International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

Identifying Trustful Node Using Hybrid Trust Evaluation Method

[1*]Mr. S. Ramesh, [2]Dr. R. Kannan
[1*]pursuing Ph.D , Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore.
[2]Associate Professor, Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science.

Abstract: A wireless sensor network referred as (WSN) is defined as a collection of distributed sensor nodes to work together for monitoring the physical and environmental conditions. Trust metrics in the wireless sensor networks is denoted as the important problem and it helps in solving the problem of access control, reliable communication, privacy and secure routing scheme. This paper establishes a new kind of approach to evaluate the trust value in WSN. The proposed algorithm and its evaluation made on the trust value of each node seen in the network depends on the metrics, trust attributesand trust parameters.

Keywords: WSN, Trust, Direct Trust, Indirect Trust, Security, Reliability**.**

1. INTRODUCTION

Wireless sensor networks referred as (WSNs) have thewide applications because of these sensor nodes ease of deployment, such as rescue missions, environment monitoring and smart houses. Maximum interest and effort are being concentrated on this new network topic. But Wireless Sensor networks referred as (WSNs) are stated to be highly vulnerable to attacks because of its nature of the wireless media and restricted resource. WSN that contains the sensor nodes that has only limited communicating capabilities, has only lesser computation power also less memory deployed among the environment to monitor the events and to report back to the cluster head or said as the base station [1]. Due to the wireless nature of everynode, they are vulnerable to various attacks. So, developing the trust framework which addresses the security, reliability, privacy, robustness, authentication and authorization between the wireless sensor networks is very important. In literature, the trust value is essential to consider the level of assurance or confidence that a person can have on another person or a thing. In network, the trust is the level or the degree of confidence that a node has on another node.

Trust (or, said as symmetrically, distrust) is based on a particular level resulted on the subjective probability through which an agent will perform a particular action, that is both before he began to monitor such action (or said to be independently its capacity to monitor it) or in a context in which it may causeaffects to his own action. In WSN, the trust is defined as, “the combined characteristics model for providing the security, reliability, privacy like respecting its mobility is called trust”. Establishing the trust and evaluating the trust value in WSN enables the node can have secure, reliable communication with other node or network depending on their trust values. Trust worthiness of each node produced in the network helps in solving the problem and ensures secure routing, providing reliable path for the packet and the selection of secure mobility model.

1.1. Characteristics of Trust in WSNs

Some essential characteristic features of trust are given as follows:

- Innovative: It might increment else decrement by the period that is dependent on fruitful and ineffective collaborations.
- Intransitive: If node i trusts node j, node j confides in node k. it isn't vital that node i trusts node k.
- Asymmetric: Two or more nodes do not consist of same trust key.
- Trust is closely connected with risk: If there is no danger involved, there is no motive behind to believe.
- Auto catalysis: There are nodes interactions references on the further nodes.
- Unqualified: Node i does not rely on node j for any action, but it will depend on the specification.
- Supportive: The nodes that are produced and organized in environments are supportive to each other by replacing data

1.2. Trust Metrics

Some of the trust metrics are listed below in the Table 1Each of the nodes produced in the WSN shall update the trust metrics of its neighboring nodes for every event recorded in the whole network. The indirect trust that is (IT) on any neighboring node can be evaluated by collecting the information about that node from all other neighbors [2].

Table:1: rust Metrics

SNo	Trust Metrics
1)	Data packets forwarded
2)	Data packet delivery
3)	Control packet/message forwarded
4)	Control packet/message precision
5)	Availability based on beacon/hello messages
6)	Routing protocol execution (routing actions)
7)	Message Cryptography
8)	Consistency of reported (sensed) values/data
9)	Packet Misroute
10)	Reputation
11)	Packet address modified
12)	Battery lifetime
13)	Packet Delay

1.3. Trust Values

Trust values are given to understand the trust stand and behavior of trust (as shown Table2).

