Behaviour based Trust Management using geometric mean approach for Wireless Sensor Networks

Ch.Satya Keerthi.N.V.L^{*1}, A.Manogna$^{\#2}$, Ch.Yasaswini$^{\#2}$, A.Aparna$^{\#4}$, S.Ravi Teja$^{\#5}$

** Lecturer, Department of Information science and Technology*

# Department of Information science and Technology,
KL University, Guntur – 522 502, Andhra Pradesh, India

***Abstract*— The resource constraints of Wireless Sensor Network (WSN) make it easy to attack and hard to protect. Although carefully designed cryptography and authentication help to make WSN securer, they are not good at dealing with compromised node and ageing node, whose misbehavior may impair the function of WSN. Hence, they are not sufficient for secure routing of message from source to destination in WSNs. Alternatively Trust management schemes provide a powerful tool for the detection of unexpected node behaviours. A solution is obtained by first figuring out the malicious nodes in the network and then separating them from the benevolent nodes present on the basis of trust levels assigned. In this paper, we propose a new Trust Management System by considering the behaviours of sensor nodes, direct and indirect trusts based on Geometric Mean (GM) of the QoS characteristics (trust metrics) among the nodes, which allows for trusted nodes only to participate in routing messages.**

***Keywords*—Wireless Sensor Network (WSN), Geometric Mean (GM), Trust Metrics, Quality of Services (QoS).**

I. Introduction

Wireless Sensor Networks (WSNs) are ad-hoc networks, consisting of spatially distributed devices (motes) using sensor nodes to cooperatively monitor physical or environmental conditions at different locations. A sensor node is a tiny and simple device with limited computation and resources. Sensor nodes are randomly and densely deployed in sensed environment. WSN is designed to detect events or phenomena, collect and send back sensed data to the user. The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real-time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to *in situ* monitoring of the health of structures or equipment.

The characteristics of wireless infrastructure and characteristics of WSNs cause the potential risks of attacks on the network. Depending upon the application, WSN deployment environment may be hazardous, unattended and/or hostile and sometimes dangerous. The cryptographic, authentication and other security mechanisms in WSNs cannot detect the node physical capture, the malicious or selfish nodes. Hence, they are not sufficient for secure routing of message from source to destination in WSNs ([1]-[3]). Also, the traditional cryptographic, authentication and other security mechanisms in WSNs consumes significant node resources and requires sophisticated software, hardware, large memory, high processing speed and communication bandwidth. Another intricacy of the WSNs is that they operate in infrastructure less manner which further complicates the applicability of legacy security solutions [2].

Trust is defined as the subjective expectation a peer has about another's future behavior based on the history of encounters. Trust [1] is "the degree of reliability" of other node in performing actions and can be formed by maintaining a record of the transactions with other nodes directly as well as indirectly. From this record a trust value will be established. Trust can be defined as "The subjective probability by which node A depends on node B to fulfil its promises in performing an action and at the same time being reliable in reporting its sensed data". Trust is dependent on time; it can increase or decrease with time based on the available evidence through direct interactions with the node or recommendations from other trusted nodes. Trust-modelling is mathematical representation of node's opinion of another node in a network. We need mathematical tools to represent trust and reputation, update these continuously [1].

Trust management system for wireless sensor networks (WSNs) is a mechanism that can be used to support the decision-making processes of the network [4]. It aids the members of WSN to deal with uncertainty about the future actions of other participants (trustees). As WSNs are highly application oriented, these various applications bring various security needs. Survival of a WSN is dependent upon the cooperative and trusting nature of its nodes. Hence, the trust establishment between nodes is must.

Many researches on trust related in WSN are processed, but it is required to design and develop a light weight trust management system that takes the less resources of the node in calculation and management of trust between/among the nodes. The trust management of the WSN should be as simple as possible, i.e. without constraints on software, hardware, memory usage, computing, processing speed and communication bandwidth, and detect the different attacks easily, and mange and update trust relations accordingly.

A new approach of trust calculation considering both direct trust and indirect trust based on geometric mean (GM) of the QoS characteristics such as packet forward, data rate, power consumption, reliability, etc. among the nodes is presented. We have presented graphically, the trusted relations formed by all benevolent nodes of the WSN. Routing of data can take place through these benevolent or normal nodes present in the network thus reducing packet latency and dropping of packets. Simulated results for different number of trust metrics for different trust threshold of this new trust management model are presented.

