Drill System based Hierarchical Trust Calculation to detect Selfish nodes in Wireless Sensor Network

Mr Christhu Raj M.R [#1], Mr Edwin Prem Kumar G [*2], Mr Kartheek Kusampudi [#3]
[#] PG Scholar Dept. of Information Technology, Karunya University
Karunya Nagar, Coimbatore, India
[1] mrchristhuraj@gmail.com
[3] krthk33@gmail.com
[*] Assistant Professor, Dept. of Information Technology, Karunya University
Karunya Nagar, Coimbatore, India
[2] edwin@karunya.edu

***Abstract*— Wireless sensor networks applications are numerous in today's trend. Sensing data, aggregating and forwarding data are prime functions in a sensor network. Sensor nodes have serious constrain like energy, memory, battery, Computational power. One of the main issues in sensor network is that nodes get compromised or selfish which results in performing various attacks and malfunctioning of network. Trust is one of the main security mechanisms to provide security. To calculate trust of a node and identify nodes as malicious takes quite amount of time and parallel sensed data may be dropped or altered. To overcome this issue, we propose a drill based trust calculation-using concept called DTS Commands (Drill Test Sending) integrating with double cluster head. Our System gives efficient security mechanism using trust and simulation results system reduces time taken to detect nodes as selfish nodes and consumes less energy.**

***KEYWORDS*— CLUSTER HEAD, INTIMACY, HONESTY, DRILL TEST SYSTEM COMMANDS, VICE CLUSTER HEAD**

I. INTRODUCTION

A sensor network is an infrastructure comprised of nodes capable of sensing, computing and communication elements. The various basic components in a wireless sensor network are [1] an assembly of distributed or localized sensors, an interconnecting network, a central point of information clustering and a set of computing resources. The main components of WSN are sensor nodes and base station. Sensor nodes are very small having hardware equipped with microcontroller; transceivers and battery. Microcontrollers are constrained devices in terms of memory and computational power. Transceivers functions towards a common goal of forwarding or routing; and finally battery, which determines the lifetime of each individual node. Base stations sometimes called "Heart of Sensor Networks". Base stations enable to collect the processed or unprocessed information from the nodes and store it for later use. Sometimes it issues some control orders to modify the behavior of sensor node. The sensor nodes are designed to perform the functions like Monitoring,Alerting,Information on Demand,Actuating.Based on applications sensor networks can be classified into C1WSN (Category 1 Wireless sensor networks)and C2WSN(Category 2 Wireless Sensor Networks). In C1WSN it is mesh-based systems with multi-hop radio connectivity and in C2WSN it is point to point or multipoint-to-point systems with one or single hop radio connectivity [1]. The various applications includes health monitoring, home control, Building Industrial automation, Medical applications, Highway monitoring, Military application, Habitat monitoring, Wildlife and Instrumentation.

A. Research Issues and Resource Constrains-

The various research issues includes [2] Biological applications- Biological Task mapping, Biomedical signal monitoring. In Commercial applications includes – Smart parking, Vehicular Telematics, Security of Intra-car, Event Detection, Structural Health Monitoring. In Environmental application the research issues are as follows, Green house monitoring, Habitat Surveillance. The various resources constrains in sensor networks are energy, memory, computational power and challenges in sensor networks can be classified by the following criteria like cost, Mobility, Security, Routing Data aggregation. The major issue is that the nodes may be compromised, leading to various attacks. Providing Security is the biggest task in sensor network, security solutions should be effective by providing best security and consuming less resources like energy, memory and computational power. Once the nodes gets compromised it can carry out various attacks as follows:[3]

1) Sniffing attack: Overhear Valuable data from by other nodes.[3]
2) Bad Mouthing attack: Propagate negative information about Good nodes.[3]
3) Good Mouthing attack: Propagate positive information about Bad nodes. [3]

4) Black Hole attack: Attract the traffic to be routed as Shortest Route and Drop the packets
5) Sybil Attack: Clone Several Nodes and Replica the information [3]
6) Dos Attack: Prevent any part of WSN from Functioning.
7) Sink Hole Attack: Attract nearby Traffic through Comprised node
8) White washing attack: Using white washing attack the nodes, which have their trust value less than the threshold value, will try to re-enter into the system.
9) Intelligent Behavior attack: According to the intelligent behavior attack, the nodes may provide good or bad services according to the threshold of trust rating.