Table 2: Trust Value Estimation

Trust Stands	Trust	Behavior of Trust
1	Excessive Trust	Trust
1 to 0.75	High Trust	Trust
0.75 to 0.50	Middle Trust	Trust
0.50 to 0.25	Short Trust	Unsafe
0.25 to 0	Week Trust	Unsafe
0 to -0.25	Short Distrust	Threat
-0.25 to -0.50	Middle Distrust	Threat
-0.50 to -0.75	High Distrust	Threat
-0.75 to -1	Same Distrust	Threat

The trust metrics is considered as very important for the sensor nodes deployed in the unattended and military environments. Hence the evaluation made on the trust worthiness should between the nodes produced among the network to have trusted communication [8]. We look at the issue of security and reliable communication through considering its mobility of the node in the sensor network using the trust evaluation [3].

Hence this paper is structured as follows, Section II, comprise of related works. Section III that clarifies about the proposed algorithm for trust value calculation. The Result & Discussion is shown in the section IV. Finally, section V presents concluding remarks and future work.

2. RELATED WORKS

In [5], proposed a TCNPR trust calculation method is introduced to detect the malicious nodes generated in wireless sensor network and provide trustworthiness between sensor nodes also their neighboursby evaluating different trust metric and recommendations from neighbour nodes. Direct trust is thus evaluatedthrough the properties of nodes which are judged by different trust metrics on the other part the indirect trust is evaluatedthrough the recommendations from neighbours. And also discussed that some properties of node can be of higher priority and other can be of lower priority. Also, priority of trust metrics changes according to the application type.

In [6], a Distributed Trust based Intrusion detection method have been introduced in the wireless sensor network WSNsin order to detect the intrusion through evaluating the trust of sensor node. In this method, a trust is established depending on its different factor of sensor node such as honesty, intimacy, energy, etc.

In [7], present a trust framework model which is evaluated on both the direct trust metrics and indirect trust of any node in WSN based on aggregation. Here the review node or aggregated node improved the essential packet delivery ratio by replacing it with Poisson distribution.Dempster Shafer theory of combiningevidences always gives more accurate outputto find indirect trust. And also calculated the performance of aggregated node that means if though there are some malicious nodes are present, aggregated node do preformed aggregation correctly.

In [8], proposed a safe, flexible, reliable and universal IoT WSN trust computing mechanism. Analyzing the basic features of WSN trust measurement and its design principle of trust computing model, synthetically evaluating direct trust value, indirect trust and intrinsic trust value, this paper tends tointroduce a low complexity and high reliability IoT of WSN trust computation mechanism. It is a lightweight TCMDII trust computation model shows low complexity and just storing local trust information in evaluation node so that greatly reduce node resources loss.

In [9], by estimating the trust metrics of the sensor nodes, a trust management systemdeveloped on the node recovery technique is introducedin order to decrease the probability of task execution failure. At first, the traditional binary model used for the interaction results that is progressed to the trinomial distribution. Secondly, both the direct and the indirect trust degree are calculated through implyingthe effective Bayesian theory and updated through the decay factor to improve the sensitivity. e simulation results proves that our proposed TMBNRT effective

***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

algorithm is bestsuitable on the reliability requirements of Wireless Sensor Network WSN and outperformed other representative algorithms of WSN.

3. PROPOSED METHODOLOGY

Trust Calculation functionsbased on thenode's properties and its recommendations from neighbours method is proposed to calculate trust value of sensor node to detect intrusions in WSN. Based on this method any node belong to WSN can calculate trust of neighbour nodes. Neighbour nodes are those that belong to radio range of sensor node. Trust value is stated as the level of confidence that depends on time. Trust value may change with respect to time based on nodes behaviour while performing transactions among them. The Trust value can be calculated depending on past experience with node and the recommendations that are given by neighbour nodes. Here past experience means behaviour of node through analyzing different factors i.e.,we call them as trust metrics [4][5].

Every sensor node in WSN is expected to update the values of trust (as shown in figure1.) metric about its neighbour node for every activity occurring in network. The record created by observation of neighbour nodes is implied to analyze the Direct Trust referred as (DT) of neighbour node. Indirect trust (ID) of any neighbour node can be evaluated based on information got from all other neighbour nodes.

