ISSN (Online) : 2454 -7190 **ISSN (Print) 0973-8975**
Copyright © J.Mech.Cont.& Math. Sci., Vol.-14, No.-1, January-February (2019) pp 444-468

Two Step Verification technique For Detection of Malicious Nodes in Wireless Sensor Networks

[1*]Mandeep Kumar, [2]Jahid Ali

[1]Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India

[2]Professor & Director, SSICMIT, Badhani, Pathankot, Punjab, India

[*] mandeep_recj@yahoo.com

https://doi.org/10.26782/jmcms.2019.02.00032

Abstract:

The wireless sensor network is the application oriented network which performs task of monitoring and object tracking. The wireless sensor node has the architecture which involves wireless interface for the communication. The design of the wireless sensor network depends upon the significant of application, cost and type of hardware. The architecture of WSN is dynamic due to which security and energy consumption are the major constraints. The Sybil attack is the attack which is possible in wireless sensor networks and it affect network performance. The attacker node generates multiple identities to attract network traffic and leads to denial of service in the network. In this research work, two step verification technique is proposed for the detection of malicious nodes from the network. In the two step verification technique, the cluster heads detect the node as untrusted if its energy consumption is abnormal. The extra observer nodes are deployed in the network, which observe network traffic. On the basis of network traffic observations, the node is declared as trusted or untrusted. When the cluster head and observer node both declare on node as untrusted node, then that sensor node will be considered as malicious node. The experiment is conducted is NS2 by considering certain simulation parameters. It is analyzed that two step verification technique detect malicious nodes successfully and it also leads to improve network performance in terms of Delay, PDR and Packetloss.

Keywords : wireless sensor network, sensor node, Sybil attack, malicious nodes, observer node, network performance

1. Introduction

Wireless Sensor Networks (WSNs) consist of large number of sensor nodes, densely deployed over an area [I]. The sensor nodes are capable of collaborating with one another and measuring the condition of the environment [XX]. A particular sensor node might be able to sense temperature, pressure and even any object that is moving around them. The sensed measurements are transformed into digital signals and processed to reveal some properties of the phenomenon around sensors [XXXIII].

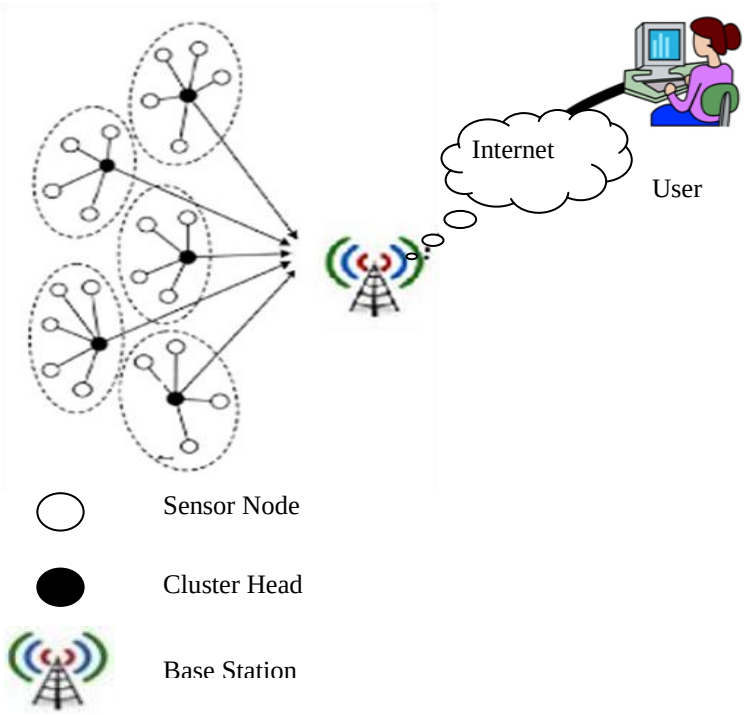

Fig. 1. *A Cluster based typical WSN.*

Fig. 1 shows the cluster based structure of typical WSN. The wireless sensor networks have diverse types of applications in medical purposes, healthcare, space applications, agriculture and other various maintenance purposes [XXII]. The sensor nodes are placed in unattended and hostile environment, which attracts various types of attacks like wormhole attack, selective packet dropping or Sybil attack [IX]. The attacks are dangerous to the communicated sensitive data and to the proper functioning of wireless sensor network [XVII]. The traditional security mechanisms cannot be employed for WSNs due to limited resources in the network such as limited computation power, battery and communication range [XXV]. Therefore, the trust management mechanisms become effective means for providing security in sensor networks [XII]. In trust based schemes, the sensor nodes are analyzed and evaluated on the basis of different characteristics, so as ensure safe transmission of data between nodes.

1.1. Sybil Attack

Sybil attack is firstly illustrated by Microsoft researcher John Douceur [VII]. Sybil attack is that attack in which a single node, called a malicious node, can illegitimately takes multiple identities [II]. An attacker can use multiple identities to act maliciously, either by stealing the information or disrupting network

communication. Further any type of communication with a malicious node may result in loss of data and it becomes dangerous for a network [V]. It is critical to detect Sybil attack and identify its dangerous in order to protect the network from this attack.

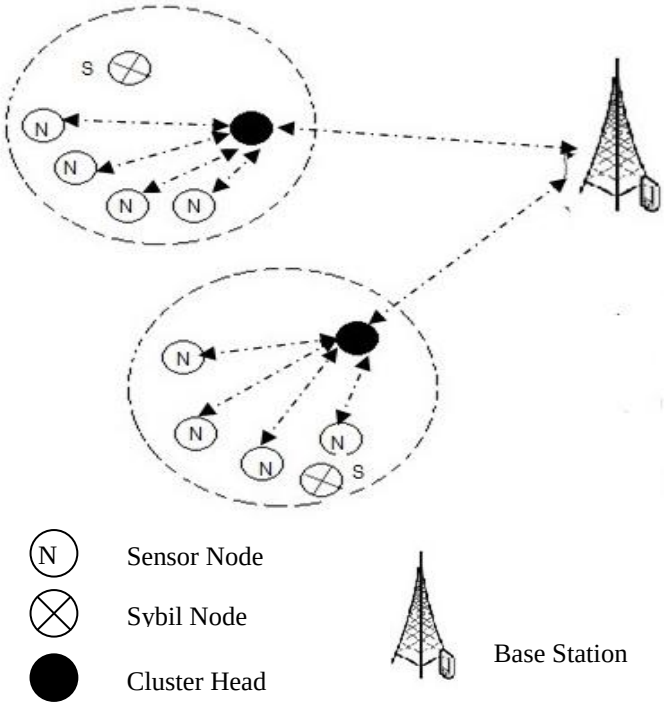

Fig. 2. *Sybil attack in WSN*

Fig. 2 shows the WSN architecture with Sybil node. The node that illegitimately takes the identity of other node is called Sybil node S and the other one is a regular node N. In a normal communication system only N nodes should communicate with cluster head. But here, S node comes in another form and launches an attack on the network. This causes confusion in the network and it gets collapsed.

1.2 Sybil Attack Classification

It Sybil attacks are classified into various forms on the basis of the manner of attack on the network. They are as follows.

1.2.1 Direct and Indirect Communication:

The type of communication between regular node and malicious node must be considered before launching Sybil attack in a sensor network [XXVI]. In case of direct communication, the attacker can communicate directly with the regular node

with the help of spoofed identities. In case of Indirect communication, the attacker cannot communicate directly with the regular node, but the communication with regular node is done through intermediate malicious node. The attacker used its legal identity to communicate with regular node, and then forward its malicious data to the regular node through the legal node. Direct communication type of Sybil attacks are more difficult to detect and the attacker can also launch these types of attacks easily. All section heading

1.2.*2 Simultaneous and Non-Simultaneous:*

The attacker can create the Sybil nodes one by one or all simultaneously. In case of simultaneous attack, all the Sybil identities are created at once .The multiple identities are created simultaneously at same time in the network. In case of non-simultaneous attack, the attacker creates the identities one by one and over a period of time [III]. The non-simultaneous attack classification is just like one identity is leaving the network and the other identity is joining the network. The attacker in this case swaps among different identities to do the attack. For example in simultaneous attack, the Sybil identities like 101, 102, 103 and 104 all are created simultaneously at time t1 through Sybil node S where as in Non-Simultaneous attack, the attacker first create 101 identity at time t1 then after a while at time t2 it create identity102.

