A Lightweight Trust System with Provisioning for Detecting Malicious Node in Clustered Wireless Sensor Networks

SudhaRani.S[#1], George Samuel Raj. V [*2], Earnest Paul. S [#3]

[#]*Assisitant Professor, Department of Computer Science, Karpagam College of Engineering, Coimbatore, India*

[*]*P G Scholar, Department of Mechanical Engineering , Karunya University, Karunya Nagar, Coimbatore, India*

[#]*P G Scholar, Department of Renewable Energy (EEE), Karunya University, Karunya Nagar, Coimbatore, India*

***Abstract*— Wireless sensor networks is one of the prominent computing network emerged worldwide due to its applications and features. One of the wireless sensor network is clustered wireless sensor network in which a set of sensor nodes are partitioned into certain number of clusters and within each cluster active sensor nodes are associated as cluster members, a sensor node with strong computing power is elected as a cluster head. Malicious node in clustering network is a key problem. A lightweight trust system is employed to reduce the effects of malicious node and a dogger timer is used to detect the malicious node in less time. Incorporating lightweight trust system with provision to detect malicious node along with time factor will avoid problem such as drop of data, defragmenting network and isolating network.**

***Keywords*— Sensor networks, Security, Trust management, Lightweight Trust System, Dogger timer.**

I. INTRODUCTION

A Sensor network consists of tiny autonomous, geographically scattered and dedicated sensor devices for monitoring and recording the physical conditions of the environment. Large number of sensor nodes are densely deployed inside the phenomenon or far away from the phenomenon or very close to the phenomenon. Wireless sensor networks are strictly constrained in terms of limited memory, computational capacities, energy, bandwidth and low power consumption. Each sensor node has its own hardware components such as sensing unit, processing unit, power unit, transceiver unit, power generator, mobilizer and location finding system. Sensing unit consists of two components: Sensor and ADC (analog to digital converter). Processing unit is made up of processor and a storage. The factors which influence the design of sensor network includes fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission range and power consumption [1].

Sensor networks can be broadly classified into two categories: Category 1 WSN (C1 WSN) used for dynamic routing with a multi hop connectivity and Category 2 WSN (C2 WSN) used for static routing with a single hop connectivity [1]. Based on the services offered, wireless sensor network performs four different function such as monitoring, alerting, information on-demand and actuating [7]. The fundamental operation of sensor network is sensing of data, processing of sensed data and forwarding processed data to the desired destination. Initially, smart dust motes also called as sensor nodes are scattered in a particular environment to sense the data, then the sensed data is processed and forwarded to the sink node also called as base station (desired destination).

A. Current and future Applications

Wireless sensor networks are eventually applicable in the fields of Military, Health, Environmental, Home and Commercial [2]. Military applications are monitoring of friendly forces, monitoring equipment and cartridge, battlefield surveillance, reconnaissance, targeting (C4ISRT) system, detection of nuclear, biological and chemical attack [1]. Environmental application includes forest fire detection, flood detection, tsunami detection, earthquake detection, precision agriculture [1]. Health applications are monitoring human physiological data, tracking and monitoring doctors as well as patients inside hospitals drug administration. Home application includes home automation, Heating Ventilation and Air Conditioning (HVAC), Smart environment [1]. Commercial applications are monitoring and managing building material stocks, robot control, environmental control in office buildings, interactive museums, detecting and monitoring car thefts, vehicle tracking [1]. Some other applications are monitoring floods, monitoring traffic of automobiles, monitoring parameters such as temperature, humidity, pressure, wind direction and speed, brightness of light intensity, sound magnitude, power line voltage, chemical concentrations, pollutant levels and vital body functions [1], [2]. Future applications are research oriented applications which includes Biological Task Mapping, Biomedical signal monitoring related to Biological applications. Environmental application includes Green house monitoring, Habitat Surveillance [3]. Commercial applications are Smart parking,

Vehicular Telematics, Security of Intra-car, Event detection, Structural Health Monitoring [3].

The discussion of the paper is as follows. Section I provides a brief description about Wireless Sensor Networks and its current and future applications. Section II describes the need and importance of security in WSN with some challenging attacks. Section III gives the need of Trust Management in WSN. Section IV provides related work. Section V deals with Proposed System, Section VI describes about simulation results. Section VII concludes the paper.