3.1. Trust Calculation

In this trust calculation method, we divide trust metrics into two types such as high priority metrics and low priority metrics. High priority trust metrics are helpful to see the main functionality of a node. That is why, these trust metrics are not supposed to go below the level of trust threshold level. For example, values of trust metrics that can be data packets forwarded and control packet forwarded that are not supposed to be less than comparing to the higher priority threshold as functionality of nodes are hidden within these metrics. Other metrics of trust can be regarded as low priority category of trust metric.

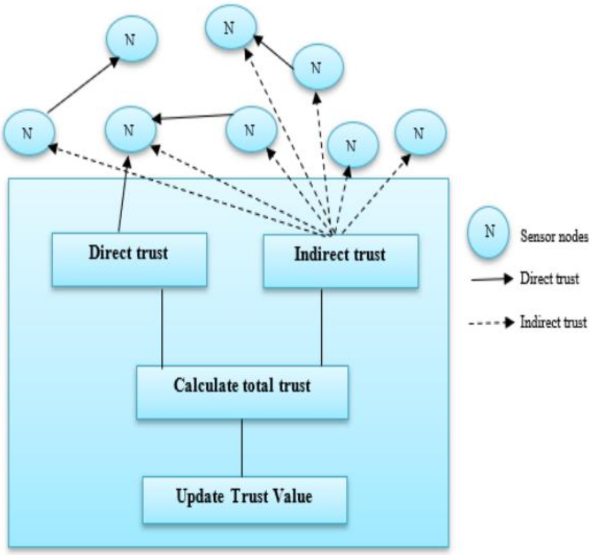

Figure 1: Updating Trust Value

In WSN, a node can have two types of trust

1. Direct Trust
2. Indirect Trust

3.2. Direct Trust

A Direct trust is dependent on the node's own perception in indiscriminate mode. A node can communicate with other node directly in the wireless network and gets all traffic inside its radio reach despite the fact that it isn't routed to it. Every node seen in the network notices neighbors utilizing a trust system that consumes battery power. Sensor nodes functions on the battery as power consumption, if sensor nodes have power, then it communicates or survive in the network.

In our trust calculation model, particularly the direct trust value of any neighbour node is considerably evaluated based on weighted sum of geometric mean of high priority trust metric and the arithmetic mean evaluated on low priority trust metric. Here value of each high priority of the trust metric value must be larger than threshold value. Direct Trust (DT) of neighbour node can be intended based on following equation.

$$DT^{A,B} = \\ +W_L^{DT} X \frac{1}{l} [\sum W_H^{DT} X [\prod (tm_1^{A,B}, tm_2^{A,B}, tm_3^{A,B}, \dots, tm_k^{A,B})] (tm_1^{a,b}, tm_2^{a,b}, tm_3^{a,b}, \dots, tm_k^{a,b})] \quad \text{---- (1)}$$

In above equ (1)W_H^{DT}, W_L^{DT} are denoted as the weights that are assigned to high priority and low priority trust metrics respectively such that W_H^{DT} + W_L^{DT} = 1.

3.3. Indirect Trust

An Indirect trust functions on the other node or recommender for communication in the wireless network.

***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

Indirect trust communicates to node to another node via any recommender nodes in the wireless network. In this Trust model shows the indirect trust how to communicate with deployed sensor nodes and these are in distributed way in the network. Indirect sensor nodes also have battery or power consumption for communication in wireless network.

Indirect trust value of any node in the network can be evaluated based on the recommendations from neighbour nodes. Neighbour nodes can be differentiated into most trusted neighbour or normal neighbour. Every node maintains history of trust apart from trust metric data. Based on the history, some nodes are considered highly trusted and other nodes are considered as less trusted. High trusted neighbour nodes are considered for recommendation as they can recommend positively.