1.2.3 Stolen and Fabricated Identities: In the case of fabrication, an attacker can generate randomly new identities. For example, if any regular node has the identity of length 64 bit, then the attacker creates a 64 bit random value from a malicious node. In case of stolen identities, the attacker actually stole an identity from the regular node. So it creates a new identity similar to that of stolen identity. This type of theft cannot be detected [XIV].

1.3. Sybil Attacks Ways

If access can be gained to the sensor network by Sybil attacker then the attacker can perform its operation in following ways:

Routing Sybil attacks can even disturb the routing protocols in wireless sensor networks, especially geographical and location based routing protocols. The regular nodes can exchange the location information during routing and the packets addressing is also done geographically. In geographical routing the Sybil nodes may appear at more than one place at one time [XV]. In this type of attack, when routing is disturbed, the regular nodes can send the packet to malicious node and then the malicious node will not transmitting the packets to the destination [XI].

Voting type Sybil attack is created in systems where voting scheme is used to take decisions in sensor network. For example, reporting and analyzing the behaviour of malicious nodes. The attacker node can create multiple identities to report the regular nodes. By repeatedly reporting, the regular nodes can even be removed from the network. Thus this attack is destructive in nature.

The file systems in wireless sensor network can also be attacked by the Sybil attack. This type of attack is on data fragmentation and data replication in the file system. When the Sybil node is having multiple identities in the system, then the

attacker can get the data easily from memory. When the distributed storage system is created to fragment or replicate the data across multiple nodes, then it actually started storing the data on forge identities.

Data aggregation eliminates redundant data transmission and thus improves the lifetime of sensor network. In this type of attack ,the Sybil node can add malicious information to the aggregation process and finally the result will be in inconsistent form. The malicious node can modify the aggregation process with multiple identities [X].

II. Related Works

The sensor nodes in WSNs are deployed in hazardous and unattended environments, which cause the sensor network to suffer from various types of attacks and in addition to attacks found in traditional networks [XVI]. The security measures are required to improve the security of the sensor network. The security measures of sensor networks are different from security measures of other networks. The security measures of sensor networks should accurately detect and defend attacks in resource constrained sensor networks [VI]. Recently, lot of attention has been given to the trust concept to increase security and reliability in adhoc[XVIII] and sensor networks[XIII]. Trust is calculated as an expected value of the parameter output and the behaviour of the node is decided upon a global threshold; if the trust value is below a threshold, the node is malicious, otherwise it is regular cooperative node. The survival of a sensor network is dependent on the cooperative and trusting nature of its sensor nodes. The trust establishment in the network nodes is mandatory to analyze and evaluate the trustworthiness of other nodes. The use of trust concept for the detection of Sybil attack in MANETs and other systems is already proposed in some literatures. The trust topic in WSN for the detection of Sybil attack is still an open challenge. The authors in the literature review proposed various threshold parameters for the detection of Sybil attacks such as identity, energy, behavioural characteristics etc. Following are the some of the related work in the literature.

V. Sujatha et al. [XXIX] discussed three levels of process for the detection of Sybil node in the sensor network. At first level, the certificate of the node is verified against the certificate stored in the group head of the location. At second level, it construct a distance table, where the proposed method consider the distance between the neighbouring node. At third level when a node enters and exit the sensor network, the method check the variation in RSSI value. Based on three levels of checking , the proposed method declares the node as Sybil node, if a node do not pass the three level of checking. The authors showed the proposed method a robust approach in detecting Sybil nodes in the mobile wireless sensor networks. The limitation of proposed method is storing and exchanging of certificates by group head consumes lot of energy.

Rupinder Singh et al.[XXXI] discussed a trust based identity detection (TBID) scheme for the detection Sybil nodes. The proposed scheme is based on calculating the trust values of neighbouring nodes. The nodes with trust values less than the threshold value are declared as Sybil nodes. The trust value is calculated on the basis of number of times a node changes its identity. Whenever a node changes its identity,

it will have different neighbours. The trust value of node is decreased when it changes its identity. The authors three phases for detection of Sybil nodes which includes Node behaviour determinations, Trust value calculations and finally separation of Sybil Nodes. The authors evaluated the effectiveness of trust based identity scheme using ns2 and showed results showed a high performance for the factor of throughput, PDR, delay, overhead. The limitation of the proposed scheme was that the authors done the implementation using only 42 nodes and with limited parameters only.

G.D. Putra et al.[XXIII] presented a trust based approach in adjacent vehicles to detect Sybil attacks in VANET. The VANET systems have no dedicated infrastructure and thus relying only on the vehicle to vehicle communications. The trust system proposed is based on the message passing between adjacent vehicles in the transmission range of vehicles. The method follows a basic principle that says vehicles transmission range is limited, including the forge identity vehicle. The limited transmission range of vehicle will create a different group of neighbours and thus making it exploitable to perform collaborative inspection to identify a normal and impersonated vehicle. The neighbouring vehicles are informed about the malicious identities through a public channel utilizing Diffie-Hellman key distribution. The limitation of the proposed scheme is that it assumed the vehicles mobility in high density environment and attacker node transmission power is limited. The proposed scheme works well on a lab-scale environment as per the conditions assumed by the authors but the real-world implementation of proposed scheme will be difficult as per the conditions.

Samaneh Rashidibajgan [XXVIII] proposed a new scheme for trust in opportunistic networks to detect Sybil attack. Opportunistic networks allow user nodes to connect to each other via wireless communication without connecting to the internet. The nodes in the network can be trusted or untrusted nodes. The nodes trust is checked by analyzing the received signals from neighbours and node's prior knowledge. The nodes in the network maintain an observation table where the nodes record the observations of neighbouring nodes in this table. When nodes are in the communication range and made a trust with each other, they start exchanging and updating the observation tables. The proposed approach simulation results shows improve false positive rate and accuracy in the network.

Noor Alsaedi et al. [IV] discusses energy trust model for detecting Sybil attacks in clustered wireless sensor networks. The trust model proposed works on three steps to detect Sybil nodes. The first two step is verify the identity and position of a node but the third step add energy as a metric parameter. The energy transmission value received by cluster head from sensor nodes are compared against energy value saved in cluster head for the calculations of trust value. The authors further cancel any feedback and recommendations between sensor nodes and cluster heads of the system to save energy and reduce communication overhead. The limitation of this scheme is that the authors assumed that cluster heads are trustful and are not compromised by any attack. The other limitation is the authors used only energy as a limited parameter for calculation of trust values.

Aditi Paul et al.[XXIV] discusses a new approach based on trust model to defend Sybil attack. The proposed trust model is based on fuzzy system and neural networks. The proposed method has three phases. In the first phase, the Sybil nodes are detected on the basis of behavioural observations. In the next two phases, the nodes detected in first phase as Sybil nodes are verified using fuzzy inference and neural network expert system. The head node calculates a resource utilization of all other nodes and set a threshold value at particular time. Any deviation from threshold value decreases the trust value of that node and finally the distrust node behaviour is determined by a neural network to decide that the node is Sybil or not. The authors discussed that using three phases, the accuracy level in detecting Sybil node is increased.