II. Necessity For security in WSN

As wireless sensor network deals with real time applications, security plays a very important role because of its wireless communication [24]. In wireless channel, attackers can be easily access data anywhere in network at any time, hence different security schemes need to be integrated when data sent from sensor nodes to base station [24]. Security mechanisms provides data integrity, data confidentiality, data authentication, non-repudiation, availability, self-organisation, time synchronization, data freshness, secure localization, flexibility, robustness and survivability, access control, user privacy and continuity of service [4], [5].Wireless sensor networks are characterized by denser levels of node deployment, unreliable communication of sensor nodes, compact size, severe power, computation capabilities, memory space, bandwidth and energy constraints in which sensors are being deployed in the adverse environment thus sensor nodes are vulnerable to several types of attacks [4]. As a result, security in wireless sensor networks has been an everlasting challenge in such resource constrained network. Attacks can be performed in a variety of ways. Different possible attacks created by malicious nodes are as follows:

- Bad Mouthing Attack: Propagate negative reputation information about good nodes [5], [6].
- Good Mouthing attack: Propagate positive reputation information about bad nodes [5].
- Energy Drain Attack: Radiate a large amount of traffic and require other nodes to respond [5], [6].
- Homing Attack: The attacker investigates network traffic to interpret the geographical area of cluster heads or base station [4]
- Node Replication Attack: Unique ID of sensor node can be duplicated by an attacker and assign to new added malicious node in the network [4]
- Sinkhole Attack: Attacks nearby network traffic through compromised node [5], [6]
- Exhaustion: Dominates the power resources of the nodes by causing them to retransmit the message even when there is no collision or late collision [4].
- Sniffing Attack: Overhear valuable data from the closeness nodes [5], [6].
- Greyhole Attack: Drop certain types of packets [5], [6].
- Conflicting Behaviour Attack: Attacker damages good node's recommendation of trust by performing differently to different nodes [21], [5].

III. NEED FOR TRUST MANAGEMENT IN WSN

In recent years, research community considered Trust Management in wireless sensor network has an interesting "state-of-the-art" because it deals with secure routing and secure data on resource constrained WSN [5]. The first trust management system proposed by Blaze et al. (1996) was "PolicyMaker" [9]. Trust management helps to improve the security of wireless sensor networks [7].

A. Concepts

Trust: In general, trust is the level of confidence and level of assurance in a person or a thing [8]. In wireless sensor network, person or thing corresponds to sensor nodes. Trust is interpreted as belief, subjective probability and reputation [5]. Trust is a subjective opinion in the reliability of other entities or functions which includes veracity of data, path connection, node processing capability and availability of service etc. [5] [25]. Trust is the value based on the past behaviour of nodes [21]. When the trust value of nodes is known in the network, the nodes will take appropriate action against malicious nodes during operational decisions [26], [21]. The characteristics of trust are subjective, dynamic, asymmetric, incomplete transitive, reflexive and context-sensitive [5]. The primary purpose of employing trust in WSN is to provide self-sufficiency [7] and self-healing [5]. Self-sufficiency means network must be able to configure itself not only during normal operation of network, but also during abnormal events [7]. Self-healing refers to network must be able to prevent diverse attacks inside networks. The development of trust leads to different types of trust such as data trust, communication trust, authorization (hard trust), evaluation (soft trust), node trust, path trust and service trust [7].

B. Terminologies

- Trust: Trust is based on how the node would behave in the future [21].
- Reputation: Reputation is based on the performance of the node in the past [21].
- Direct Interaction: A value which is calculated by the node regarding its neighbours. It is also called as first-hand information [21], [8].
- Indirect Interaction: A calculated trust value provided by neighbouring node regarding its neighbouring nodes and it is also called as second-hand information [21], [8].
- Trust Value: A value which is assigned between the ranges of 0-100. Values can also range from negative to positive [21].