To provide secure network the need of trust management in encountered. Trust is a security mechanism used to detect the unexpected behavior of nodes in the network. There is various trust techniques used to detect the nodes and eliminate the selfish nodes. In general, trust is a level of belief or assurance. In sensor network and wireless adhoc network sensor reliability is measure of node's competence in assuring the requested service [4],[5],[6],[7],[8] There are many benefits when we establish trust in a network. Trust gives corresponding solution for access control based upon the metrics of SN. This problem cannot be solved by traditional security mechanism [8][9]. Trust provides reliable routing path which does not have any malicious or selfish nodes [10][11]. The contributions towards our system are as follows, Unlike other trust techniques, we consider both Qos metrics and Social metrics [12] to identify nodes as malicious or selfish [13]. We introduce a new concept called DTS Commands to send commands between nodes and calculate trust between nodes. The concept of Double cluster head [14], [15], [16] integrated to increase network lifetime. The rest of the paper is organized as follows. Section I gives over all knowledge of wireless sensor network and its application including various attacks on nodes. Functions of Trust are explained. Section II, We survey the various existing trust techniques and identify there advantages and disadvantages. Section III we propose our system model that explains complete topology, parameters of nodes, trust calculation metrics, DTS Command, bootstrapping process. Section IV We develops a probability model to evaluate trust between nodes and assign trust values. Section V simulation results are shown which consumes less energy for calculating trust and reduce time taken to calculate trust of a node. In section VI, We conclude the paper with future scope and Section VII we acknowledge the references that laid the foundation of our work.

II. RELATED WORK

In this literature work for wireless sensor networks, we identify clustering schemes such as LEACH [17], PEGASIS [18], TEEN [19], HEED [20]. Apart from clustering schemes, sensor nodes can be deployed in groups [21]. There are many trust management schemes for wireless adhoc networks and sensor networks. Only efficient trust management techniques give best security and consume fewer resources like energy, battery and memory. Reputation based framework for sensor Networks (RFSN) [22], Agent Based Trust Reputation Management (ATRM) [23], Parameterized and Localized Trust management scheme (PLUS) [24], Group-Based Trust Management Scheme for Clustered Wireless sensor networks (GTMS) [8] and Hierarchical Trust Management Protocol for WSN[13] research work have proposed trust. There are other works for trust management in literature like [25] proposed a Trust management problem in Distributed Wireless sensor networks where only node's QoS property is considered discuss trust in detail ,[26] proposed a Modeling trust in Wireless sensor Networks from the sensor Reliability Prospective which failed to address the trust evaluation in group based sensor networks.[27] proposed a location verification and trust management scheme and applied for routing .The main drawback is that there is no Hierarchical trust management for managing clustered wsn and trust is not addressed in deep. H.chen et al [28] proposed a Reputation based trust in wsn. Only node's Qos property is considered and trust value is based on past interactions.Gritzalis [29] deals with Hybrid trust management protocol wsn which combines certificate based and behavior based trust evaluations. The work was carried out in flat architecture that is not scalable and only node's QoS property was considered for trust evaluation. To compare our work with above works we considered node's QoS and Social networks property. Capra et al [30], [31] discussed the human trust, which was formed on three sources: recommendations, credentials and direct experiences. Sensor nodes have restricted resources like energy and memory power. Capra work consumes high energy to evaluate trust because of three sources. In our work, we considered only direct experiences and recommendations to calculate trust of a node.

To shortlist, the best trust techniques RFSN, ATRM, PLUS, GTMS, Hierarchical Trust Management work best suited to calculate trust techniques. RFSN[22] proposed by Ganerial et al based on reputation based framework for data integrity. The technique used here is Watchdog mechanism for monitoring and direct observations to detect selfish nodes in the network. Again nodes QoS Property is considered. In this scenario, each SN maintains the reputation value for neighboring nodes .Trust values are calculated on reputation and use Bayesian formulation for representing reputation of node. It considers that interactions with neighbor nodes are enough and reputation reaches a stationery state. This will not suite if node mobility is high and system fail. The next work ATRM [23] works on specific agent based platform and again node's QoS property alone considered

to evaluate trust. GTMS [8] provides best trust scheme by proposing a lightweight protocol, which employs clustering. It consumes less energy, memory and communication overhead which reduces cost of trust evaluation It is more suited for large scale sensor networks. It considers node's QoS and Social metrics parameters but only difference between our works is Scalability. GTMS is not scalable and trust value is based on experiences. Trust formation issues are not addressed in this model. PLUS [24] based on highly abstracted parameters to evaluate its neighbor's which will be stored in each node. Trust is calculated based on direct and indirect observations. In this scheme, HSN (Hashed sequence number) is introduced. All Control packets generated by base station should contain HSN and inclusion of HSN results in increasing packet size and consuming high energy. Since there is consumption of high transmission and receiving power, it results in decreasing energy of node and increases sensor cost. Hierarchical Trust management protocol [13] research work considers both QoS Property and Social networks property are considered. This system suits best for detecting selfish nodes in the network and gives best results compared with other works like GTMS, RFSN, PLUS, T-RGR. Hierarchical Trust management protocol considers both QoS and Social Networks to evaluate trust value of each node. Trust evaluation is based on SN-SN trust evaluation and CH-SN trust evaluation Each Node calculate trust using parameters like energy, intimacy, honesty and unselfishness. It follows two levels of hierarchy, periodic peer –to-peer trust evaluation and SN-CH Trust evaluation. It is efficient algorithm or protocol but to find trust value and according to trust value assigning a node as malicious or selfish takes 80 hours and if a node becomes selfish at starting then till it reaches 80 hours the sensed data are dropped or altered. The possible way of node becoming, a selfish or compromised are Hardware fault failures, Environmental Factors and by malicious attacks like introducing an intruder. There is no specific clustering scheme mentioned in the work and communication overhead takes place when cluster size increases. The node, if needs stores the trust value of all nodes in the cluster, which is again using memory in the sensor. We tried to overcome above problem from other work by combining QoS and Social Parameters. Intimacy and Honesty [13] are considered as Social networks [13] parameters and energy from QoS metrics. Our proposed work is similar to [13], were we are considering the social and Qos parameters and including our concept namely DTSC Commands with Double Cluster Head.