Indirect trust is combination of indirect information obtained through nodes that have high priority and normal neighbour nodes. Hence the Geometric mean will be usedfor high priority nodes and its arithmetic mean will be applied to less priority nodes. W_H^{IT} AndW_L^{IT} are denoted as the weights that areassigned to high priority and low priority nodes correspondingly.Following equ (2) can be implied to calculate the indirect trust in general.

$$IT^{P,Q} = W_H^{IT} X \left[\prod_{i=1\ or\ t} W_{P,N_i} X\ T^{N_i,Q}\right]^{1/r} +$$
$$W_L^{IT}\ X\ \frac{1}{S}\sum_{j=1}^{S}\left(W_{A,N_j} X\ T^{N_J,Q}\right) \text{---- (2)}$$

IT= Geometric mean of high priority neighbour nodes + Arithmetic mean of Low priority neighbour nodes Indirect trust of node P on Q can be computed by using following equation.

Where $W_{P,Nj}$ is recommendation weight made by jthneighbour of node P.

3.4. Hybrid Trust (H)

A new kind of trust evaluation method is defined here that is Hybrid Trust (H) for WSNs. Through implying this method, any node of WSN can illustratethat how much trust it is attained on its neighbouring nodes. Here, neighbouring nodes refers to the, nodes those are connected using theeffective node's radio signal. The trust value, which is referred here is the level of confidence, is a time dependent entity. That means the trust may vary as time goes on based on the nodes' behaviour in transactions performed among them. The trust value can be evaluated through the history of transactions recorded on the node and by the referencesrecorded by the other neighbouring nodes. Here, the history denoting the behaviour of the node has different aspects, i.e. trust metrics, also referred as the Quality of Service Characteristics [10] [6] . The calculated level of confidence extracted from trust metrics is called direct trust (DT). The indirect trust referred as (IT) can be extracted from the recommendations, called indirect information referredby itsneighbouring nodes. As the overall Trust (T) on any node of WSNs can be functioned by manipulating these direct and indirect trusts. As displayed in figure2, node A is evaluating trust on node B. It evaluates the direct trust through its direct experiences and indirect trust (IT) through the information shared by itsneighbouring nodes.

Hence every node in the network constantly checks on the behaviour of their neighbouring nodes and sustains a record on them for every event occursover the network. Particularly this record contains all the data about neighbouring node QoS and its characteristics. This trust metrics information will be usefulto calculate the direct trusts (DT) on them. Also, when it is essentially requested by neighbouring nodes, the trust metrics of one node, can be transferred to other nodes, and there it helps in evaluating the indirect trust. In our trust evaluation method, the trust metrics of any node in the network on its any neighbouring node is a function of DT and IT.

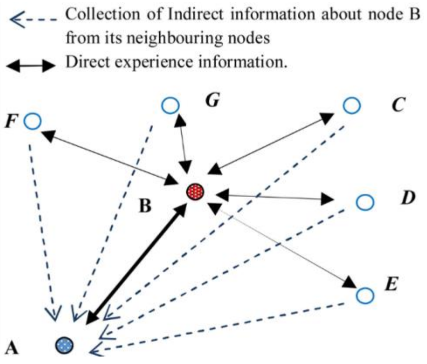
Collection of Indirect information about node B from its neighbouring nodes
Direct experience information.
F
G
C
B
D
E
A

Figure.2: Node an Evaluating trust on Node B

Calculation trust value of sensor nodes resolved constructed on the direct trust (DT), indirect trust (IT) and sensor node. Trust will be revived after a time span and is connected with all trust which is resolved subject to the legitimate data of individual node without seeing some network components, for instance, node flexibility, trust spoil as time goes on, and some malevolent attacks [7].

Trust calculation =$W_1\ T_{ini} + W_2\ T_s + W_3 T_{mob} + W_4\ T_r$

where, Tini = initial trust,

T_s = secure trust model,

T_{mob}= mobility trust model,

T_{rel} = reliability trust,

W_1, W_2, W_3 and W_4denotes the weight related to direct trust, reliability trust in addition indirect trust correspondingly for example

$W_1 + W_2 + W_3 + W_4 = 1$, and each weight differs from 0 to l dependent on bothsubject node and object node are one hops neighbor or multi-hops neighbor.