IV. RELATED WORK

A. Based on Reputation and Trust Systems

Saurabh Ganeriwal et al [12] proposed a reputation framework for sensor networks which determines the state of worthiness based on the node's activity. This is the first framework designed and developed for sensor networks. It allows nodes to exchange only good and direct reputation

information being propagated. This method is mainly used to identify malicious nodes in the network. It makes use of first-hand information and second-hand information to update reputation values. In this framework, each node maintains reputation and trust value only for their neighbouring nodes because nodes require prior reputation knowledge about a node. A watchdog method is used to form the first-hand and second-hand information to obtain the trust level value using reputation value. Once the trust value is higher than certain threshold, framework identifies whether the node is trustworthy or not to continue its operation. It is assumed to pursue a probability distribution and Beta distribution model for reputation computation. Framework also uses a Bayesian formulation which is as follows,

$$\textbf{P (Belief / Observation)} = \frac{\textbf{P(observation/belief)} * \textbf{p (belief)}}{\textbf{Normalisation}}$$

Srinivasan et al [13] proposed a Distributed Reputation and Trust based Beacon Trust System. A distributed model is specially designed to solve location beacon sensor network problems which uses both first-hand and second-hand information. It consists of symmetric beacon node (BN) and asymmetric sensor node (SN) where BN identifies location of SN to send data to SN enabling sensor node to exclude the malicious location information provided by malicious beacon node. Thus the model avoids the malicious behaviour of any BN. A watchdog method will watch the neighbour node when communication takes place between sensor node and beacon node. It allows node to exchange both positive and negative reputation information.

Marti et al [17] proposed a Mitigating Routing misbehaviour in mobile Adhoc Networks which uses a watchdog and path-rater components. It avoids any malicious node that takes place in routes. Watchdog is used to detect the denied packets by malicious node during forwarding. Path-rater is used for trust management and routing. A method called rating is used to rate every path used for forwarding of data in the network. Thus the good nodes are strengthened against malicious nodes by using rating method.

Mirchiardi and Molva et al [16] proposed a collaborative reputation mechanism to enforce node cooperation in Mobile Adhoc Networks. The main objective of reputation framework is to reduce the false detection of the misbehaviouring nodes. It consists of subjective reputation, indirect reputation and functional reputation to compute reputation value. Subjective reputation deals with observation of nodes behaviour. Indirect reputation deals with positive reports provided by other nodes. Functional reputation is about task specific behaviour. It consists of two type's protocol entities, a requestor and a provider to compare the reputation values generated by both malicious node and non-malicious node using a two way symmetry communication and dynamic source routing protocol.

Buchegger and Boudec et al [15] proposed a security model called as Cooperation of Nodes-Fairness in Dynamic Adhoc Networks to identify the misbehaviour of nodes based on unselfish concern and selfish concern. It makes use of both first-hand and second-hand information to compute the reputation value. It uses a routing protocol called as Dynamic Source Routing (DSR) to route the nodes in the network. Malicious or misleading nodes are punished using isolation method in which nodes are segregated to access the network resources and sends a message called friend only to its trusted members.

The concepts used in CONFIDANT are monitor, trust manager, reputation system and path manager. Monitor protocol will continuously monitor the network to identify any malicious behaviour. Trust manager protocol handles incoming and out-coming ALARM messages. Reputation system consists of a table in which reputation values of nodes entry is done. Path manager protocol removes the misleading paths generated by misbehaviour nodes in the network. This security model allows nodes to exchange only negative information.

Buchegger and Boudec et al [14] proposed a Robust Reputation System for Peer-to-Peer and Mobile Adhoc Networks. It makes use of both positive and negative first-hand and second-hand information. RSS uses Bayesian formulation with Beta distribution for updating reputation. Two main concepts called as: reputation and trust is used where reputation is used to identify nodes as either normal node or abnormal node whereas trust is used to classify nodes as either trustworthy or untrustworthy. Using deviation test method the reputation information and trust information is varied according to certain threshold and then nodes are evaluated as normal, abnormal, trustworthy and untrustworthy node. A robust reputation system exchanges only fresh information and concentrates more on the current behaviour information than on past behaviour information of trust and reputation. This method is mainly used to identify malicious behaviour of nodes.