III SYSTEM MODEL

This Section describes about our system model. Nodes are deployed and it is static once it is deployed. To increase network life (energy) and reduce the workload of Cluster Head we introduce Vice Cluster Head (VCH). This concept is obtained from [14], [15] and [16] to increase the network life time, therefore VCH was introduced. We are integrating our DTS (Drill Test Sending) Command, along with the concept of VCH(Double Cluster Head) to provide efficient security trust algorithm, thus increasing network life time and reducing time taken to detect node as malicious or selfish nodes. Trust mechanism research paper starts the trust value of node from 0.5 initially and increases or decreases according to algorithm. While deploying a node, initial trust value may be 0.5 and if there is any hardware fault then node stops sensing and forwarding, which is ultimate and prime function of sensor nodes. Even best algorithm cannot provide trust quickly and will take around 80 hours [13] to detect it as selfish. While doing it increases the network lifetime but will result in losing sensed data. When a sensor node is not performing its intended function, it will result in malfunctioning of entire network. This should be identified soon and precaution measures should be taken. In order to increase the network lifetime and detect a node selfish quickly, we propose the Drill based system with help of VCH Concept. Drill system is a commonly adopted, to make citizens aware of the possible dangers and how to react in such situations, if it really happens. Various countries like Japan and China where Tsunami is common and countries like India, Kuwait, Brazil and Indonesia were Earthquakes are common have adopted this system. Government will alert the possibility of an impending natural calamity, thus preparing people and rescue teams. Therefore, if it really occurs citizens and rescue teams will have knowledge of how to escape and proceed, since they had previous experience with Drill System. This will help in saving lives. Moreover, time taken to react will be less since they had previous experience. This same concept is applied in our research work. Instead of assigning a random trust value initially, then calculating trust according to trust algorithm and finally detecting that a node is selfish; this will take time and also result in loss and alteration of sensed data. We make use of QoS and Social Parameters. The nodes are deployed stationary and each cluster has Vice Cluster Head and Cluster Head. It follows HEED technique for Clustering and the Vice Cluster Head is placed at the center of the cluster. It follows star topology where communication between VCH and SN is one hop, communication between SN and VCH takes multihop. Radio range of VCH is for the entire cluster AND nearby cluster and radio range of CH will be for two to three Clusters. Trust of Sensor node is evaluated by VCH and VCH by Cluster Head and Cluster Head by base station Radio range and Energy: CH > VCH > SN

A. Bootstrapping Process

During the bootstrapping process, the CH and the VCH stores the node ID (SID) and location of each sensor node; to make Drill system easier. Each sensor node in the network is identified by Sensor Node ID (SID) and location is identified by using RSSI [31].Each VCH and CH knows the location of each sensor node ID and

location in the cluster .Similarly each sensor node knows its one-hop neighbor's SID and location. Each Sensor node stores the Sensor ID and location of its one-hop neighbors within its Radio range. If a cluster Head finds that a part of network in the cluster is not covered by any sensor node or if there is no sensor to sense the area it sends join() message to Base station with Cluster Head ID stating that it needs an additional sensor node in the cluster. So while deploying a new sensor node, it should have unique ID and send location and SID to VCH, CH and one-hop Neighbour radio range sensor nodes. Whenever the base station receives the join() message with the cluster head ID, the base station deploys new a node in the cluster. If a node wants to join any cluster without prior information of base station then CH reads the count of each sensor node with VCH, CH ID in the cluster and it sends to nearby cluster Head with a message called decision(). Whenever a CH receives the decision() message, it counts the number of nodes in cluster and sends the count to the Base station along with the Cluster head and the Vice Cluster Head IDs. Base Station then query for Number of sensor nodes in each cluster by sending the same decision() message to other Cluster Heads which didn't send the decision() message. For this purpose the Base station stores the Cluster Head, Vice Cluster Head information like ID, number of nodes in cluster, starting value and ending value of Sensor Node ID's in cluster and finally location of VCH and CH. The base station after receiving the decision() message from all CH in the entire network, it will decide where to deploy the new node and inform to the requesting CH about the deployment with new Sensor ID.