The paper is organized as follows. In Section II, we present the related work on WSN trust models. In section III, we describe the design of Geometric Mean based Trust Management based on direct trust and indirect trust while in section IV we describe Behaviour based trust framework. We show the efficacy of the model through simulation results in section V. Lastly, we conclude the paper in section VI.

II. RELATED WORK –TRUST MODELS FOR SENSOR NETWORKS.

Wireless Sensor Networks are categorized into three. They are centralized, hierarchical and distributed. Tae Kyung Kim, and Hee Suk Seo in [6] suggested a trust model using fuzzy logic for centralized WSN. Reputation defined as a perception of a party creates through past actions about its intentions and norms. The different components in the suggested trust modelling are minimum trust, maximum trust and un-trust. They assumed that base station has the reputation value of each node. In most of the applications WSNs are either distributed or hierarchical, and hence the proposed model may not be suite for practical applications. Even if the WSN is centralized, they have not mentioned the way how base station evaluates the trust of a node.

Trust management can be distributed or central. In totally distributed mode, every node maintains its trust table of other nodes. Evidence of trust comes from direct observations of those nodes. In the central mode, every node reports its observations to a central node which acts as a trust authority in the WSN. While the former needs a long time to get the real estimation of a node's trustworthiness, the latter invokes a quantity of communication and subsequent high energy cost. Hybrid architecture may be much preferable than the former two. Because most interaction in WSN happens within neighbourhood, a reasonable mode is that every node maintains trust itself of neighbours while exchanging opinions with each other intermittently within the neighbourhood.

Mohammad Momani [1] proposed different methods for modelling and managing trust to enable WSN to be secure and reducing the computing and communication overheads. He proposed an algorithm for trust calculation and risk assessment based on trust factors and dynamic aspects of trust. He modelled the direct trust computation with direct experiences, and indirect trust with recommendations given by the neighbours. The direct trust A of node N_1 on node N_2 is defined as the sum of trust values node N_1 is having on node N_2 for different trust metrics such as packet forward, data rate, error rate, power consumption, reliability, competence, etc. The indirect trust B of node N_1 on node N_2 is defined as the average of recommendations given by the neighbours of node N_2 (nodes N_3, N_4, N_5, N_6, N_7 as shown in Fig. 1. He modelled total trust using traditional weighting approach for direct trust and indirect trust as shown in following equations. A is direct trust (*experience*), B is indirect trust (*recommendations*), C is total trust. The direct trust A of N_1 on N_2 is given by the following equation.

$$A = \sum_{i=1}^{m} W_i * T_{N_{1_i}}(N_2).$$

Sum of trust values of N_1 on N_2 for ***m*** different trust metrics with different weights (W_i). The indirect trust B of node N_1on node N_2 is given by the following equation.

$$B = \frac{1}{k} * \sum_{i=1}^{k} T_i(N_2)$$

The indirect trust B of node N_1 on node N_2 is the average of direct trusts of ***k*** neighbours on N2.

$$total\ trust\ C = F(A, B)$$
$$C = A * W_A + B * W_B$$

The weights W_A and W_B can be assigned using different approaches. Some nodes may be given more weight for direct trust; others may be given more weight in indirect trust. i.e $W_A > W_B$ or $W_A < W_B$. Weights to the direct trusts of some metrics may be given more importance, and others are less importance. Similarly, for indirect trusts nearby nodes may be given more importance and others less. He introduced beta distribution system [7], [8] for weighting direct and indirect trusts in the case of communication trust. The trust management and modelling methods proposed by [1], are not light weight in consuming resources of node in the WSN.

In trust management scheme proposed in [9] honest nodes are favoured by giving them the credit for each successful packet forwarding, while penalizing suspicious nodes that exaggerate their contribution to routing.