3.5. Hybrid Trust Evaluation Algorithm

The proposed trust evaluation method is referred as a hybrid trust evaluation method. First, it tries to find the trustworthy neighbouring node from the available trust metric database. If any node's trust value is resulted efficiently asgreater than or equal to trust threshold then that neighbouring node will be particularly selected for packet transmission for that moment. But if not even one node is found trustworthy then it takes another way to search and evaluate the trustworthy node for packet routing. When node needs to start the communication with its neighbouring nodes for collecting indirect information data, it just sends a request command to its neighbouring nodes. This command may take only one byte or two byte in size. But, when it is getting indirect information the size of the message from each neighbouring node may be approximately 20 to 25 bytes by assuming that each node's information takes 2 bytes and it may have 10 neighbours. The communication among nodes for indirect information will take place only when there is risky situation and not all the time as explained in the following algorithm. Hence, this hybrid trust method is not only energy efficient but also helps to reduce the communication overhead.

Algorithm 3 Hybrid Algorithm for node level trust calculation

Initial condition: Node wants to communicate with another node in the network.

Input: Node from source to destination with trust.

Output: Trust value calculation and communication.

```
Begin:
    Initial trust calculation of the node: $T_{initial}=((S+U)/(T_i+S))$ or $P_r$;
    If ($T_{initial}$is sufficient for data communication)
    Allow data communication using the node.
    Else calculate the trust worthiness by using the security model for the particular node. endif.
    $T_s=A+E+R$;
    If ($T_s$ is sufficient for data communication)
    ThenAllow data communication through the node.
    Else calculate the trust value for the mobility model for the node. endif.
    If node is static
    Then assume the trust value of the node in the mobility model is zero.
    Else calculate the trust worthiness value of the node is in mobility.
    $T_m=M_e+E_m$; endif.
    If (Tm is sufficient for data communication)
    ThenAllow data communication through the node.
    Else calculate the trust worthiness for the node in the reliability model.
    $T_r=D+Ed$; endif.
    If ($T_r$is sufficient for data communication)
    ThenAllow data communication through the node;
    Else calculate the Hybrid trust value for the particular node.
    Hybrid trust=$T_{initial}+T_s+T_m+T_r$; endif.
    If Hybrid trust is adequate for communication
    ThenAllow data communication through the node.
    Else
    Deny the data communication through the node. endif.
End.
```

4. PERFORMANCE EVALUATION

The performance evaluated on the proposed Hybrid Trust evaluation technique has been evaluated through computer simulations. Using MATLAB, a new simulation package for routing has been developed based on distance of neighbouring nodes towards the Sink node. To analyze the behavior and performance of all the nodes that present in the network, the following three metrics from the list of Table 1.were used.

To evaluate packet delivery ratio, packet modification ratio and packet misroute ratio simulation is done with 50 normal nodes. All packets are 512 bytes. After that evaluate same metrics with 50 nodes add with 5 malicious nodes then compare the performance of every node.

4.1. PDER (Packet Delivery Ratio):

PDR of the no. of packages attained from the source node to the destination node. The number of delivered data packet to the total number of packets to be delivered by the node is called packet delivery ratio.

***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

$$\text{PDER} = \frac{\text{Number of Packet's Transmitted by Node}}{\text{Total Number of Incoming Packets}}$$

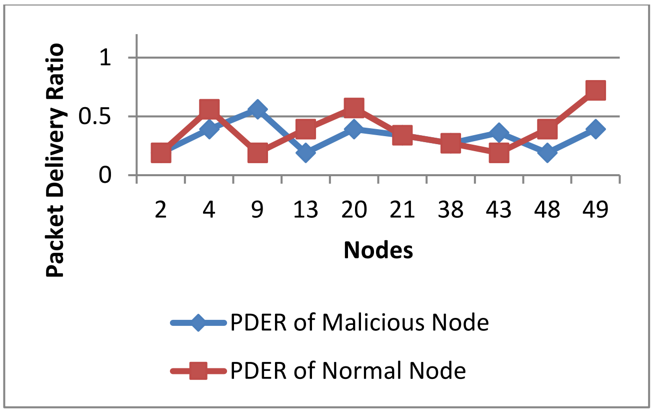

Figure:3. Packet Delivery Ratios

Figure: 3shows about the packet delivery ratio of each node though this graph compares the performance of normal node without insert malicious node and with insert malicious nodes. The preliminary malicious node gave better performance.