B. Based on Lightweight Trust Systems

Riaz Ahmed et al [8] proposed a Group-Based Trust Management Scheme for clustered Wireless Sensor Networks. The main objective is to detect and prevent malicious, selfish and faulty nodes. A lightweight scheme is used to evaluate the trust of a group of sensor nodes. It does not focus on the trust values of individual sensor nodes rather focus on trust values of group of sensor nodes. Broadcast based strategy is used for data communication. It is suitable for large scale sensor applications. The calculation of trust values depends on both direct and indirect observations of network. It uses two different types of topologies: Intragroup topology and intergroup topology. Intragroup topology is a distributed trust management and Inter topology is a centralized trust management. In Intragroup topology, trust value assignment is done in three possible states: trusted, untrusted and uncertain. Once the states been assigned to the nodes the centralized trust management takes place. This trust model falls into three categories of phases: Trust calculation at the node level, Trust

calculation at the Base station level. At node level, calculation is done using either time-based past interaction and peer recommendations. Due the resource constrained feature of sensor nodes, trust system is modelled lightweight.

Xiaoyong Li et al [18] proposed a LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks. The main objective is to reduce the effect of malicious, selfish and faulty nodes to facilitate less communication overhead and storage overhead in clustered wireless sensor networks. There are two levels of trust relationship: Intracluster trust and Intercluster trust. Intracluster trust evaluation is of two levels: cluster member-to-cluster member and cluster head-to-cluster member feedback. Intercluster trust evaluation is of two levels: cluster head-to-cluster head and base station-to-cluster head feedback. Communication between cluster members to cluster head makes the system lightweight and communication between cluster head to cluster head makes the system as Dependability enhanced system. It makes use of self-adaptive Weighting method to do trust aggregation of cluster heads to obtain a global trust degree. No broadcast communication takes place thus reduces the flooding problem and saves energy. The system in overall improves the efficiency since it is using peer recommendations. The trust degree calculation is done using direct observation and indirect feedback. It is applicable in a very large wireless sensor network applications.

C. Based on Energy Trust Systems

Guoxing Zhan et al [19] proposed a Trust Aware Routing Framework for Wireless Sensor Networks. The main objective designs are throughput, energy efficiency, Scalability and Adaptability. It does secure multi-hop routing against attackers to avoid replaying routing information by evaluating trustworthiness of nodes and its neighbour's nodes. It incorporates trustworthiness of nodes and energy efficiency into routing decisions. Energy efficiency evaluates hop-per-delivery as,

$$\textbf{Hop-per-delivery} = \frac{\textbf{Number of all hops}}{\textbf{number of all delivered data packets}}$$

It deals with three main concepts: the neighbouring nodes communication, trust level, energy cost. When system deals with these concepts, they use two main components: EnergyWatcher and WatchManager. EnergyWatcher is responsible for recording the energy cost for each known neighbour based on the one-hop transmission to reach its neighbours. TrustManager is responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about packets which not being delivered. The energy cost can be established using the following relation,

$$E_{Nb} = E_{N \to b} + E_b$$

E_{Nb} is node's energy cost, the average energy cost of successfully delivered data packet is $E_{N \to b}$, and broadcast energy is E_b. Thus system not only prevent malicious nodes corrupting good node's identification like deceiving network traffic but also provides efficient energy usage.

Christhu Raj et al [20] proposed a Drill System based Hierarchical Trust Calculation to detect Selfish nodes in Wireless Sensor Network. When identifying malicious nodes and calculating trust value of node, network takes huge amount of network time. Hence system is designed in such a way that it reduces time taken to calculate trust values and consumes less energy. The model consists of vice cluster head which calculates the trust value of sensor nodes, then assigns trust value to sensor nodes and finally sends the trust values to cluster head. It consists of three different rankings: Peer-to-peer trust calculation, vice cluster head trust calculation, Cluster head to base station trust calculation.

V. PROPOSED SYSTEM

In wireless sensor network, the two most important component is base station and sensor node also called as motes or smart dust motes. Sensor nodes are used to sense the physical phenomenon of the environment such as temperature, humidity, etc. and forward the sensed data to its neighbouring node which inturn forwards it to the final destination called base station using wireless channel [7]. Base station acts as the "powerful device" and collects all the sensed information from nodes and stores it for later use [7]. In Wireless communication, source sensor node, neighbouring sensor node and destined base station is sometimes prone to security problems such as neighbouring senor node gets compromised or damaged, and also tries to compromise other sensor nodes in the network. In order to filter out compromised nodes from sensor networks, modelling of lightweight trust system is required [5].