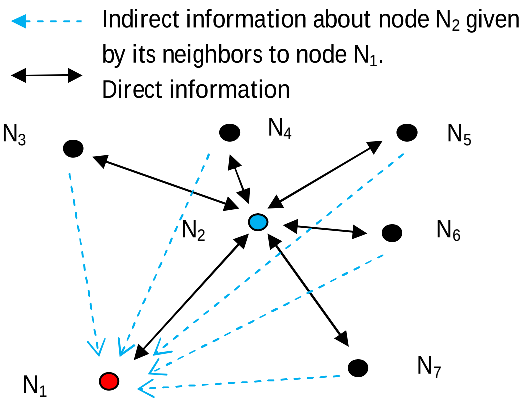
Indirect information about node N_2 given by its neighbors to node N_1.
Direct information
N_3
N_4
N_5
N_2
N_6
N_1
N_7

Figure. 1. Node’s trust relationship.

Trust establishment system proposed in [10] has two ways to establish trust in computer networks. First, when the subject (first party) can be directly observing the agent (second party). Second, when the subject receives recommendations from other entities about the agent, indirect trust can be established.

A novel flexible trust management system proposed in [2] defined the trust as the ratio of successful transactions to total transaction made by the node. The proposed model is a decentralized trust scheme, i.e. the trust management functionality is distributed over the network nodes. In this model, each node is responsible for computing its own trust value per relation in the network, collecting direct and indirect information. The both direct and indirect trust values are used to evaluate each node’s trustworthiness. The proposed model has inherent reputation scheme of getting trustworthiness of any node, when direct evidences does not suffice, i.e. the number of direct evidences remain under threshold.

III. THE GEOMETRIC MEAN BASED TRUST MANAGEMENT SYSTEM

In this section, we propose a new trust model suitable for many practical applications of the Wireless Sensor Networks (WSNs). The concept here is each node in the network, will maintain a record for every its neighbour node. This record contains the information about different trust metrics, i.e. QoS characteristics for all its neighbours regarding the number of events occurred in the network. This trust metrics data will be helpful for calculating the direct trust of its every neighbour node. Also, as and when required, trust metric data of one node, can be transferred to other nodes, and act as indirect information for calculating indirect trust of nodes.

The proposed trust model is a decentralized trust scheme, i.e. the trust management functionality is distributed over the network nodes. Each node is responsible for computing its own trust value per relation in the network, collecting events from direct relations, and collecting trust values from other nodes in the network (in other words, indirect information). This means that both direct and indirect trust values are used to evaluate each node’s trustworthiness. The indirect (second-hand) information may be particularly useful when no or limited direct interaction has been experienced.

One of the most important aspects of trust management schemes is the process of data collection for trust calculation. The direct trust value of a neighbouring node can be determined by the different trust metrics of that particular node in different events occurred in the network. The trust metrics [11], i.e. the QoS characteristics that can be taken into account are shown in the Table 1.

TABLE 1. Trust Metrics

Data packets forwarded	m_1
Data packet/message precision	m_2
Control packet/ message forwarded	m_3
Control packet/ message precision	m_4
Availability based on beacon/hello messages	m_5
Routing protocol execution (routing actions)	m_6
Consistency of reported (sensed) values/data	m_7
Sensing communication	m_8
Reputation	m_9
Packet address modified	m_{10}

The listed trust metrics data for different events are essential and can provide a useful feedback to the system, towards the proper decision making by the trust management system. Here, depending on the application, we can insist the minimum level (threshold) to all the trust metrics, or we can have different thresholds to different groups of trust metrics. Once one/more trust metric threshold/s are fixed, our trust management system see that no node is trusted unless the node is having minimum threshold level in a given trust metric strictly. This is the main advantage of our proposed trust management model comparing with other models.

The direct trust of any node, say N_1 on the node $N_2$is a function of the all trust metrics values as shown in Fig. 2. Here, $m_1, m_2, \dots, m_n$ are the trust metric values of N_1on the node N_2. These trust metrics tells node N_1, how node N_2 behaved in different QoS characteristics.