1) **Decision()** – Message to base station from CH stating a sensor nodes needs to join a cluster without prior information to base station .The base station reads the count of sensor node in each cluster and inform the CH about the deployment of new sensor node
2) **Join ()** – Message to Base station from CH stating need of new sensor node in the cluster

So each CH and VCH will have count of sensor nodes in cluster including SID and location. This is done to ensure the connectivity is enforced within cluster.

B. Range Definition

Range defined for CH is higher than VCH and SN. The border nodes of the cluster are equipped with omnidirectional antenna form efficient communication within the cluster. Functions of Cluster head are as follows

1. Cluster Head evaluates trust between peer CH
2. The final Trust value is calculated for VCH by CH
3. Forward data to other CH and Base station

The Functions of VCH are as follows

1. Calculate the trust value of Sensor nodes
2. Assigns the trust value to Sensor node
3. Sends the trust values to Cluster Head.

IV DRILL SYSTEM PROTOCOL

Hierarchical trust management is implemented by using three levels of Hierarchy namely Peer-to-Peer Trust calculation, VCH-CH Trust calculation and CH-Base station Trust calculation. This protocol is carried out after specific intervals of time. This protocol will be executed for a span of five minutes within which it the trust values will assign, after which the nodes resume their normal operations. Only after a define time will the protocol be run again to check the trust values.

A. Peer-to- Peer Node level Trust

In this trust level, SN Node trust is calculated using three parameters Honesty, Intimacy and Energy. Honesty is the property of a node to successfully complete the work assigned by DTS Command .DTS system is used to give commands like forward packets. The Drill Test Sending Command (DTSC) Packet format is shown in figure 1.

SOURCE NODE	DESTINATION NODE	DTSC MESSAGE AND TIMER	DTSC PATH	ROUTE PATH

Fig 1.DTS Commands Packet format

Source Node field denotes the node which sends DTS Commands and Destination node field denotes the destination node, DTS Command messages are simple unique messages and timer indicates the freshness of the message and also helps in preventing attacks.DTS Path denotes the path in which the DTS Command message

should pass through and finally it defines the routing path information. We also maintain a timer at the source node, this is to avoid indefinite wait for the acknowledgement from the destination node. For Example, consider five nodes, which will be in radio range of node 1. Node 2, 3, 4, 5 are radio range for node 1. Initially node trust value is 0.0, after deployment, nodes first evaluates the trust for 5 minutes, and then starts sensing the data. Now node 1 sends a DTS Command like *"Send HI"* to node 4 through node 3, node 5 and node 2. Now Routing is mentioned in Route path field of DTSC Packet format, node 1 will send DTS Command Packet format to node 3.DTS Commands packet will be like

Source Node	**Destination Node**	**DTSC and Timer**	**DTSC Path**	**Route Path**
1	4	Hi	3→5→2	1→3

Fig 2: DTS Command Packet format in node 3

And once node 3 receives, the DTSCommand packet it forwards the command to node 5 and in node 5 the DTS Command Packet format looks like

Source Node	**Destination Node**	**DTSC and Timer**	**DTSC Path**	**Route Path**
1	4	HI	3→5→2	1→3→5

Fig 3: DTS Command Packet format in node 5

Node 5 receives the DTSC Packet with information of source node, destination node, DTSC message and timer, DTS Path and routing path states that packet came from node 1 and node 3. Now node 5 will look into DTS Path and finds that DTSC Packet needs to forward to node 2 and update it's and sends to node 2(1→3→5→2). In the above packet format only the final field, route path will change and all others fields remains same. Node 5 will forward to node 2. Now node 2, receives the packet and looks into DTSC Path and in this scenario, since there is no other node, node 2 takes the decision and forwards the packet to the destination node. Node 4, upon receiving the packet it checks if it is the destination node and then send an acknowledgement to the source node through the reverse route path.

Source Node	**Destination Node**	**DTSC And Timer**	**DTSC Path**	**Route Path**
1	4	HI	3→5→2	1→3→5→2

Fig 4: DTS Command Packet format in node 2

Node 4 will send an acknowledgement to node 1 with reverse route path and timer in DTSC Message format, Node 1 starts trust calculation of Honesty factor mentioned in equation (1) and it broadcasts a ***success*** message to all nodes mentioned in DTSC path including destination node, so each node can evaluate trust of other nodes mentioned in DTSC Path. It means, in stage 2, node 3 can calculate the trust of node 5 by using equation (1).