During routing operation, sensor nodes need to know which other nodes to trust for forwarding data [7]. During sensing and communicating process, a node might need to trust other neighbouring nodes for checking abnormal activities such as data disclosure decisions, privacy, hardware protection [7]. Malicious nodes not only compromise other nodes data but it also compromises keys used for communication, to overcome this problem we employ some cryptographic measures [22], [27]. Cryptographic measure includes Key management, secure routing and secure communication [23]. Along with cryptographic measures, it is mandatory to use trust management schemes also [7].

A. Motivation

Detecting malicious Cluster Member (CM) and Cluster Head (CH) is important in resource constrained nodes of clustering network. At the same time, the amount of time taken to detect malicious node need to be less. In a hostile environment, such malicious node may cause the problems like network fragmentation, network isolation causing the data to drop and also drains the energy of nodes. To prolong the network lifetime considering time as a factor, we use both a lightweight trust system [18] and dogger mechanism to set the

dogger timer to detect malicious node in clustered wireless sensor networks.

B. System Model

A framework of trust oriented clustered WSN is developed. A mechanism of detecting the malicious nodes are elected as cooperative nodes. A node in clustered WSN can be cluster member (CM) and cluster head (CH). Cluster member in the cluster will communicate with their cluster head (CH) directly. Cluster head (CH) will forward the aggregated data to the centralized base station through other cluster head's (CH's). Clustering is assumed to be organized by LEACH (Low energy Adaptive Clustering Hierarchy). A secure communication channel is established using cryptography Key management mechanism which includes schemes such as SPINS, LEAP and Tiny sec

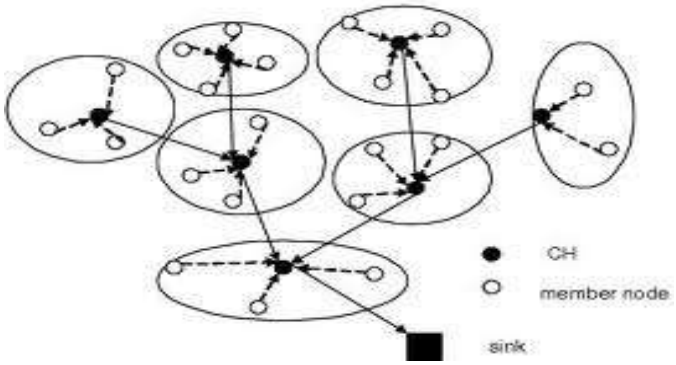

Fig. 1 Clustered Wireless Sensor Networks

Clustered wireless sensor network is created using LEACH protocol [1] [2]. It is created using Mannasim patch in NS2 2.29. Fig.2 shows LEACH clustering graph with X-axis as time in (milliseconds) and Y-axis as data rate in (kbps). Using the trace file generated the graph is plotted. This shows the way how clustering is done for lightweight system.

C. Methodology

Lightweight trust system deals with two types of trust direct trust and indirect trust. Direct trust is a value calculated by node regarding its neighbours. Indirect trust is a calculated trust value provided by neighbouring node regarding its neighbouring nodes [18]. In lightweight trust system, direct trust deals with cluster member to cluster member (CM-to-CM) and cluster head to cluster head (CH-to-CH). Indirect trust deals with cluster member to cluster head (CM-to-CH) and cluster head to base station (CH-to-BS) and vice versa.

Using the trust value, the malicious node effects are reduced in the network. Trust value is a value being assigned between the range of 0 - 100. Value can be either a positive value or a negative value. Initially, trust value of node starts from 0.5 and then increases or decreases according to trust decision making operations. Lightweight trust system provides a strong security against intelligent attack. An intelligent attack is the one the malicious node provide services good or bad according to the threshold of trust values.

Dogger timer is to detect the malicious node considering time as a factor, we use dogger mechanism to determine node misbehavior by copying packets which to be forwarded into a buffer and monitoring the behavior of the neighboring nodes with respect to packet forwarding. We propose a timer called as dogger timer to detect the malicious node. We propose certain new commands for timer to detect the malicious node. It is an electronic timer that is used to detect and recover from node malfunctions. During normal operation, the node regularly restarts the timer to prevent it from elapsing or timing out. If, due to a hardware fault or program error, the computer fails to restart the dogger, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the node in a safe state and restoring normal node operation.