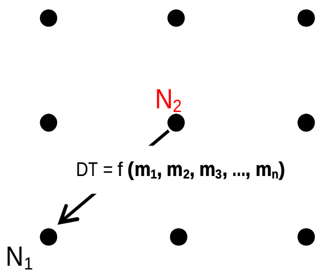

Figure 2. Direct Trust function

In our trust management system, the direct trust is Geometric Mean of all different trust metrics for different events occurred in the network on that particular node. These trust metrics are different from the trust metrics of other surrounding nodes. Like this, every node will be having a separate record of data of every surrounding node in different trust metrics for different events occurred in the network. From these records, Direct Trust (DT) is calculated based on Geometric Mean of the QoS characteristics as given in the below equations.

$$DT = geometric\ mean\ of\ trust\ metrics$$

$$DT = \left[\prod (m_1, m_2, \dots, m_n)\right]^{1/n}$$

$$DT_I(J) = \left[\prod_K (m_{I,J,K})\right]^{\frac{1}{K}}$$

Here, $m_1, m_2, \dots, m_{10}$ are the trust metrics of node. The $DT_I(J)$ in the above equation is the Direct Trust value of node I on node J, calculated for K different type of trust metrics. Every node maintains the database of all its neighbours, and the contents of database are shown in Table 2.

The Indirect Trust on node N_2 with respect to N_1 can be calculated from the direct trusts (DTs on N_2 with respect to its neighbours) sent by the neighbouring nodes of N_2. The neighbours of any node N are shown in Fig. 3. In our proposed model we have defined neighbour nodes to any node N are N_1, N_2,N_3, N_4, N_5,N_6, N_7, N_8 in clockwise as shown in Fig. 3. For example the neighbours of node N_2 are N_3, N_4, N_5, N_6, N_7 as per the Fig. 1. The Indirect Trust (IT) of node N_1 on node N_2 is defined as the Geometric Mean of the DTs of neighbour nodes (N_3, N_4, N_5, N_6, N_7 as per Fig. 1.) on N_2.

TABLE 2. Node's Database of its neighbour nodes

Nbr	k_1	k_2	k_3	...	k_n	DT	IT	TT	TE
N_1	a_1	a_2	a_3	...	a_n	DT_1	IT_1	TT_1	TE_1
N_2	b_1	b_2	b_3	...	b_n	DT_2	IT_2	TT_2	TE_2
N_3	c_1	c_2	c_3	...	c_n	DT_3	IT_3	TT_3	TE_3
N_4	d_1	d_2	d_3	...	d_n	DT_4	IT_4	TT_4	TE_4
N_5	e_1	e_2	e_3	...	e_n	DT_5	IT_5	TT_5	TE_5
N_6	f_1	f_2	f_3	...	f_n	DT_6	IT_6	TT_6	TE_6
N_7	g_1	g_2	g_3	...	g_n	DT_7	IT_7	TT_7	TE_7
N_8	h_1	h_2	h_3	...	h_n	DT_8	IT_8	TT_8	TE_8
N_i neighbours i=1 to 8, k_1 ,k_2 , ...,k_n are type of trust metrics. DT direct trust.									
IT indirect trust, TT total trust and TE trust evaluation between two nodes.									
a_i , b_i , .., h_i for i=1 to n are trust metric values for k_i category for 8 neighbours									

$$IT = geometric\ mean\ of\ trust\ \text{information given by neighbour nodes.}$$

$$IT = \left[\prod (DT_1, DT_2, \dots, DT_8)\right]^{1/8}$$

$$IT_I(J) = \left[\prod\nolimits_L (DT_L(J))\right]^{\frac{1}{L}}$$

Here, $DT_1, DT_2, \dots, DT_8$ are the DTs given by the neighbour nodes. The $IT_I(J)$ is the Indirect Trust value of node I on node J, calculated for indirectly given information by L neighbours of J. This is shown in Fig. 4 clearly. The IT of node S on node X is geometric mean of DTs of neighbours on node X. The total trust of any node with respect to any other node is again a function of Direct Trust (DT) and Indirect Trust (IT). Our proposed model also uses the traditional weighting approach for combining direct trust (DT) and indirect trust (IT) and form the total trust (TT) per relation in the network. As shown in following equation, DT is direct trust (*experience*), IT is indirect trust (*recommendations*), TT is total trust.

$$total\ trust\ TT = F(DT, IT)$$
$$TT = DT * W_a + IT * W_b$$

The weights W_a is weightage given to DT and W_b to the IT where $W_a + W_b = 1$. Weights can be assigned using different approaches. Sometimes DT may be given more weight, and IT may be given less weight i.e. $W_a > W_b$.