Source Node	**Destination Node**	**DTSC And Timer**	**DTSC Path**	**Route Path**
1	4	Hi	3→5→2	4←2←5←3←1

Fig 5: DTS Command Packet format in node 1

Once node 1 decides the node 3, 5 and node 2 performs intended DTS Command it gives value 1 for node 3, 5 and node 2.If node 3 or 5 or 2 failed to perform DTS Command operations it results in assigning value 0 to nodes which failed to do so. Timer is included to prevent various replay attacks and denotes freshness of message. Now each node in radio range will send two tasks to all nodes, which are one-hop Neighbour. As mentioned in above paragraph when node receives success message it calculates trust of other nodes mentioned in DTSC Path. This made our work and system to consumes less energy and detect selfish nodes quickly compared with other system. The trust algorithm is very efficient to detect selfish nodes and consuming very less energy. Even if cluster size increases, it is efficient and in above scenario node 1 giving command to node 3 and node 5, thereby node 3 giving command to 5. This DTSC Messages are carried out until all nodes receives one or two DTSC commands and one DTSC generated by individual node. Finally it measures the Honesty factor or parameter for nodes. It is calculated as

$$Honesty_{(1)} = \frac{DTSC_1 + DTSC_2}{2} \quad (1)$$

The final trust calculation is done by VCH in following equation (2)

$$T_{sn} = \frac{0.3(energy) + 0.4(Intimacy) + 0.3(Honesty\ VCH)}{3} \quad (2)$$

Where T_{sn} is trust calculation of sensor node and energy, Intimacy factor are calcuted by VCH.

Energy Factor:

Vice Cluster Head will read the remaining energy of each and every node and if a node is selfish is it assumed to have high energy compared with threshold value energy because it stops sensing and if node has low energy compared with threshold energy then it is assumed to be compromised because it performs attacks, which consumes high energy. The important factor is to set a threshold value by VCH. It is based on several parameters like idle time, sleep time, sense power, sleep-prob, event radius minimum, event radius maximum and time of node in active state. These parameters determine the threshold value of energy [32],[33] to calculate the Initial threshold value (ITV) .Now the VCH compares the ITV with remaining energy of a node and finally a value is taken from the table and applied in the equation(2). The energy values are assigned comparing with threshold value and the energy value of each node. If energy of node is very low compared to the threshold then a very low value is taken (case in compromised nodes) and if energy of node is very high, then very low value is take (case in selfish nodes).An example is depicted in table , these values are the applied in the equation. VCH then calculates energy parameter and maximum value will be 1. Finally it is then applied to equation (2). As mentioned above using [32][33] methods, Initial Threshold Value(ITV) is calculated using various parameters by VCH. The final value from the table 1 will be used in equation (2). For Example the ITV value is calculated for a node

Initial Threshold Value (ITV)	Value	Initial Threshold Value(ITV)	Value
ITV-1	0.8	ITV+1	0.9
ITV-2	0.7	ITV+2	0.85
ITV-3	0.6	ITV+3	0.8
ITV-4	0.5	ITV+4	0.7
ITV-6	0.3	ITV+6	0.5
ITV-7	0.2	ITV+7	0.4

Table 1: ITV Table

Intimacy Factor:

Intimacy is referred to closeness and relationship between the nodes. It is calculated by adding the value of the Honesty factor of the node mentioned in equation 1. Example: after calculating the Honesty factor value from DTSC Commands each node in the radio range will have its own value of Honesty in one-hop Neighbour. Node 1 will have honesty factor of its radio range nodes like node 2, 3, 4, 5.Node 1 intimacy value is calculated by VCH by getting the values from its neighbours like 2, 3, 4, 5. By adding the value and dividing the number of nodes count will give intimacy factor value. Example node 2 ,3, 4, 5 has honesty factor calculated by equation 1 through DTS Command 0.25 , 0.5, 1, 1 .Then the intimacy is calculated by 0.25+0.5+1+1/4 = 0.68 and it is assigned for intimacy factor.

Honesty Factor by VCH:

As explained above the honesty value is calculated by DTS Commands within the radio range of sensor nodes. It is useful for intimacy calculation as mentioned in above paragraph. Now similar type of DTS Commands is passed by VCH to all the sensor nodes. It is same as explained like each node will get two commands. If the node performs as intended DTS Commands then value will be 0.5 and if it's wrong then – 0.25 will be assigned. It is carried for two scenarios and final value is applied in the equation (2). The main advantage of this scheme is that sensor nodes performs DTS Command for 2 minutes and then continues to perform normal operation like sending data and sensing data. Only VCH calculates the trust calculation using intimacy, energy and honesty factor. So only two minutes the sensor nodes will perform DTS Commands including commands from the Vice cluster Head. So there is no need to evaluate trust and send data to CH which is traditional network trust techniques like GTMS, RFSN, PLUS, Hierarchical Trust Management Protocol .This will definitely increases the network life time since its consuming less energy and VCH calculating only trust value and CH assigning trust value and sending data to other CH and Base station