Table I
Dogger Timer commands

DogTime	DogCTL	DogPAT	DogState

DogTime sets the timeout period before attempting to enable the timer. If the dogger function is enabled, the time-out period is immediately reset so that the new value can take effect. An error (EINVAL) is displayed if the timeout period is less than 1 second or longer than 180 minutes. DogCTL enables or disables the dogger and/or capacity. It uses the reset_enable member to enable or disable the system reset function. It uses the dog_enable member to enable or disable the dogger function. An error (EINVAL) is displayed if the dogger is disabled but reset is enabled. If DOGTIME has not been issued to set up the timeout period prior to this CTL, the dogger is not enabled in the hardware. DogPAT rearms or pats the dogger so that the dogger starts ticking from the beginning that is, to the value specified by DOGTIME. If the dogger is enabled, this CTL must be used at regular intervals that are less than the dogger timeout or the dogger expires. DogState gets the state of the dogger and reset functions and retrieves the current time-out period. If DOGSTATE was never issued to set up the timeout period prior to this CTL, the dogger is not enabled in the hardware. The DOGSTATE CTL requires only that open ( ) be successfully called. This CTL can be run any number of times after open ( ) is called and it does not require any other DOG CTLs to have been executed.

Dogger timer not only detects the malicious node in less time but it also provides strong apposition against greyhole attack. Greyhole attack is an attack in which certain packets or data is dropped by malicious node in the network.

VI. SIMULATION RESULTS

We performed our simulation in Network Simulator (NS2) 2.29 along with Mannasim used as a patch for NS2. Execution is done using corresponding tcl files at the front end and C++ files at the back end using appropriate routing protocols. The graphs indicate the simulation work being done in NS2. In first graph, we plotted the number of packets being dropped with respect to time in hours. X- axis indicate time (hours) and

Y- axis indicate the drop packets. Fig.3 shows the greyhole attack by indicating the number of dropped packets.

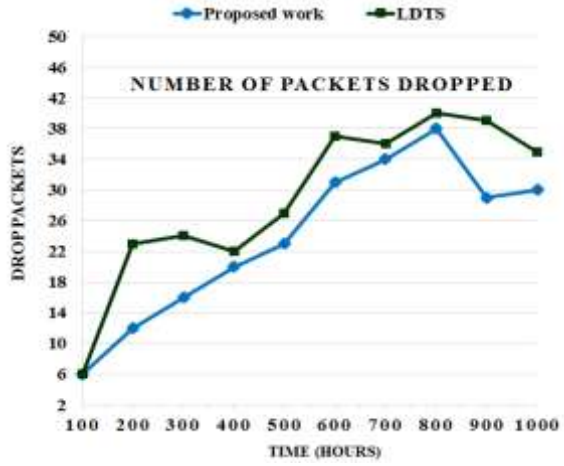

Fig 3. Number of Packets Dropped

The above graph indicates that the number of dropped packets is less compared to the existing work LDTS. Hence we can show the reliability of the network. The reliability of the network is indicated using packet successful delivery ratio. Fig 4 and Fig 5 shows the packet successful delivery ratio at cluster member and Cluster Head respectively in terms of percentage.

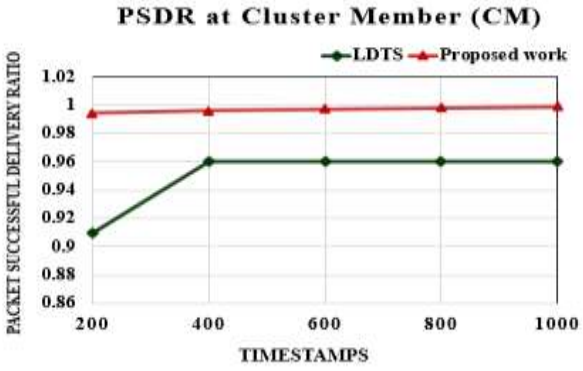

Fig 4. PSDR at Cluster Member (CM)

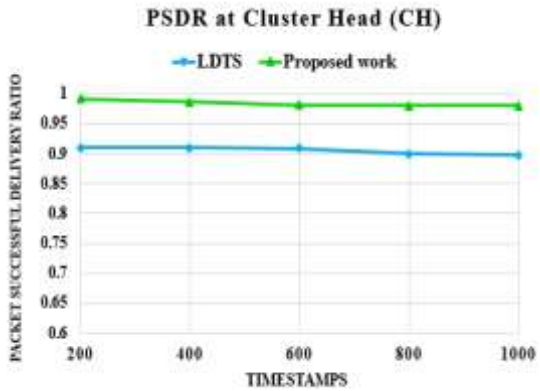

Fig 5. PSDR at Cluster Head (CH)

PSDR at cluster member is 98.5% and PSDR at cluster head is 96%. We plotted X-axis with time stamps and Y-axis with Packet successful delivery ratio.