Huanhuan Zhang et al. [XXXVI] uses trust and distrust information to defend Sybil attacks on online social networks. The authors first utilized the similarity-based graph pruning through which the entire network is divided into non-Sybil and Sybil regions. Secondly the authors proposed unified ranking mechanisms to detect Sybil nodes where trust and distrust scores are formed by the nodes in the network. The authors also use existing anti-Sybil methods to produce reliable Sybil seeds. Various experimental results are presented like calculation of false positive and false negative to show that the proposed methods achieve better performance than existing techniques.

Guojun Wang et al.[XXXIV] proposed a trust system against Sybil attack in peer to peer e-commerce applications using neighbour similarity. The objective of the trust system is to ensure that honest peers are identified accurately as trustworthy and Sybil peers as untrustworthy. The authors used the trust parameters like historical factors of the peers and recommendations from other peers to detect Sybil peers in the network. A peer trust value is increased on the basis of positive recommendation and peer trust value is reduced on negative recommendations from other peers. In case, distrust value reaches a certain threshold value, the peer can be expelled from the group.

III. Proposed energy model for Sybil node detection

This research work is based on the isolation of malicious nodes based on trust factor of the sensor node. The trust model uses energy as a parameter for the detection of Sybil nodes. The network architecture, assumptions and proposed trust based energy model and other factors is explained as follows.

III.i. Network Architecture

Wireless Sensor Network (WSN) consists of large number of self-organized sensor nodes which communicate via wireless medium. The sensor nodes are placed in hazardous and unattended environment to sense and collect data around them. When the sensor nodes are deployed in remote location and left unattended, they can be compromised by various attacks like selective packet dropping, Sybil attack etc. The Sybil attacker can mislead other regular nodes by showing multiple false identities or duplicate identities of the regular nodes in the sensor network. The

multiple identities make fool of the system and cause inaccurate information and affect the functioning of network.

The architecture of proposed technique has four level hierarchical systems. The hierarchical system includes four kinds of nodes: Sensor nodes, Cluster head (CH), observer node (OS) and Base Station (BS). Sensor nodes are involved in sending, receiving and forwarding messages or packets. Sensor nodes are organized as groups or clusters and cluster head node manages them. Cluster head forward the data obtained from sensor nodes to the base station in the upper layer. The base station is a master node. Data sensed by the cluster heads is routed back to a base station. The base station is a computer where data from the sensor network will be compiled and processed. The base station may communicate with the Remote Controller node via Internet or Satellite [XXVII]. Users controlling the sensor network send query and receive responses through the base station. In the proposed technique, n number of sensor nodes is deployed in the cluster under the control of cluster head node. The observer nodes are the extra nods in the network which are responsible to calculate trust level of the sensor node. The trust level of the sensor node is calculated by the observer node and also calculated by the cluster heads. The cluster head calculate trust factor based on the energy dissipation of the sensor node. The observer nodes calculate trust factor based on the four factors which are residual CMF, DMF, residual energy and honesty factor. The sensor is considered as the malicious node when the any sensor node is declared as un-trusted node both by the cluster head and observer node. These nodes are well equipped, energy efficient and promising nodes in the network.

III. ii. Network Assumptions

The proposed trust based energy model is based on various assumptions which are as follows:

- n sensor nodes are deployed in the network forming clusters with each having a cluster head. All the sensor nodes are assumed to have similar capabilities along with similar workload and their behaviour is similar under normal conditions.
- The network consist of a malicious node who do alterations or dropping of packets before forwarding them. The malicious nodes have network resources similar to normal nodes, but have different behaviour as compared to others.
- Each sensor node continuously listens to the network channel in order to observe various parameters.
- Base Station and Cluster Heads are trustful and are not compromised by any attack. In addition, they have more power and resources than sensor nodes.
- The unique identity ID and location information LOC about each node remains same whereas energy used in transmission E_T is updated with every acknowledge response ACK.
- The observe nodes are deployed in the network which calculate trust of the sensor nodes. The observer nodes calculate trust based on the four factors which are CMF, DMF, residual energy and honesty level.

- The sensor node is declared as the malicious nodes when both observer node and cluster head declare an node as untrusted node.
- The election of cluster head could be chosen based on an election protocol such as HEED [XXXIV]
- MAC Layer protocol exists in the network that is used to manage broadcasting of packets to avoid occurrence of a collision.

III. iii. Trust Calculated by the cluster head

The cluster head calculate the trust of the sensor nodes based on the energy model. This trust calculation model is lightweight can easy to implement. The Sybil attack is that attack in which the malicious node illegitimately takes multiple identities and finally the whole functioning of the network is disturbed [XXX]. The trust based energy model is based on a network in which the whole network is divided into clusters with each cluster having a number of sensor nodes. There is one cluster head node which managers the sensor nodes in its cluster. The election of cluster head is based on an election protocol HEED [XXXV]. HEED is hybrid energy-efficient distributed clustering approach and is used to increase the lifetime of sensor network by selecting the cluster head based on the residual energy of each sensor node. The probability of becoming a cluster head, CH_{pr} as follows

$$CH_{pr} = Cper \times E_{UN}/E_M \quad (1)$$

Where

Cper: Initial percentage of cluster head among all n nodes (say 5%). It is used to limit the initial cluster head announcements.

E_{UN} : The current unused energy in the sensor node.

E_M : Reference maximum energy of the sensor node.

During sensor node creation, each node will receive a request (REQ) message from cluster head. The entire node responds to the cluster head with a acknowledge (ACK) message with <ID, Location, and Energy transmission>. Then this information is stored in a NODE INFO_table under the control of cluster head of the cluster. The entire cluster is presented as in equation (2)

$$C= \{(n1, n2,.....ni), CH\} \quad (2)$$

Where m is the number of nodes in the network. Each node is deployed in the network as LOCATION(ni)= (rand(x), rand(y)), where x,y is any location within the network area. The cluster head sends a request REQ packet to all the newly created nodes in the cluster which can be written as in equation (3) :

$$CH(Msg, TS) = \sum_{i=1}^{m} ni \quad (3)$$

Where n1, n2.....ni are nodes.

The energy trust model works in three phases: Analyzing, Calculations and Filterations

III. iii. A Analyzing

Each node in the network is sending an acknowledgment (ACK) packet to the cluster head (CH), which can be written as <ni ACK CH>, where the ACK packet consist of following:

$$ACK = \{ID(ni), LOC(ni), E_T(ni), TS(ni)\} \quad (4)$$

Where

ni denotes the ith node.

ID(ni) denotes identity of the ith node.

LOC(ni) is the position of the ith node.

E_T (ni) is the energy used in transmission of ith node.

TS(ni) denotes the timestamp of the ith node.

The parameter E_T is used to verify that the node is a Sybil or not.

III. iii. b Trust Calculations

The trust for every sensor node depends on the energy factor associated. Each node

will receive a request REQ message from cluster head. The entire nodes respond to the cluster head with an acknowledgement ACK message. The ACK message is analyzed by the cluster head. The energy used in transmission (E_T) is calculated using the equation (5)

$$E_T = \sum(E_U + E_{UN}) \quad (5)$$

$$E_U = \sum E_S = E_T + E_R + E_{SH} \quad (6)$$

The sensor node sends its ACK to its cluster head and when a ACK arrives at cluster head, the cluster head detect Sybil attack the basis of energy used by a sensor node. The cluster head node checks E_T in equation (7).

$$E = E_T + E_V \quad (7)$$

Notation used above:

E_U : Total energy used by a sensor node

E_{UN} : Energy that is left unused in a sensor node

E_S : Energy used in all the states of a sensor node

E_T : Energy used in transmission to cluster head

E_R : Energy used in receiving the data

E_{SH} : Energy used in shifting from one state to the other state

E : The value of energy of a sensor node as saved in cluster head

E_V: Energy variation rate.

The sensor node is declared as untrusted node by the cluster head on the basis of equation (7). When ($E= E_T + E_V$), then trust (T) number is increased; otherwise, the distinct (D) number is increased. When the distinct value is increased to threshold then that node is declared as untrusted node.