B.Vice cluster Head and Cluster Head Evaluation

The same concept mentioned above for sensor nodes is applied for VCH-VCH and where DTS Commands are passed VCH for Honesty factor, where CH will make use of Intimacy calculation, Cluster Head DTS Commands are passed, and energy is measured. The same function like VCH for SN is carried out here by CH for VCH Trust evaluation. So trust is calculated by equation 3

$$T_{VCH} = \frac{0.3(energy) + 0.4(Intimacy) + 0.3(Honesty\ CH)}{3} \quad (3)$$

The same process is carried out for VCH like energy, intimacy and Honesty CH. To calculate the SN trust value VCH evaluates the process and for VCH, the CH evaluates the process and for CH, Base station (BS) evaluates the process. Equation 4 is for CH Trust evaluation

$$T_{CH} = \frac{0.3(energy) + 0.4(Intimacy) + 0.3(Honesty\ BS)}{3} \quad (4)$$

The main reason for splitting the trust components like Intimacy, Honesty and energy is to provide the best trust mechanism algorithm. This System unlike other methods does not calculate the trust frequently. DTSC Algorithm makes use of consuming very less energy and assigning trust value soon, which reduces time. The trust value us updated for every 20 hours.

V SIMULATION RESULTS

We carried out the simulation in Network simulator ns2 and results obtained enabled us increase the network life time and quickly finds selfish nodes. The concept of cluster head and VCH including DTS Commands are carried out using C++ code, calling from tcl file. Finally the node performs the intended function and increases the network life time. This enables to find out the trust value of each node soon and reduces the time taken to evaluate the trust calculation. We carried out our simulation work by creating 7 Clusters with Cluster Head and vice cluster Head. Each Cluster consists of 40 nodes and tested our system. Initially Energy and communication range are set high to Cluster Head. The graphs show our simulation work. In first graph, fig 6 shows time taken to detect selfish nodes. We plotted graph by keeping time (hours) in X axis and selfish nodes (number) in Y Axis. Our system quickly detects the selfish nodes and we made some changes in the home tcl files of agent and routing files. We altered the function of node and tried the simulation.

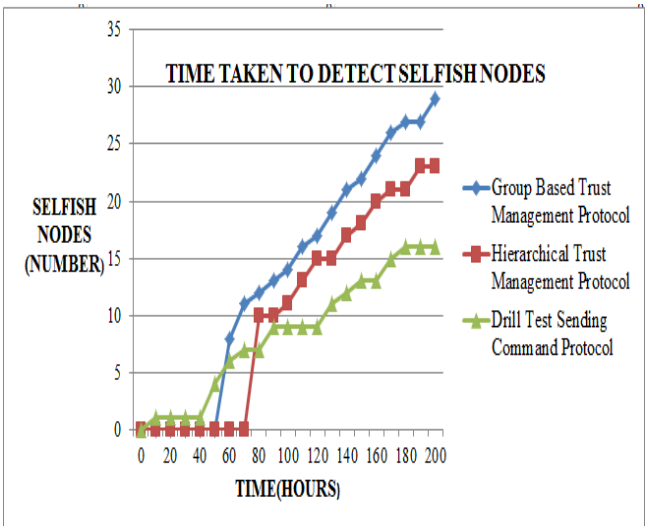

Fig 6 Time taken to detect selfish nodes

Our system detects the selfish nodes quickly compared with other system. Finally number of selfish nodes decreases according to our system, whereas other system starts the trust value 0.5 and proceed the trust algorithm and updates for 80 hours (Hierarchical Trust Management). Our system outperforms other systems by consuming less energy and after 200 hours of simulation the number of selfish nodes is very less than the other two systems

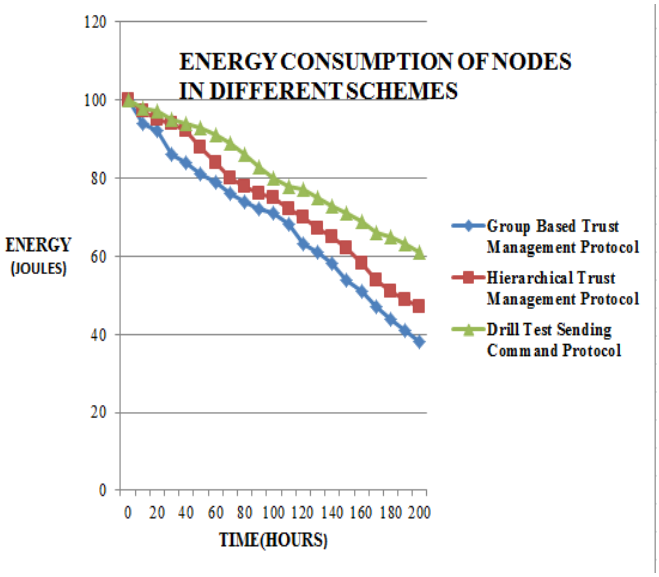

Fig 7 Energy Consumption

Fig 7 shows the graph, where our system consumes less energy. The outcome of the graph shows for simulating various systems for 200 hours with each system the initial energy was set to 100 joules. This is done by using Energy Model concept in ns2.