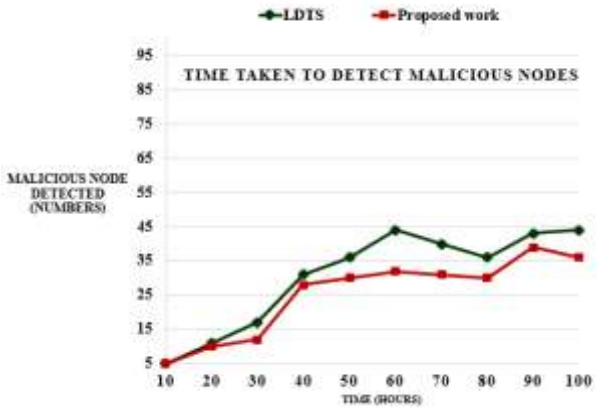

Fig 6. Time taken to detect malicious node

Fig 6 shows the X- axis with time (hours) and Y-axis with malicious node detected (number). The graph indicates that the malicious node is detected quickly using proposed work when compared to existing work.

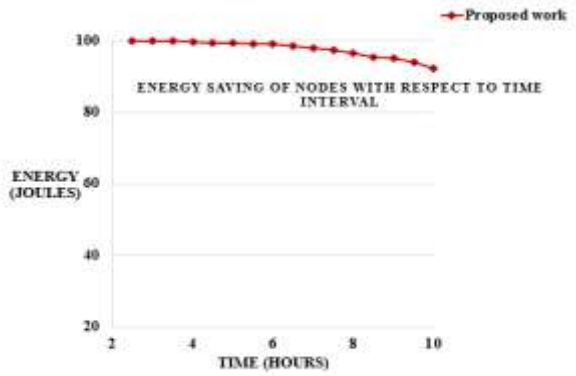

Fig 7. Energy consumed with respect to time

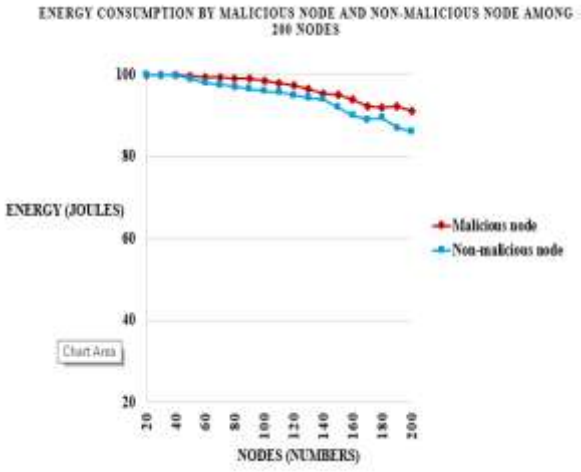

Fig 8. Energy Consumption among 200 nodes

Fig 7 and Fig 8 shows the Energy simulation work. Fig 7 shows the graph with X-axis time (hours) and with Y- axis

energy (joules).The graph shows that our proposed system saves more energy by detecting the malicious node in less time. Fig 8 shows the graph with X-axis node (number) and with Y-axis energy (joules). Initial energy been set is 100 joules. This is done using the concept of energy model in NS2. The graph of fig 8 shows that our proposed system consumes less energy.