4.2. PMOR (Packet Modification Rate):

Network can modify the address of node by using the routing protocol. The larger number of packet delivery ratio shows the performance level of the node. Change the content of the packet during transmission is called packet modification. Most of the time this is done accidently and some node do this intentionally.

$$\text{PMOR} = \frac{\text{Number of Packet's Modified by Node}}{\text{Total Number of Incoming Packets}}$$

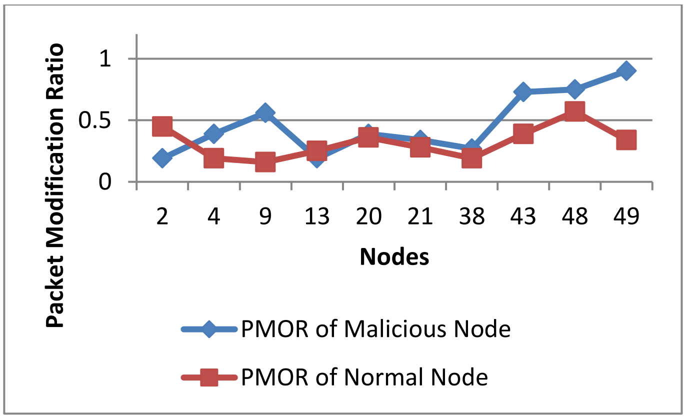

Figure: 4: Packet Modification Ratios

Figure4 illustrates the packet modification ratio of each node. After sometimes malicious node started doing malicious activities as modification of packets.

4.3. PMISR (Packet Misroute Rate):

Node sends packet to the wrong destination such packets are called misrouted data packet.

$$\text{PMOR} = \frac{\text{Number of Packet's Misrouted by Node}}{\text{Total Number of Incoming Packets}}$$

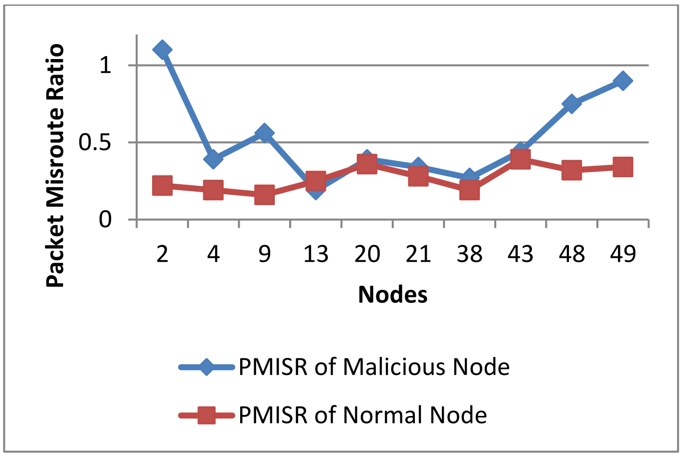

Figure:5. Packet Misroute Ratios

Figure 5illustrates the packet misroute ratio of each node. After sometimes malicious node started doing malicious activities as misroute of packets.

4.4. Comparison of Evaluation Models:

We have evaluated the performance of our trust evaluation mechanism with multi-hop routing protocol. The other settings and assumptions are given in Table 1.

Table:1. Simulation Parameters

Simulation Parameters	Values
WSN deployment	Random in a square area.
WSN area	200 × 200 square meter
No. of nodes	50
Trust metrics	3 Categories
Neighboring nodes	max. 10% of total nodes
Initial Trust	0.5(initially all nodes are trusted)
Malicious nodes	0% to 30%
Trust threshold (Tth)	0.35 to 0.5
Direct Trust weight	varies from 0.75 to 0.5
Indirect Trust weight	varies from 0.5 to 0.75
Packet Generation	Randomly with Poisson probability of 0.3

Article Received: *26 August 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *02 November 2023*

Table: 2. Compares the result with proposed model

No of Nodes	**Malicious Node**		
	Direct Trust	**Indirect Trust**	**Hybrid Trust**
10	0	0	3
20	0	5	8
30	2	5	9
40	3	7	12
50	5	9	15