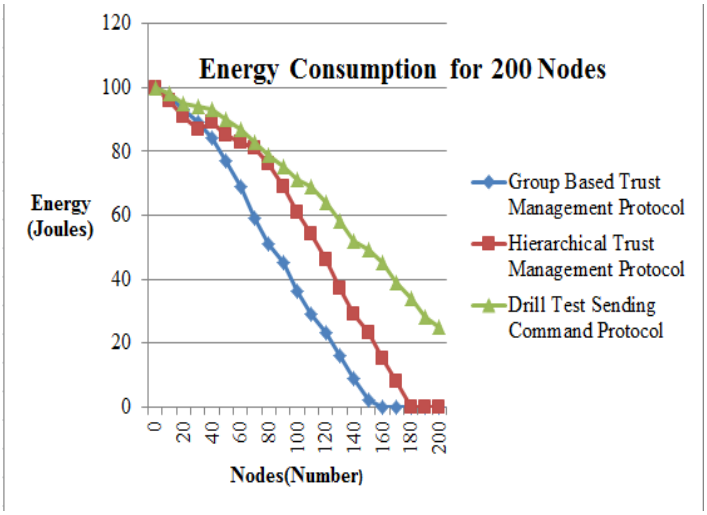

Fig 8 Energy Consumption of nodes

The below graph denotes the variation in trust value of a single node. Initially node trust value starts from 0 and by applying our Drill Test Sending Commands system node value decreases and reaches minimum value soon. As we explained before our system reduces the time taken to detect selfish nodes and consumes less energy. We made a node as a selfish and implemented our system to check the variation in trust value of one node. Once node was identified as selfish the trust value decreases and reached minimum value.

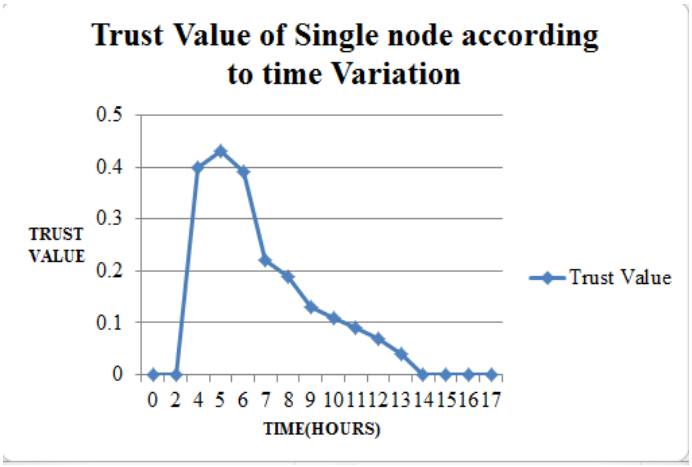

Fig 9 Variation in Trust Value of a single node

VI CONCLUSION

The DTS Commands with integrating Vice Cluster Head concept is used to evaluate the trust value and reduces the time taken to evaluate trust of node. VCH takes care of entire internal trust evaluation i.e. with in cluster and Cluster Head takes care of trust evaluation by external network. This paper solves the issue of trust component and detects the node as a selfish or compromised soon when compared with other work and consumes less energy to evaluate and calculate trust. The future work may include testing the same concept for Dynamic networks including proper clustering scheme.

V11 REFERENCES

[1] Kazem sohraby , Daniel Minoli , Taieb ,znati,*Wireless Sensor Networks Technology ,protocol and applications*, Second edition 1991
[2] Edwin Prem kumar Gilbert , Baskaran Kaliapermal, Elijah blessing Rajsingh "Research issues in Wireless sensor network Applications: A Survey"- *International Journal of information and electronics engineering*, Vol 2 No 5 September 2012[3].
[3] Yanli Yu ,Keigiu Li, Ping Li "Trust Mechanism in wireless sensor networks :Attacks analysis and countermeasures", *Journal of networks and computer applications press 2011*
[4] A.A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-Hoc Networks," Proc. 27th Australasian Computer ScienceConf. (ACSC '04), pp. 47-54, Jan. 2004.
[5] Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.
[6] R.A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y.J. Song, "Trust Management Problem in Distributed Wireless Sensor Networks,"Proc. 12th IEEE Int'l Conf. Embedded Real-Time Computing Systems and Applications (RTCSA '06), pp. 411-414, Aug. 2006.