$$TT_I(J) = DT_I(J) * W_a + IT_I(J) * W_b$$

The average Trust ($T_{I,J}$) between any two one hop nodes is given by the average of Total Trusts found each other as shown in Fig 5.

$$T_{I,J} or T_{J,I} = \frac{1}{2} * (TT_I(J) + TT_J(I))$$

This method provides many advantages as compared to the existing ones. It also allows us to find out the levels of trustworthiness of all neighbour nodes, even when the TE_{TH} value cannot be decided or evaluated, and hence the separation of benevolent and malicious nodes is possible. This method allows us to give more weight to certain trust metrics, depending on the requirement in the application. Calculation of direct trust of a single node with respect to another node based on number of parameters is accomplished by taking the average of the individual single parametric trusts in Momani's model [1]. In Momani's model, if the trust metric value for successful transmission of packets is 0 and the rest trust metrics have a high values, the overall trust value may be the above the trust threshold and the node will be trustworthy.

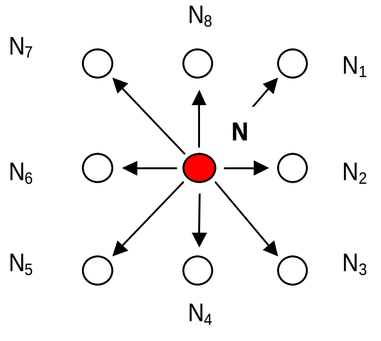

Figure 3. Node N and its neighbours N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8.

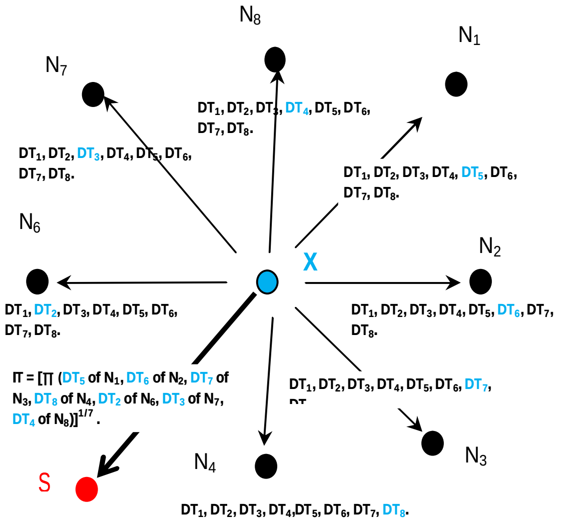
N_8
N_1
N_7
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$
N_6
X
N_2
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$
$IT = [\prod (DT_5$ of N_1, DT_6 of N_2, DT_7 of N_3, DT_8 of N_4, DT_2 of N_6, DT_3 of N_7, DT_4 of $N_8)]^{1/7}$.
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7,$
S
N_4
N_3
$DT_1, DT_2, DT_3, DT_4, DT_5, DT_6, DT_7, DT_8.$

Figure 4. Indirect Trust of node S on node X based geometric mean of direct trusts given by its neighbours.

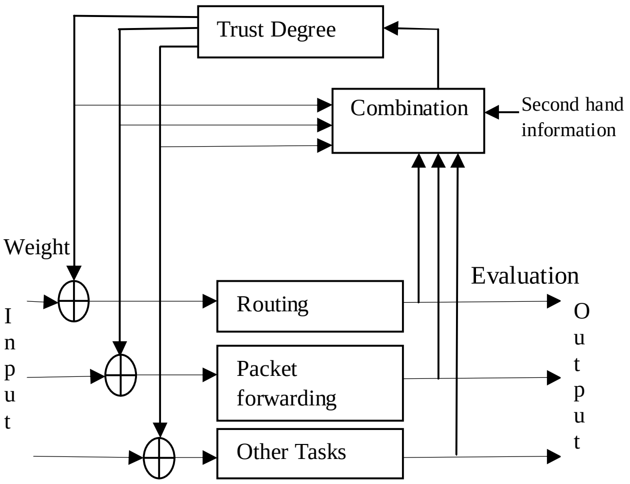

Figure. 5. The process of behavior-based trust management

That means it cannot detect the malicious/faulty nodes. But, our proposed trust model, this situation will be solved differently. The node will be treated as faulty or malicious because one of the trust metrics is failed to form trusty relation. In our trust model, trustworthy relation will be formed between two nodes only when the level of trust metric value for a given trust metrics is greater or equal to trust metric threshold.