The trust and distrust amounts were calculated on the result of equation (8)

$$E \begin{cases} = E_T + E_V \text{ , This increases the trust value (T)} \\ \neq E_T + E_V \text{, This increases the distinct value (D)} \end{cases} \quad (8)$$

III. iv. Trust Calculated by the Observer nodes

In the network some observer nodes are deployed which does not perform any task of data sensing. The observer nodes only observe behaviour of the sensor nodes which are present in the network. The observer nodes are responsible to calculate the trust values based on the behaviour of the sensor node. The observer node calculates the indirect trust. The observer node calculates below factors based on the communication between sensor nodes and cluster heads. The trust of the sensor node is calculated based on the four factors. The factors which are included to calculate trust value are :-

1. Control Message Forwarded (CMF):- The control message forwarded is the first factor which is involved in the trust calculation. This factor is represented by the CMF notation. The CMF is calculated based on number of control messages correctly forwarded by the sensor nodes to cluster head against total number of control messages.
2. Data Messages Forwarded (DMF):- The data message forwarded is the second factor which is involved in the trust calculation. This factor is represented by the DMF notation. The DMF is calculated on the basis of number of data message corrected forwarded by the sensor node to cluster head against total number of data messages.

3. Residual Energy:- The third factor is the residual energy and it depends upon the activity of the sensor node. The activity means number of packets received or transmitted by the sensor node. The residual energy also depends upon the traffic which is overheard by the sensor node during ideal condition. The energy consumption of the sensor node needs to be calculated before calculating residual energy. The energy consumption of the sensor node is calculated by adding energy consumed during data transmission and energy consumed while receiving data. The energy consumed during data transmission is given by equation 8 and energy consumed during data transmission is given by equation 9

$$E_{Tx}(k, d) = E_{elec} * k + \epsilon_{amp} * k * d^2 , d>1 \quad (9)$$

The $E_{TX}(k,d)$ is the energy consumed during data transmission. E_{elec} is the energy consumption to carry out data transmission and it is calculated in terms of nj/bit. The k is the volume of data which is transmitted by the sensor node. The ϵ_{amp} is the constant which define the energy consumption for the expansion of coverage area. The d is the distance between the data sending node and data receiving node

$$E_{Rx}(k) = E_{elec} * k \quad (10)$$

The E_{Rx} defines the data consumed while receiving data. E_{elec} is the energy consumption to carry out data transmission and it is calculated in terms of nj/bit. The k is the volume of data which is received by the sensor node

The total energy consumed by the sensor node is given by the equation 11

$$Total_{EC} = \Sigma E_{Rx} + \Sigma E_{Tx} \quad (11)$$

The $Total_{EC}$ is the total energy consumed by the sensor node. The E_{Rx} is the energy consumed while receiving data. The E_{Tx} is the energy consumed during data transmission. The residual energy is calculated by subtracting total energy consumed from initial energy of sensor node. The residual energy is calculated with the equation 12

$$Energy_{residual} = Energy_{initial} - Total_{EC} \quad (12)$$

The $Energy_{residual}$ is the residual energy of the sensor node. The $Energy_{initial}$ is the initial energy of sensor node. The $Total_{EC}$ is the total energy consumed by the sensor node

4. Honesty level: The honest level of sensor node is calculated based on previous experience and basis current misbehavior activity, average misbehavior activity and current honesty level. The current honesty level is measured based on the past malicious activities of the sensor node. The honesty level of the sensor node is defined with the equation 13

$$A_{xy} = \frac{Bxy}{Bxy + Cxy} \quad (13)$$

The Bxy is the bad behavior of the sensor node and Cxy is the good behavior of the sensor node. The Axy define the honesty level of the sensor node. The bad behaviour of the sensor node is calculated based on the number of data packets which are incorrectly forwarded by the sensor node. The good behaviour means the number of packets which are correctly forwarded by the sensor node.

The trust value of the sensor node is calculated by the observer node and it is defined with the equation number 14

$$Trust = weight1 * CMF + weight2 * DMF + weight3 * residual\ energy + weight4 * honesty\ level \quad (14)$$

The trust value of the sensor node is combination of the control message forwarded, data message forwarded, residual energy and honesty level. The weight 1,weight 2 ,weight 3 and weight 4 are the weight ratio of factor which is associated with that factor. The weight varies from 0 to 1, the weight is empirical factor and addition of

weight 1, weight 2, weight 3 and weight 4 is 1. The threshold value of the trust is defined as α, if the trust value of the sensor node is below α then that node is declared as the untrusted node.

III. V. Filtering of malicious nodes

The filtering process will filter the malicious nodes from the sensor network. The architecture of the proposed mode is presented in the figure 3.

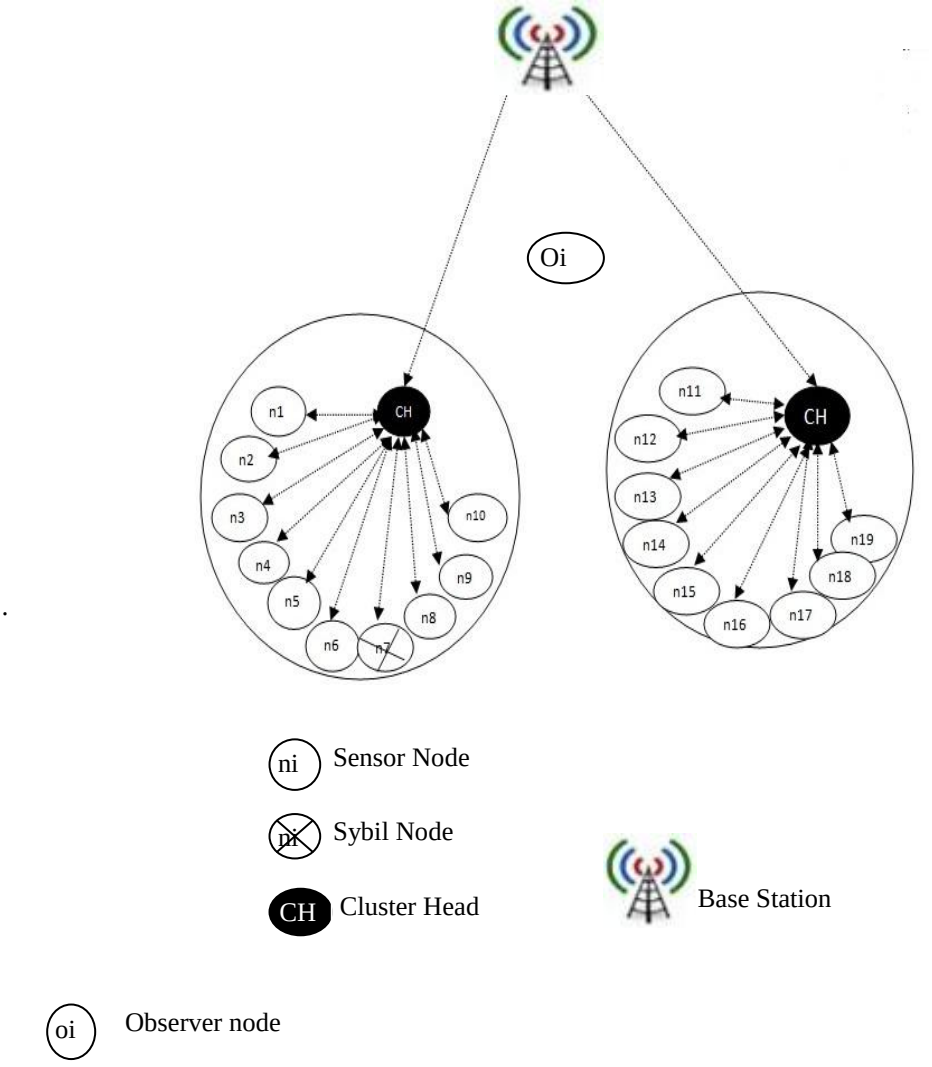

Fig. 1. *Proposed Architecture*

Fig. 3 shows a wireless sensor network having Sybil

nodes. The figure consists of two clusters with cluster

As shown in figure 3, the Cluster head (CH) is represented in dark black oval. The cluster on the left consist of sensor nodes from n1 to n10. The sensor nodes are represented as normal oval. The observer nodes are represented with the normal oval shape. The node n7 in the network is Sybil node and is represented as crossed oval. The Sybil node n7 mislead the network functioning and cause inaccurate information into the network. The Sybil attack detection is to reveal fake identities of the network.

