

HOPCOUNT:

It refer to the number of devices, usually routers, that a piece of data travels through.

IV. EXPERIMENTAL SETUP AND RESULTS EVALUATION

A. *EXPERIMENTAL SETUP*

This methodology uses the cpp and tcl scripts to evaluate the nodes in WSN in computer.All other relevent parameter are shown in the table.

Name	*Parameter*
Memory	8Gb (RAM)
Processor	Any processor above500MHz
Operating System	Ubuntu
Development Environment	NS2,related libraries
Language	C++, Tcl files
Sensor position	Random
Routing protocol	AODV
Transmission rangefor wormhole nodes	As long as tunnel

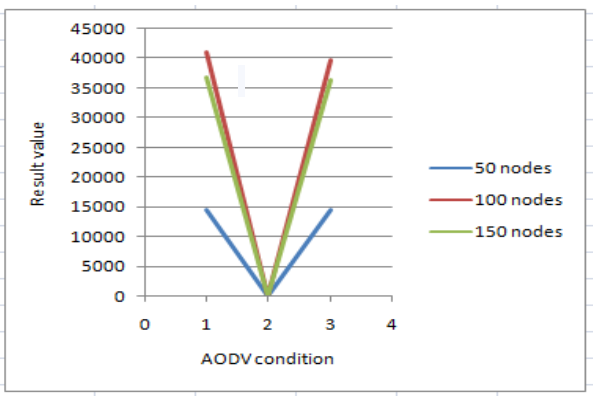
B. *EXPERIMENTAL RESULTS*

The sensors locations are stored in a computer file/text file to read those locationsin additional runs. This is often done to possess constant positions for all implemented files. In different words, network topology should be anequivalent for the network implementation, the network under attack implementation, and therefore the secured network implementation to possess a good comparison. The transmitted data could bea computer file of size 2842 bytes. it's divided into chunks of five hundred bytes then placed in a very buffer. Then, generate packets from that buffer, send them so at the destination scan the buffer and append the content to a buffer to reconstruct the initial file.

Table 1 : Throughput result

	Normal AODV	AODV under attack	Secured AODV
50 nodes	14482.9	4	14402.6
100 nodes	41089.9	2	39702.7
150 nodes	36909	0	36400

Figure 5: Energy Consumption



In this work a distinct event simulator for networks is employed, referred to as network simulator (NS2). The used version during this work is version of 2.35. The NS2 is especially used for analysis and academic purpose. The NS2 machine is supplied with the NetAnim animator that's accustomed shows visualization image. The Fig. gift the secured technique analysis once the malicious sensors are detected within the network.This is often once the wormhole tunnel is minimum hops or a lot of long however once having a wormhole tunnel of a less length it would not observe the malicious sensors and so have a performance just like the malicious situation.

Table 2 : Delay result

	Normal AODV	AODV under attack	Secured aodv
50 nodes	2	20	4
100 nodes	1	19	1
150 nodes	3	18	3

Figure 6: End to end delay

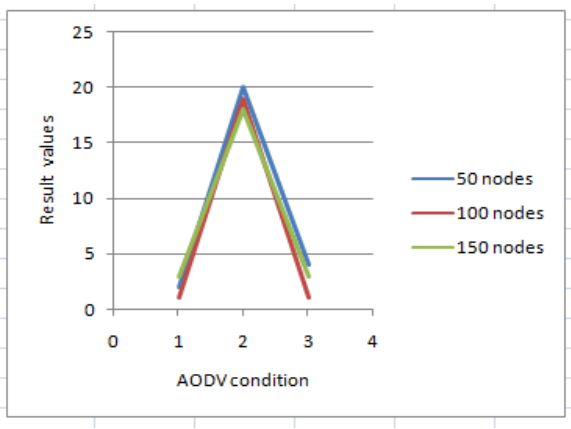


Fig. 5 presents the delay worth that's known by the time needed to deliver the whole file and since malicious sensors drop packets, it'll ne'er be delivered utterly. Therefore, an infinity value isemployed for the attack case as a result of it'll ne'er deliver the message. It's terribly clear that the planned secured technique has little increase with in the delay worth that's hard to be mentioned.