IV. Behaviour based trust framework

The process of the behaviour-based trust is depicted in figure 5.After every task, the behaviour of the node is evaluated. The evaluation result is combined with old trust degree to form a new one. The new degree is considered in the next task allocation in term of weight. For example, the data from node with high degree should play a more important role in data fusion, and the trustworthy nodes should be chosen to transmit data with higher probabilities than untrustworthy ones. To calculate the trust degree here the geometric mean based Trust management system is used.

Nodes with their previous activities and behaviour patterns are distinguished as reliable nodes and unreliable nodes. Reliable nodes are nodes with high confidence level and unreliable nodes are nodes with low confidence level, i.e., to say that nodes crossed the threshold confidence level are reliable, which have confidence level value less than that are unreliable. As this is a distributed system [5], each node has the confidence level values of its immediate neighbours. So, it may turn out be an unreliable node for one node might be reliable for another node. Every node maintains confidence level matrix of its immediate neighbours, which are later required for trust management.

V. PERFORMANCE RESULTS

The performance of the proposed trust management system has been evaluated through computer simulations. A new software simulation package has been developed using the MATLAB platform to model our approach. A Wireless Sensor Network with 30 nodes is placed in the environment based on the locations in the coordinate system. The figure 6 shows the random network deployed. All the nodes in the network are self organising i.e, ad-hoc. They are randomly placed based on the coordinate locations. Once the nodes verify their locations they check for their neighbours based on their communication range. In our simulated network the range of communication for each node is 200. The neighbours of the nodes are represented using the connecting lines between them.

The trust values computed through the geometric mean approach are used for obtaining the best path in routing the data to the internet through the gateway. All the neighbours of the nodes and their trusts are stored in the form of a three dimensional matrix in MATLAB. For instance the node 1 in the simulated network has node 2 and 10 as its neighbours. The corresponding data table at node 2 will store the trust of node 1 in the perspective of node 2 computed through the behaviour based trust framework. To obtain the effective trust of node 1 we need to find the average of the trusts at all its neighbours.

From the graphical representations of trust values among the WSN nodes as shown in Fig. 7, we can see how the trusts of nodes vary with the tasks and their performance. The node 31 in the graph is the gateway which has the highest trust value so that all the nodes in its neighbourhood can communicate with it to transfer the data to the base station.

The results shown are for randomly taken trust metrics only, not for practical live metric values.