The table (I) shows the trust values which is calculated by the cluster head and observer nodes. The clusters head calculate the trust based on the energy consumption of the sensor node correspond to the ACK messages. When the energy consumption of the sensor node is not equal to correspond to ACK value then the distinct value is increased. When the distinct value is increased to threshold value then that node is declared as the untrusted node. The energy calculation of the sensor node by the sensor node is shown in the table (I). The trusted node is defined with the T notation and untrusted node is defined with the notation as U. The observer nodes also define the trusted and untrusted nodes on the basis of four factors which are already defined. The notation of the trusted node is T and notation of untrusted node is U. As shown in the table (I), the node 7 is declared as untrusted by the both cluster head and observer then that node is declared as the malicious node.

Table I: Trust Calculation

Node	ID	E_T	E_V	E	CH	OB	Final Decision
n1	1032	2400.13	917.22	3317.35	T	T	Normal
n2	1211	2099.23	802.32	2901.55	T	T	Normal
n3	1321	1343.9	772.10	2116.20	T	T	Normal
n4	1512	230.17	90.32	320.49	T	T	Normal
n5	1302	352.65	102.32	454.97	T	T	Normal
n6	1451	2692.96	998.72	3691.68	T	T	Normal
n7	1092	3201.12	1011.11	3867.71	U	U	Malicious
n8	1144	1548.6	823.12	2371.72	T	T	Normal
n9	1231	2541.59	923.21	3464.80	T	T	Normal
n10	1405	1521.46	901.11	2422.57	T	T	Normal

The working of trust calculation of the sensor node by the cluster head is shown in the figure 4.