The superimposed delay for the detection technique within the 50-node network size is a pair of second. Additionally, within the 90-node network size the super imposed delay for transmission is 0.5 second. Furthermore, the 150-node network size a additional 1.2 second used for detection. The number of delay needed to perform the planned security live is completely correlative to the length of hole tunnel and therefore the neighborhood lists size. In Fig. 6 the end to end delay has the very best values for the 50-nodes network size.The throughput is known by the amount of bits transmitted per second. In Table the network under attack incorporates a zero worth for the throughput which is due malicious nodes are dropping all packets and so no additional packets exist within the path.

Additionally, the secured technique incorporates a worth that's terribly on the brink of thetraditional worth.The reason behind that's the calculation of throughput that's by dividing the whole transmitted message over the delay time and since the transmitted message is constant in size, it's affected only by the delay worth.

Therefore, and since the 50-nodes network size has the very best delay worth, it's the smallest amount decrease within the throughput. The method is energy conserving as shown in Fig. 6 wherever the common extra energy in 50-nodes network.And the network size was 70 Joules,and therefore the average extra consumed energy in 90-nodes network size was 21 Joules, and in the case of 150- nodes network size the extra energy was 129 Joules.

The amount of energy consumption needed to perform the planned security live is positively correlative to the length of hole tunnel and therefore the neighborhood lists size. what is more, energy consumption is that the highest in 150-nodes network as a result of it's a really dense neighborhood table. Moreover, the packet delivery ratio is known by successfully delivered packets to destination and once the malicious nodes are detected the secured technique uses different path for transmission and so the secured measure will deliver the whole message by this alternative path. the secured technique has dropped the energy consumption to 50% compared to the network under attack.

Moreover, in the aim was to propose an Energy efficient Intrusion Detection System by lowering the energy consumption where it was reduced by 8% compared to different existing intrusion detection systems within the AODV routing protocol.However, our planned secured technique has dropped energy consumption to ninety fifth, 96%, and 97.5% compared to networks under attack for 50-nodes, 100-nodes and 150-nodes network sizes respectively.

V. CONCLUSION

WSN's are of huge demand in the present world and the request for WSN measures increasing rapidly, as a result of growth of victimization WSN has increased. These drawbacks can create WSN varied from other networks and some small concerns that may occur in a WSN. Based on the top mentioned difficulties in the data integrity, security, there are many solutions that are available to overcome or to beat these dangers. In this way the wormhole attack is detected and it is visualized using NS2 animator.

In addition, if the nodes are less than 50 then the occurrence of the wormhole attack will be minimized due to the direct transaction between the nodes. If the nodes are above 150, the capacity of wormhole is difficult to find, then the analysis and algorithm to run and computation is more. The computation cost is highly increasing when it is going beyond the 200 node.

The energy consumption and end to end delay is also calculated for secured AODV, AODV under attack and Secured AODV. On simulation, the performance and therefore the efficiency of the network is analyzed. The behavior and the energy parameters is examined. A mechanism for making secure data transfer and preventing the attacks in a WSN must be planned and proposed. The parameters which confirms the network performance is calculated from the simulation. As the result of the numerous attacks happening in the WSN, there is less amount of security. As per the recommendation the further study can be done to detect the all types of attacks in WSN.

VI. REFERENCES

[1] Wateen A.Aliady and Saad A.Al-Ahmadi, '' Energy Preserving Secure measure against Wormhole attack in Wireless Sensor Networks",IEEE Commun. Mag.,vol 7,July 2019.

[2] Z. Qian and Y.-J. Wang, ''Internet of Things-oriented wireless sensor networks review,'' J. Electron. Inf. Technol., vol. 35, no. 1, pp. 215–227, 2014.