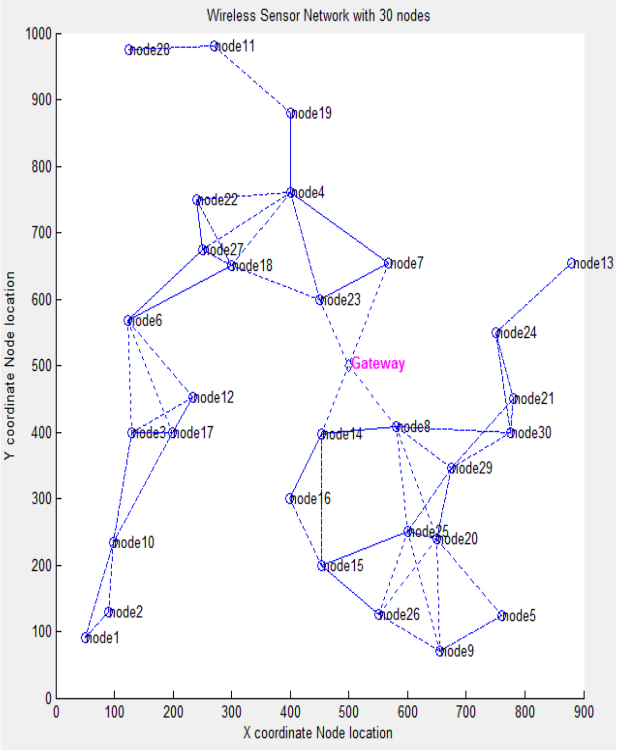

Figure 6. Wireless Sensor network with ad-hoc placement of nodes

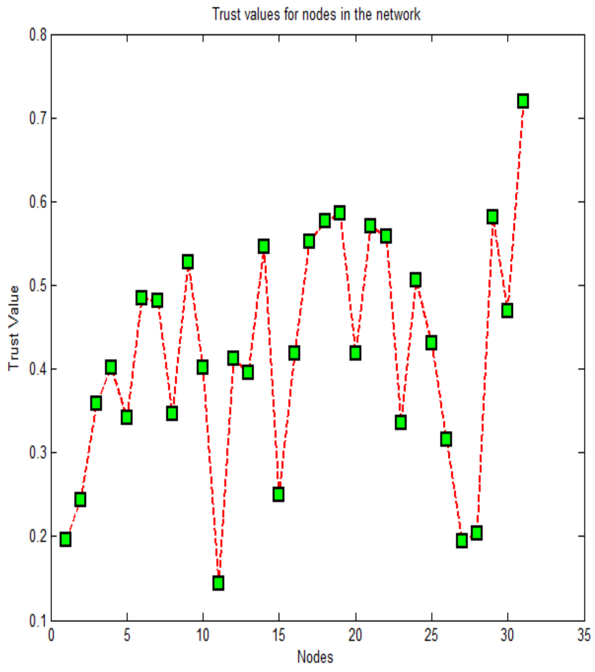

Figure 7. Trust values for nodes in the simulated network

VI. CONCLUSIONS

The trust management system presented provides the trust relations among the nodes depending on the QoS characteristics in the network. In this proposed paper, we have concentrated to form the trust evaluation between two nodes based on weightage of different trust metrics i.e. QoS characteristics, weightage of direct trust, and for overall level of trust between nodes (level of trust evaluation). We combined the geometric mean approach with the behaviour based framework for improving the reliability of the simulated environment. We deployed a WSN and obtained the trust values of the nodes in the dynamic environment. Though our proposed model is computationally simple, our future work includes finding communication overhead and modelling other malicious behaviour patterns to make the distributed system more reliable.Also, we plan to find the best trusted route among the many trusted routes from source to destination by applying our proposed model.

References:

[1] M. Momani, “Bayesian Methods for Modeling and Management of Trust in Wireless Sensor Networks,” Ph.D. Thesis, University of Technology, Sydney, July, 2008.

[2] P. Trakadas, S. Maniatis, T. Zahariadis, H.C. Leigou, S. Voliotis, “A novel flexible trust management system for heterogeneous sensor networks”, an International Symposium on Autonomous Decentralized Systems, 2009, proceedings ISADS 2009, page(s):369-374.

[3] Mayank Saraogi; Security in Wireless Sensor Networks; Department of Computer Science, University of Tennessee, Knoxville.

[4] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago, “Trust management systems for wireless sensor networks: Best practices”, *Computer Communications*, Elsevier, 33(2010) pp. 1086 – 1093.

[5] Arijit Ukil “Secure Trust Management in Distributed Computing Systems”, 2011 Sixth IEEE International Symposium on Electronic Design, Test and Application,116-121. doi:10.4236/wsn.2011.34015.

[6] Tae Kyung, and Hee Suk Seo, “A Trust Model using Fuzzy Logic in Wireless Sensor Network”, World Academy of Science, Engineering and Technology 42 2008.

[7] Mohammad Momani, Khalid Aboura, Subhash Challa, “RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks”, IEEE, ISSNIP 2007.

[8] Mohammad Momani, “Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks”, JOURNAL OF NETWORKS, VOL 5, NO 7, JUL 2010. pp 815-822.

[9] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, “Location Verification and Trust Management for Resilient Geographic Routing,” J. Parallel and Distributed Computing, vol. 67, no. 2, pp. 215-228, 2007.

[10] Yan Sun, Zhu Han, and K. J. Ray Liu, “Defense of Trust Management Vulnerabilities in Distributed Networks”, *IEEE Communications Magazine, Feature Topic on Security in Mobile Ad Hoc and Sensor Networks*, vol. 46, no. 2, pp.112-119, February 2008.

[11] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar “Geometric Mean based Trust Management System for WSNs (GMTMS)”, *2011 World Congress on Information and Communication Technologies.*