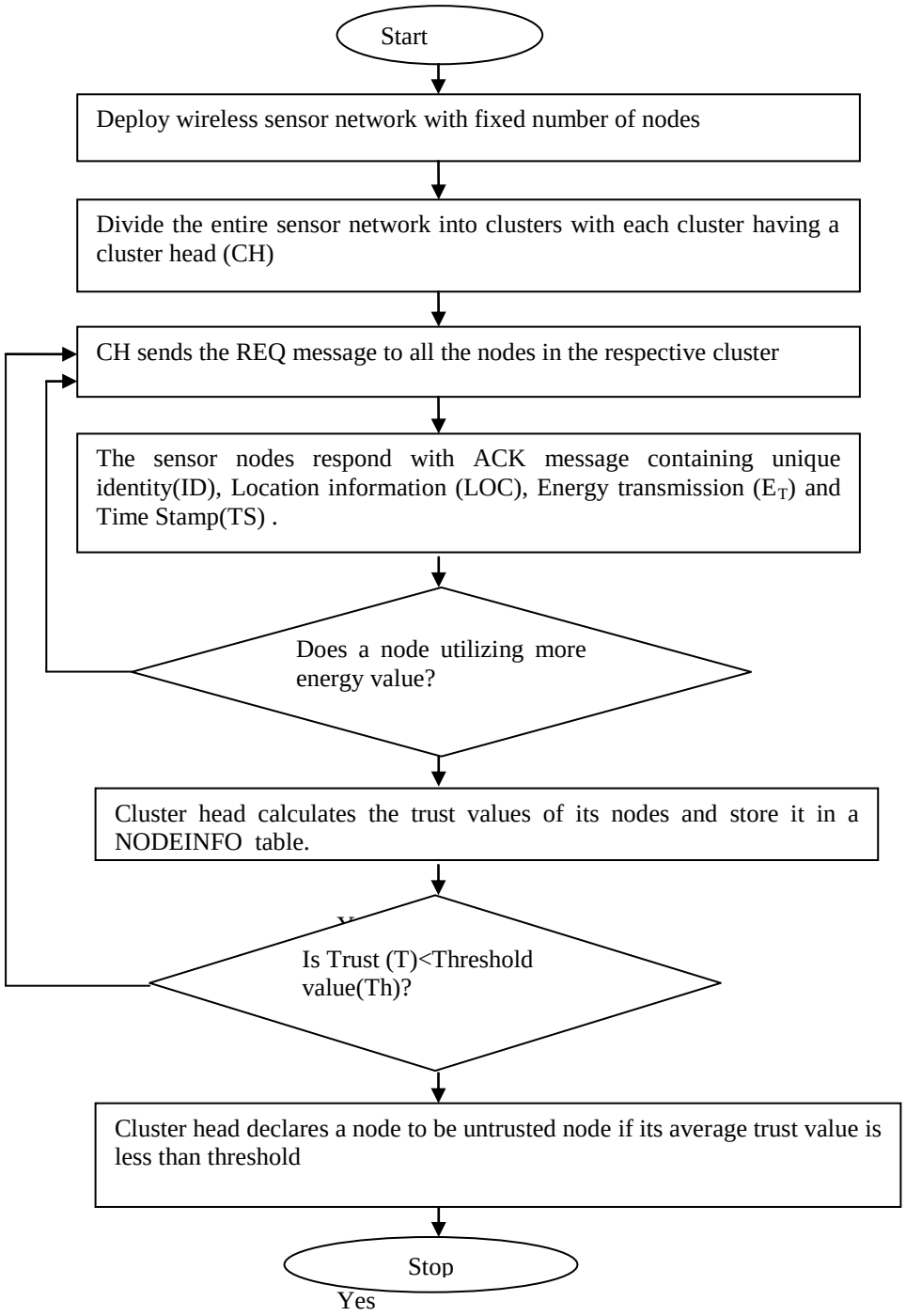

Fig.4. *Flowchart of trust calculation by cluster head*

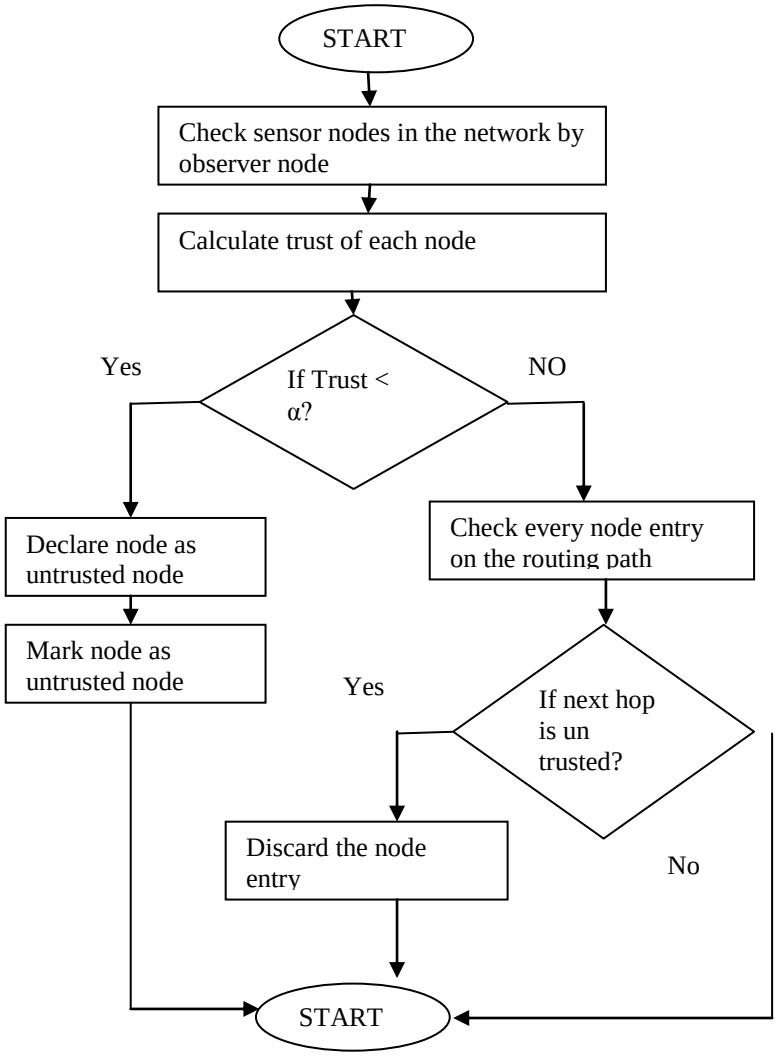

Fig.5. *Flowchart of trust calculation by observer nodes*

IV. Results and Discussion

The entire trust system model is simulated using NS2 software with 23 nodes with a network size of 800X800. All the nodes are divided into clusters and single base station is deployed in the network. The cluster head is selected in each cluster based on the energy model of HEED protocol. The cluster head of each cluster will send REQ message to sensor nodes within the cluster. All sensor nodes respond with acknowledgement ACK message to cluster head back. The cluster head analyzed the ACK of all the nodes and compares ACK received with the values stored in the table in cluster head. Cluster head finds that the energy value stored in table is not matched with the energy value in ACK received. The cluster head increases the distrust value (D) of node suspicious nodes for that time period (stored in time stamp (TS) received).

After a particular timing window, the distrust value (D) increased above the threshold value; the CH declares untrusted nodes. The observer nodes are deployed in the network which observes behaviour of the sensor nodes. The nodes also calculate trust value of the sensor nodes. The trust value of the sensor nodes is calculated based on the four factors which are DMF, CMF, residual energy and honesty of the sensor node. When the trust value of the sensor node is reduced to threshold value than that node is declared as the untrusted node. Any sensor node which is declared as untrusted by the cluster head and observer is considered as malicious node.

3.1. Pros of the proposed scheme

- The scheme uses the mechanism of cancellation of any suggestions among the sensor nodes which decreases the memory and processing overhead.
- The scheme is reliable and accurate in detecting the Sybil attack with less number of false positive and false negative.
- The scheme detects all classification of a Sybil attack
- The proposed scheme also detect the stolen identify Sybil attack
- The proposed scheme is two steps verification scheme which increase its reliability
- The proposed scheme can be employed in the ad hoc network for the detection of misbehaviour nodes

The simulation parameters for simulating proposed system is described in table 2

Table 2 Simulation Parameters

Parameters	Values
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	23
Number of Sources	1
No. of Adversaries	1 to 3

The wireless sensor network is deployed randomly with the 23 number of sensor nodes and all the sensor nodes has similar configuration is terms of hardware and

software. The sensor network is deployed randomly and has single base station. The network deployment scenario is shown in figure 5

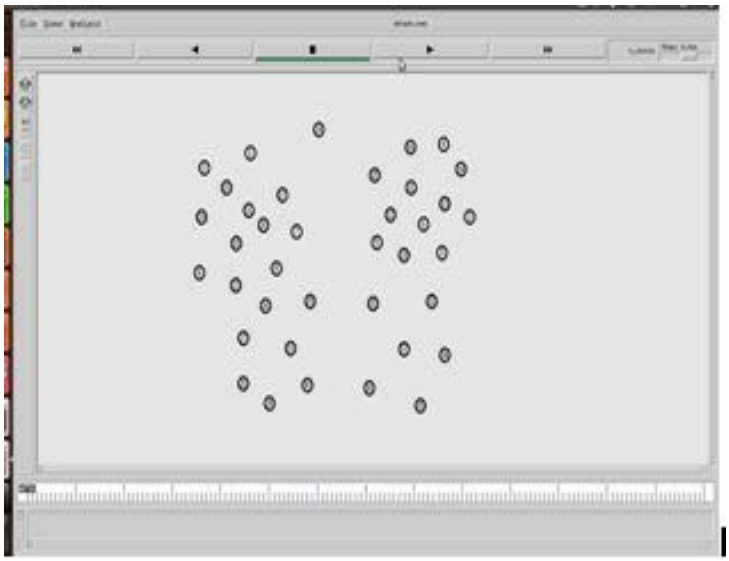

Fig.5. *Network deployment*

The sensor nodes take random position as the time of deployment and network is divided into clusters according to node locations. The sensor node which has similar location is clusters into one cluster and other are clusters into another cluster. The division of network into clusters is shown in the figure 6

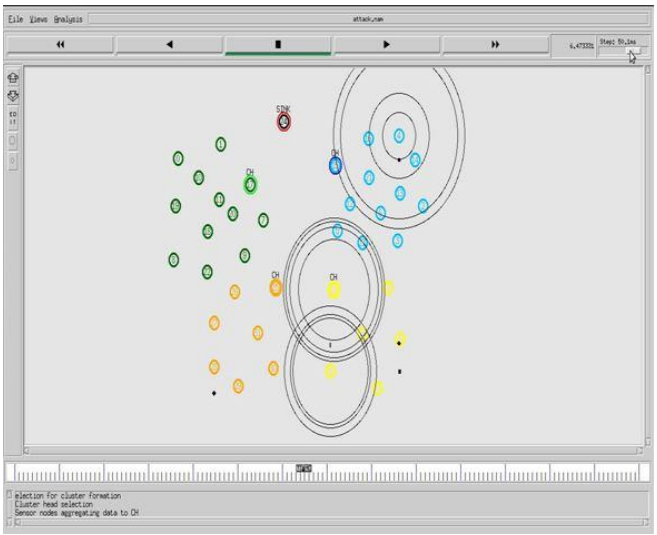

Fig.6. *Division of clusters*

Each cluster in the network has single cluster head and cluster heads are selected with the energy model of HEED protocol. In the cluster head selection process, the sensor

node which has maximum energy and least distance to base station is selected as cluster head. The cluster head in the network is responsible to transmit aggregated data to base station. Due to dynamic topology of the network malicious nodes enters the network which is responsible to trigger Sybil attack in the network. The detection of malicious node is shown in figure 7. The malicious node in the network is detected on the basis of trust calculation

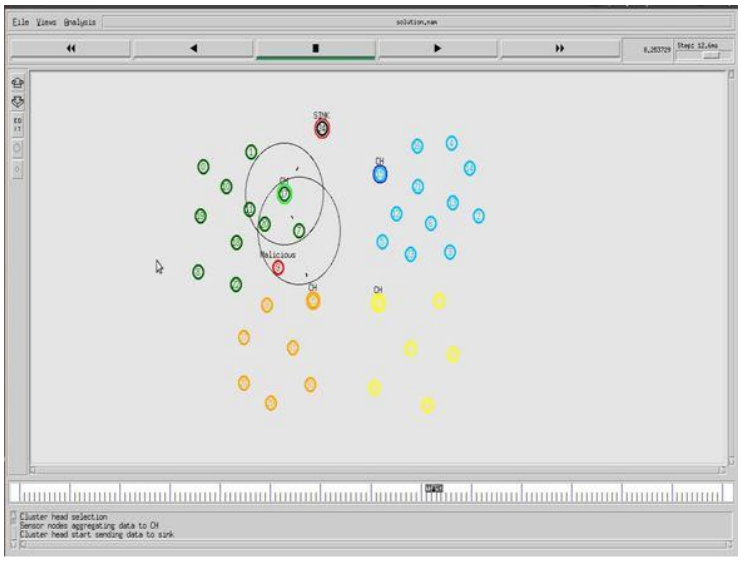

Fig.7. *Malicious node Detection*

The cluster head send REQ message to each node in the cluster. The sensor nodes reply back with the ACK message and sensor nodes which has abnormal energy consumption is declared as the untrusted node.The observer nodes also calculate the trust factor of the sensor nodes and if it is below threshold then that nodes are declared as untrusted nodes. When the cluster head and observer node declare one node is untrutsed node, then that node is considered as the malicious node. The technique of multi path routing is applied for the isolation of malicious node from the network