[3] C. Guy, ''Wireless sensor networks,'' in Proc. 6th Int. Symp. Instrum. Control Technol., Signal Anal., Meas. Theory, Photo-Electron. Technol., Artif. Intell., Nov. 2006, Art. no. 63571I

[4] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ''A survey on sensor networks,'' IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[5] G. Serpen, J. Li, and L. Liu, ''AI-WSN: Adaptive and intelligent wireless sensor network,'' Procedia Comput. Sci., vol. 20, pp. 406–413, Jan. 2013.

[6] I.Tomić and J. A. McCann, ''A survey of potential security issues in existing wireless sensor network protocols,'' IEEE Internet Things J., vol. IOT-4, no. 6, pp. 1910–1923, Dec. 2017.

[7] S. Bhagat and T. Panse, ''A review on detection and prevention of wormhole attack in wireless sensor network,'' Int. J. Comput. Appl., vol. 127, no. 13, pp. 1–4, Oct. 2015.

[8] G. Farjamnia, Y. Gasimov, and C. Kazimov, ''Review of the techniques against the wormhole attacks on wireless sensor networks,'' Wireless Pers. Commun., vol. 105, no. 4, pp. 1561–1584, Apr. 2019.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, ''Wormhole attacks in wireless networks,'' IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

[10] L. Ahmed, S. Larbi, and K. Bouabdellah, ''A security scheme against wormhole attack in MAC layer for delay sensitive wireless sensor networks,'' Int. J. Inf. Technol. Comput. Sci., vol. 12, pp. 1–10, Nov. 2014.

[11] P. Amish and V. B. Vaghela, ''Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol,'' Procedia Comput. Sci., vol. 79, pp. 700–707, Jan. 2016.

[12] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, ''Analysis of detection features for wormhole attacks in MANETs,'' Procedia Comput. Sci., vol. 56, pp. 384–390, Jan. 2015.

[13] P. Rai, V. Srivastava, and R. Bhatia, ''Wormhole attack detection in mobile ad hoc networks,'' Int. J. Eng. Innov. Technol., vol. 2, pp. 174–179, Aug. 2012.

[14] M. Sookhak, A. Akhundzada, A. Sookhak, M. Eslaminejad, A. Gani, M. K. Khan, X. Li, and X. Wang, ''Geographic wormhole detection in wireless sensor networks,'' PLoS one, vol. 10, no. 1, 2015, Art. no. e0115324.

[15] H. Chen, W. Chen, Z. Wang, Z. Wang, and Y. Li, ''Mobile beacon based wormhole attackers detection and positioning in wireless sensor networks,'' Int. J. Distrib. Sensor Netw., vol. 10, no. 3, 2014, Art. no. 910242.

[16] G. Jegan and P. Samundiswary, ''Wormhole attack detection in zigbee wireless sensor networks using intrusion detection system,'' Indian J. Sci. Technol., vol. 9, no. 45, pp. 1–10, 2016.

[17] K.-F. Krentz and G. Wunder, ''6lowpan security: Avoiding hidden wormholes using channel reciprocity,'' in Proc. 4th Int. Workshop Trustworthy Embedded Devices, Nov. 2014, pp. 13–22.

[18] N. Labraoui, M. Gueroui, and M. Aliouat, ''Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks,'' Trans. Emerg. Telecommun. Technol., vol. 23, no. 4, pp. 303–316, Jun. 2012.

[19] X. Lu, D. Dong, and X. Liao, ''MDS-based wormhole detection using local topology in wireless sensor networks,'' Int. J. Distrib. Sensor Netw., vol. 8, no. 12, pp. 1–9, 2012.

[20] T. Bin, Q. Li, Y.-X. Yang, D. Li, and Y. Xin, ''A ranging based scheme for detecting the wormhole attack in wireless sensor networks,'' J. China Universities Posts Telecommun., vol. 19, pp. 6–10, Jun. 2012