[7] M. Momani, S. Challa, and K. Aboura, "Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective," Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecomm. T.S. et al., ed., pp. 317-321,
[8] R. A. Shaikh, *et al.*, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.
[9] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Chapter 16: Wireless Sensor Network Security: A Survey," Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, ed., pp. 367- 410, CRC Press, 2006
[10] Z. Liu, A.W. Joy, and R.A. Thompson, "A Dynamic Trust Ad Hoc Networks," Proc. 10th IEEE Int'l Workshop
a. Future Trends of Distributed Computing Systems (FTDCS04), pp. 80-85, May 2004.
[11] S. Buchegger and J.-Y.L. Boudec, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems," IEEE Comm. Magazine, vol. 43, no. 7, pp. 101-107, July 2005.
[12] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *IEEE Trans. Mobile Computing*, vol. 8, no. 5, pp. 606–621, May 2009.
[13] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, ―Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection *IEEE transactions on network and service management*, Volume: 9 , Issue: 2 Page no: 169 – 183, June 2012
[14] Qiao Xuegong and Chenyan "A Control Algorithm Based on Double Cluster-head for HeterogeneousWireless Sensor Network" in 2010 2nd International Conference on Industrial and Information Systems
[15] Zhang Ruihua and Jia Zhiping, Li Xin, Han Dongxue Double Cluster-Heads Clustering Algorithm for Wireless Sensor Networks Using PSO . This research is sponsored by the Natural Science Foundationof China (NSFC) under grant no. 60903031
[16] Wang Bo, Jiang Wei. The Hierarchical Chain-Three Routing Protocol of improved GEGASIS. COMPUTER SYSTEMS & APPLICATIONS, 2009, 12:98-102.
[17] W.B. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
[18] S. Lindsey, C. Raghavendra, and S. Raghavendra, "PEGASIS—Power-Efficient Gathering in Sensor Information Systems," Proc. IEEE Aerospace Conf., vol. 3, pp. 1125-1130, 2002.
[19] A. Manjeshwar and D.P. Agrawal, "TEEN: A Routing Protocol forEnhanced Efficiency in Wireless Sensor Networks," Proc. 15th Int'lParallel and Distributed Processing Symp. (IPDPS '01), pp. 2009-2015,
[20] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient,Distributed Clustering Approach for Ad-Hoc Sensor Networks,"IEEE Trans. Mobile Computing, vol. 3, no. 4, pp. 366-379, Oct. 2004.
[21] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "A Key Predistribution Scheme for Sensor Networks Using DeploymentKnowledge," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 1, pp. 62-77, Jan.-Mar. 2006
[22] S. Ganeriwal and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," Proc. ACM Workshop Securityof Ad Hoc and Sensor Networks (SASN '04), pp. 66-67, Oct. 2004.
[23] A. Boukerche, X. Li, and K. EL-Khatib, "Trust-Based Security for Wireless Ad Hoc and Sensor Networks," Computer Comm., vol. 30, pp. 2413-2427, Sept. 2007. [26] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and Localized
[24] Trust Management Scheme for Sensor Networks Security," Proc. Third IEEE Int'l Conf. Mobile Ad-Hoc and Sensor Systems (MASS '06), pp. 437-446, Oct. 2006
[25] R.A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y.J. Song, "TrustManagement Problem in Distributed Wireless Sensor Networks," Proc. 12th IEEE Int'l Conf. Embedded Real-Time Computing Systems and Applications (RTCSA '06), pp. 411-414, Aug. 2006.
[26] M. Momani, S. Challa, and K. Aboura, "Modelling Trust In WSN from the Sensor Reliability Prospective," Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecomm. T.S. et al., ed., pp. 317-321, Springer,2007.
[27] 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.
[28] H. Chen, H. Wu, X. Zhou, and C. Gao, "Reputation-Based Trust inWireless Sensor Networks," Proc. Int'l Conf. Multimedia and Ubiquitous Eng. (MUE '07), pp. 603-607, Apr. 2007.
[29] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation managementfor sensor networks," *Wireless Networks*, vol. 16, no. 5, pp. 1493–1510, July 2010.
[30] L. Capra and M. Musolesi, "Autonomic trust prediction for pervasivesystems," in *Proc. 2006 Int. Conf. Advanced Inf. Netw. Applications*, pp. 1–5.
[31] L. Capra, "Engineering human trust in mobile system collaborations," in *Proc. 2004 ACM SIGSOFT Int. Symp. Foundations Software Engineering*.
[32] K. Benkic "Using RSSI Value for Distance Estimation in WSN Based on ZIGBEE*" in Systems, Signals and Image Processing, 2008. IWSSIP 2008. 15th International Conference on* 25-28 June 2008
[33] R. A. F. Mini, A. A. F. Loureiroa, and B. Nath, "The distinctive design characteristic of a wireless sensor network: the energy map," *ComputerCommun.*, vol. 27, no. 10, pp. 935–945, June 2004.
[34] Y. J. Zhao, R. Govindan, and D. Estrin, "Residual energy scan formonitoring sensor networks," in *Proc. 2002 IEEE Wireless Commun. Netw. Conf.*, pp. 356–362.
[35] G. Edwin Prem Kumar et al , "A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network" in *International conference on Modeling Optimisation and Computing.* Proceeda engineering 38 (2012) pp 2903-291
[36] Dave Singelee et "Location Verification using secure Distance Bounding Protocols" *International Journal of Computer Applications* Volume 56 – No 17 October 2012