V. Performance Evaluation

In order to access performance of proposed trust based model and compared to other well know techniques for the detection of malicious nodes in the network. The performance of proposed trust based model and other techniques are presented in this section. The PDR, energy and delay are parameters which used for the performance evaluation

V.i Performance Measure

The parameters used for the performance analysis are described below:-

- **Packet Delivery Ratio**

It is defined as the ratio of total packet data received to the total data sent by the sources. It is consider as the important metric in the network. The networks can

face congestion due retransmissions occur at high loss rate of packet at the intermediate nodes which uses TCP as the 2nd layer protocol in certain applications.

$$Packet\ Delivery\ Ratio = \frac{Total\ \ Data\ \ packets\ \ recei\ ved}{Total\ \ data\ \ packets\ \ sent}$$

- **Average End-to-End Delay**

Route discovery latency, retransmission by the intermediate nodes, processing delay, queuing delay, and propagation delay are all caused by end-to-end delay in the network. It is defined as the every delay can be added to each successful packet data delivery and than that sum is divides the number of total received data packets which is further used to find average end to end delay value. Video and voice transmission delay applications are proved to be more important and helpful.

$$Average\ End\ to\ End\ Delay = \frac{\sum(Time\ \ Received\ -Time\ \ sent\ )}{Total\ \ Data\ \ Packets\ \ Received}$$

- **Energy Consumption**

The energy consumption is the parameter which measure amount of energy. The energy consumption is measured with amount of number of packets multiplied per unit energy

$$Energy\ Cosumption = \ No\ of\ packets * per\ unit\ energy$$

V. ii. Experimental Results

The experimental results of the proposed trust based model are compared with the trust based model [26]. The performance is compared in terms of PDR, delay and energy consumption. The results are analyzed on the different set of nodes. The different set of nodes which are taken for the performance analysis are 23, 50, 75 and 100. It is analyzed that proposed trust based model performs well as compared to trust based model [26].

It is analyzed that energy consumption of the proposed trust based model is low as compared to trust based model [26]. The results of the energy consumption are analyzed in different set of nodes. On all the set of nodes proposed trust based model performs well as compared to trust based model. The comparison of energy consumption is shown in the figure 8

The proposed trust based model is compared to trust based model in terms of PDR (packet delivery ratio). The performance of proposed trust based model is high as compared to trust based model [26]. It is analyzed that performance of proposed trust based model is high. The performance of both models, i.e. proposed trust model and trust model. It is analyzed that PDR value of proposed trust based model is high as compared to trust based model. The comparison is shown in figure 7

The performance of trust based model [26] and proposed trust based model is compared in terms of delay. It is analyzed that delay of the proposed trust based model is less as compared to trust based model. The performance of both the models is tested on the different set of nodes like on 23,50,75 and 100. On the number of nodes proposed trust based model performs well as compared to existing trust based

model. The comparison between trust based model and proposed trust based model is shown in figure 9