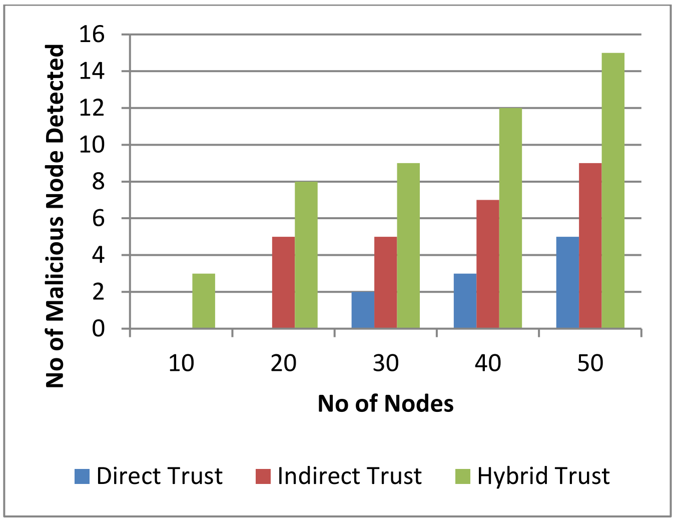

Figure: 6. Comparison of Trust Models

From figure 6 shows that proposed method gives better result than previous method. Table 2 shows the no of malicious nodes found using proposed method. When nodes cross threshold limit Hybrid Trust Evaluation Method declared the malicious nodes. Trusted relations for trust threshold ≥ 0.35 are set and trust determined.

5. CONCLUSION

This paper presents the overview on the trust worthiness of a node in the network along with the parameters and metrics. It also explains the proposed Hybrid Trust model algorithm for calculating the trust value of all the nodes that present in the network. Hence the proposed model is simple and it can be easy to implement. We are in process of evaluating the proposed Hybrid Trust Model algorithm with the standard Trust model algorithms through implying the NextworkX simulator. In the further work, we will attain new techniques and attributes like scalability and fault tolerance capacity to the model which will ensure high trust worthiness of the network.

REFERENCES:

[1] X. Mao and J. McNair, "Effect of on/off misbehavior on overhearing-based cooperation scheme for MANET", In: Proc. of International Conf. on Military Communication, pp. 1086- 109, 2010.

[2] T. Zahariadis, P. Trakadas, H.C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks", International Journal of Wireless Personal Communications, Vol. 69, No. 2, pp. 805-826, 2013.

[3] A.Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks," presented at ACM International Conference Proceeding Series, Dunedin, New Zealand, 2004.

[4] Chen, S. Garg and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks", In: Proc. of International Workshop on ACM Modelling, Analysis, and Simulation of Wireless and Mobile Systems, pp. 61-68, 2002.

[5] Amol R. Dhakne and Prashant N. Chatur, “TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network”, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.12, pp. 1-10, 2016.

[6] A. R. Dhakne and P. N. Chatur, “Distributed Trust based Intrusion Detection approach in wireless sensor network.”, 2015 Communication, Control and Intelligent Systems (CCIS), IEEE, Mathura, pp. 96-101, 2015.

[7] Arnab Ghosh and Sovan Bhattacharya, “Calculating Trust and Aggregation of a node using Poisson Distribution in WSN”, International Journal of Computer Applications (0975 – 8887) Vol. 68, No.24, pp. 43-46 2013.

[8] Li Mo, “Research on Trust Calculation Mechanism of Wireless Sensor Network of Internet of Things”, Advances in Engineering Research, volume 166, No. 20, pp. 23- 28, 2018.

[9] Ping Qi, Fucheng Wang, Shu Hong, "A Novel Trust Model Based on Node Recovery Technique for WSN", Security and Communication Networks, vol. 2019, No. 10, pp. 1-12, 2019.

[10] A. Ahmed and A. R. Bhangwar, “WPTE: Weight-Based Probabilistic Trust Evaluation Scheme for WSN,” in Proceedings of the IEEE International Conference on Future Internet of "ings& Cloud: Workshops, IEEE Computer Society, Prague,Czech, Vol. 108, No. 20, pp. 15-21, 2017