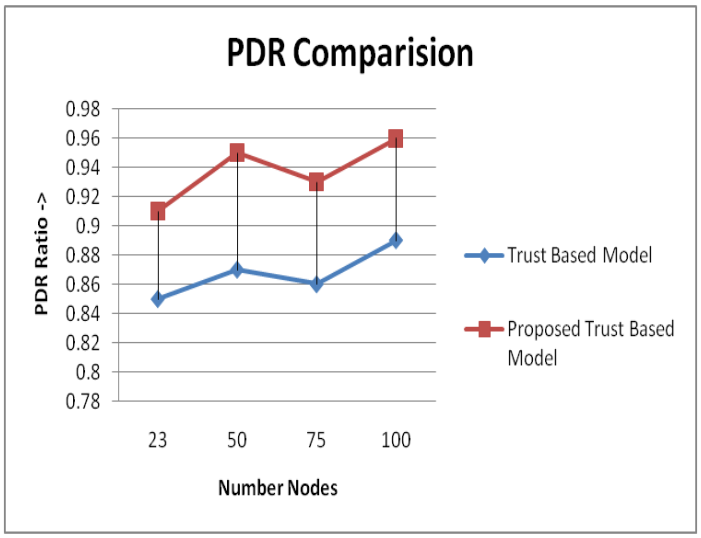

Fig.7. *PDR Comparison*

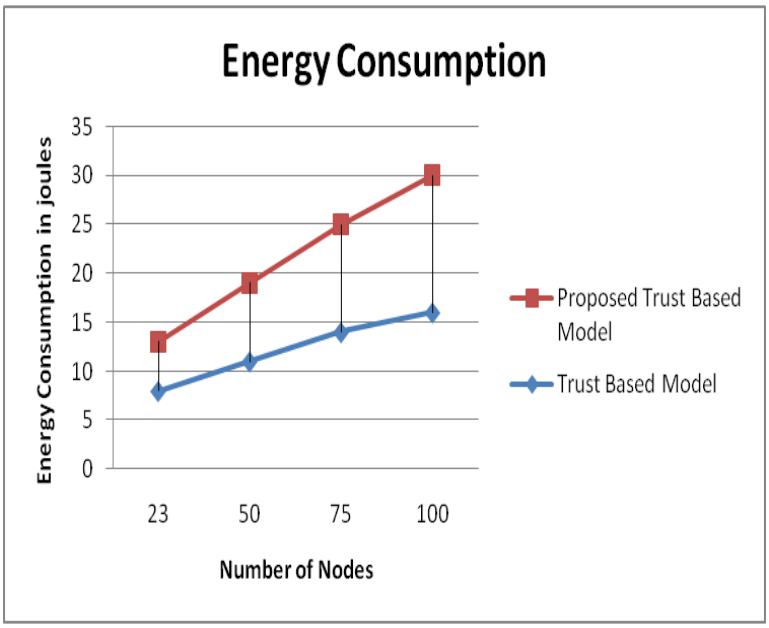

Fig.8. *Energy Consumption Comparison*

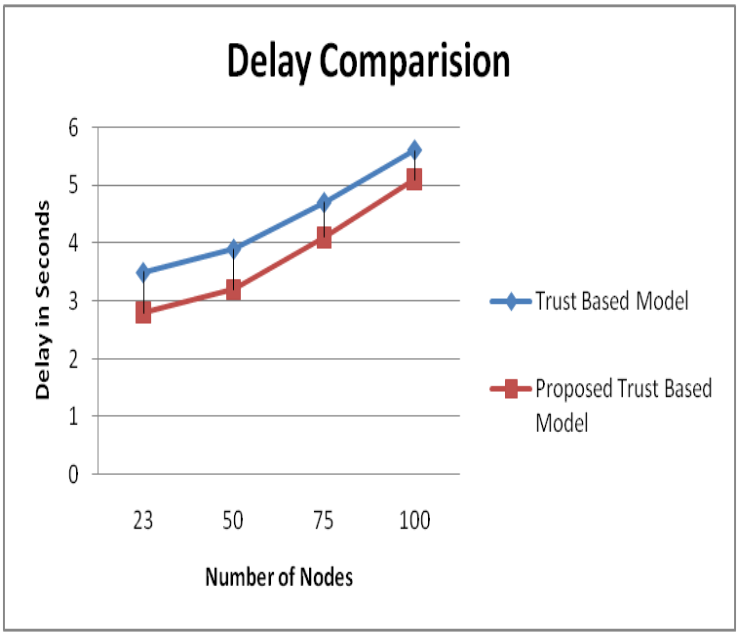

Fig.9.*Delay Comparison*

VI. Conclusion

The wireless sensor network has the dynamic nature due to which malicious nodes enter the network which affect network performance. The Sybil attack is the active attack in which attacker change its identifications multiple and source starts transmitting data to malicious nodes. The Sybil attack is the denial of service network of attack which reduces network performance. In this research paper, two step verification based security model is presented which detect malicious nodes from the network. In the proposed model cluster heads and observer nodes are responsible for the detection of malicious nodes. The observer nodes are extra nodes which are deployed in the network which observe network traffic. On the basis of its observations, it declared sensor nodes as trusted or untrusted. The cluster heads are selected from the network using HEED protocol. In every cluster, the single cluster head is selected which also declare node as trusted or untrusted based on energy consumption. The proposed model is implemented in NS2 and results are analysed in terms of Delay, PDR and energy consumption. The comparative analysis is done between the trust based model and proposed trust based model which is also called two step verification technique. It is analysed proposed trust based model performs well as compare to trust based model in terms of all defined parameters. In the fake packets can be inserted in the network to confuse the malicious node which will be the future recommendations of this work.

VII. Acknowledgments

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct the research work.

VIII. Conflicts of Interests

The authors declare no conflict of interest.

References

I. Akyildiz, I.F., Su, W., Sankarasubramaniam, y., Cyirci, E., 'Wireless sensor networks: a survey. Computer Networks', Vol. 38 no.4: p. 393-422, 2002.

II. Abirami, K., Santhi, B. (2013). ' Sybil attack in wireless sensor network', International Journal of Engineering and Technology, 5 (2), pp. 620-623.

III. Abirami, K., Santhi, B. , 'Sybil attack in wireless sensor network'. International Journal of Engineering and Technology, 5 (2), pp. 620-623.

IV. Alsaedi N, Hashim F, and Sali A. 'Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks'. IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, Nov 2015.

V. Cheng, C., Qian, Y., & Zhang, D. , 'An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Networks'. International Journal of Distributed Sensor Networks, 2013.

VI. Cheikhrouhou O., 'Secure Group Communication in Wireless Sensor Networks: A survey', Journal of Network and Computer Applications, Feb. 2016, vol. 61, pp. 115–132.

VII. Douceur J. R., 'The sybil attack', in Proc. 1st Int. Workshop Peerto-Peer Syst., London, UK, Mar., 2002, pp. 252−260.

VIII. Demirbas Murat, Song Youngwhan, 'An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks', Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570.

IX. Di Pietro R., Mancini L. V., Soriente C., Spognardi A.,

X. Dhanalakshmi T.G., Bharathi Dr.N., Monisha M., 'Safety concerns of Sybil attack in WSN', IEEE 2014.

XI. Demirbas M. and Song Y., 'An RSSI-based scheme for sybil attack detection in wireless sensor networks', Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, 2006, pp. 564-570.

XII. Eschenauer L., 'On Trust Establishment in Mobile Ad-hoc Networks', in Department of Electrical and Computer Engineering, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.

XIII. Ganeriwal S., Balzano L. K. and Srivastava M. B., 'Reputation-based Framework for High Integrity Sensor Networks', ACM Transactions on Sensor Networks, vol. v, 2007.

XIV. Hsu, K., Leung, M. K., & Su, B., 'Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks'. IEEE Journal.

XV. Karlof, C., Wagner, D., 'Secure routing in wireless sensor networks: Attacks and Countermeasures', Ad hoc Networks Journal (Elsevier) 1(2–3) (2003) 293–315

XVI. Kavitha T.,Sridharan D., 'Security vulnerabilities in wireless sensor networks: a survey', J. Inform. Assurance Security , 2010, vol. 5, pp. 31–44.

XVII. Kaschel H., Mardones J., and Quezada G., 'Safety in wireless sensor networks: types of attacks and solutions', Stud. Informatics Control, Sept., 2013, vol. 22, no. 3, pp. 323−329.

XVIII. Liu Z., Joy A. W. and Thompson R. A., 'A Dynamic Trust Model for Mobile Ad-hoc Networks', in The 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS '04), 2004.

XIX. Levine B. N., Shields C., and Margolin N. B., 'A survey of solutions to the Sybil attack', University of Massachusetts Amherst, Amherst, MA, 2006.

XX. Leopold M., 'Sensor network motes: portability and performance',Ph.D. dissertation, Dept. Comput. Sci., Copenhagen Univ.,Denmark, 2008.

XXI. Muraleedharan R., Yan Y., and Osadciw L. A., 'Detecting sybil attacks in image senor network using cognitive intelligence', Proceedings of the First ACM workshop on Sensor and actor networks, 2007, pp. 59-60.

XXII. Prasanna S., Rao S., 'An Overview of Wireless Sensor Networks Applications and Security', IJSCE, vol-2(2), May 2012, ISSN: 2231–2307.

XXIII. Putra G.D., Sulistyo S, 'Trust Based Approach in Adjacent Vehicles to Mitigate Sybil Attacks in VANET', Proceedings of the 2017 International Conference on Software and e-Business, (ICSEB '17) 2017, pp. 117-122.

XXIV. Paul A, Sinha S, and Pal S. 'An Efficient Method to Detect Sybil Attack using Trust based Model'. Proc. of Int. Conf. on Advances in Computer Science, AETACS, Elsevier, 2013.

XXV. Rathod V., Mehta M., 'Security in wireless sensor network: a survey', Ganpat University Journal of Engineering & Technology, vol. 1, pp. 35–44, 2011

XXVI. Rakesh G.V., Rangaswamy S., Hegde V., Shoba G., 'A Survey of techniques to defend against Sybil attacks in Social Networks', IJARSCCE, 2014.

XXVII. Raghunathan V., Schurgers C., Park. S, and Srivastava M. B., 'Energy-aware wireless microsensor networks'. IEEE Signal Processing Magazine 2002, Volume: 19 Issue: 2, Page(s): 40 –50.

XXVIII. Rashidibajgan S., 'A trust structure for detection of sybil attacks in opportunistic networks', 11th International Conference for Internet Technology and Secured Transactions (ICITST) 2016.

XXIX. Sujatha V., Mary Anita E.A., 'An efficient trust based method for Sybil node detection in mobile wireless sensor network', Proceedings of the 3rd International Conference on Applied Science and Technology (ICAST'18) AIP Conference Proceedings, 2018.

XXX. Singh, Kumar Shio, Singh M. P., and Singh D. K., 'A survey on network security and attack defense mechanism for wireless sensor networks', International journal of computer trends and technology 2011, Vol1, no. 2, pp. 9-17.

XXXI. Singh R., Singh J., and Singh R., 'A novel sybil attack detection technique for wireless sensor networks', Advances in Computational Sciences and Technology 2017, vol. 10, pp. 185−202.

XXXII. Tsudik G., 'Data security in unattended wireless sensor networks',IEEE Trans. Comput., Nov., 2009, vol. 58, no. 11, pp. 1500−1511.

XXXIII. Wang Q., Balasingham I., 'Wireless Sensor Networks – An Introduction, Wireless Sensor Networks: Application-Centric Design', 2010.

XXXIV. Wang G, Musau F, Guo S, and Abdullahi M B. 'Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce'. IEEE Transactions o Parallel and Distributed Systems, December 2013.

XXXV. . Younis, O., & Fahmy, S. 'HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks'. Mobile Computing, IEEE Transactions on 2004, Vol 3(4), pp. 366-379.

XXXVI. Zhang H, Xu C, and Zhang J. 'Exploiting Trust and Distrust Information to Combat Sybil Attack in Online Social Networks'. 8th IFIP WG 11.11 International Conference, IFIPTM 2014 Singapore, July 7-10, 2014.