VII. CONCLUSION

Security is one of the paramount importance to be considered in clustered wireless sensor networks because of resource constrained feature and being deployed in the hostile area. It is not an exaggeration to state that one has to be paranoid while analysing the security aspects of clustered wireless sensor networks. A network is only as secure as the weakest link in the security chain and hence it is important to analyse every trust in the network. In trust management, it was provided that each sensor node may know which neighbouring node to trust so as to forward data to the desired destination. The trust system and watchdog timer together detects the effect of malicious nodes in less time. It was also looked that the system provides increased network lifetime by analysing the simulated energy consumption results and also the reliability of the network is achieved using packet delivery ratio in terms of 98.5% and 96%.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "*Wireless Sensor Networks: a Survey*," Computer networks, 38, pp. 393 – 422, December 2002

[2] *Kazem* sohraby, Daniel Minoli, Taieb Znati, "Wireless sensor networks: technology, protocols and *applications"*. First edition, 2012

[3] Edwin prem kumar, 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

[4] Aashima Singla, Ratika Sachdeva, *"Review on security Issues and Attacks in Wireless Sensor Networks" – International Journal of Advanced Research in Computer Science and Software Engineering",* vol 3 No 4, April 2013.

[5] Yanli Yu,Keigiu Li, Ping Li "Trust Mechanism in wireless sensor networks :Attacks analysis and countermeasures", *Journal of networks and computer applications press 2011*

[6] Jyoti Shukla, Babil Kumari, "*Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview- International Journal of Application or Innovation in Engineering and Management",* vol 2 No 3, March 2013

[7] Javier Lopez, Rodrigo Roman, Issac Agudo, Carmen Fernandez-Gago, "*Trust management systems for wireless sensor networks:Best practises-",* Computer Communications, 33, pp.1086-1093, February 2010.

[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] Blaze M, Feigenbaum J, Lacy J. "Decentralized trust management". *In: Proceeding of the 1996 IEEE symposium on security and privacy*, Washington, 1996. pp. 164–73.

[10] W.B. Heinzelman, "*Application-Specific Protocol Architectures for Wireless Networks," IEEE Trans. Wireless Communication*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[11] R. Devika, B. Santhi, T.Sivasubramanian, "Survey on routing protocol inWireless Sensor Network", *International Journal of Engineering and Technology*, Vol 5 No 1 Feb-mar 2013.

[12] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Networks.*, vol. 4, no. 3, pp. 1–37, May 2008.

[13] A. Srinivasn, J.Teitelbaum, J.Wu, " DRBTS: Distributed Reputation based Beacon Trust system, In proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, USA, 2006.

[14] S. Buchegger, J. –Y.Le Boudec, "A Robust Reputation system for Peer-to-peer and Mobile Adhoc Networks", In proceedings of P2Pecon 2004, Harvard University, Cambridge MA, USA,June 2004.

[15] S.Buchegger and J-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of Nodes-Fairness In Dynamic Adhoc Networks), In Proceedings of MobiHoc 2002, Lausanne, CH,June 2002

[16] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enhance node cooperation in Mobile Adhoc Network, Communication and Multimedia security, September 2002

[17] S.Marthi, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehaviour inMobile adhoc Networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom) 2000.

[18] Xiaoyong Li, Feng Zhou, and Junping Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks",IEEE Transactions on Information Forensics and Security, Vol. 8, No. 6, June 2013

[19] Guoxing Zhan, Weisong Shi, Julia Deng, "TARF: A Trust Aware Routing Framework for Wireless Sensor Networks", pp. 65-80, 2010

[20] Christhu Raj M. R, Edwin Prem Kumar.G, Kartheek Kusampudi", Drill System bsed Hierarchical Trust Calculation to detect Selfish nodes in Wireless Sensor Network", International Journal of Engineering and Technology, Vol 5, No. 1, Feb-mar 2013.

[21] G. Edwin Prem Kumar, Titus. I, Sony. I. Thekkekara, "A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Networks, International Conference on Modeling Optimisation and Computing, Procedia Engineering 38, 2012.

[22] Sudip Misra, Ankur Vaish, "Reputation based role assignment for role based access control in wireless sensor networks", Computer Cmmunications, Vol 34, pp. 281-294, 2011.

[23] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions", Systemics, Cybernetics and Informatics, Vol. 1, No. 4, pp. 90-100, 2004

[24] Rodrigo Roman, Carmen Fernandez-Gago, Javier Lopez, "Featuring Trust and Reputation Management Systems for Constrained Hardware Devices", in Proc. Autonomics 07, 2007

[25] Adrian Perrig, Robert Szewczyk, J.D. Tygar, /victor Wen, David E. culler, "SPINS: Security Protocols for Sensor Networks", Mobile Computing and Networking, Vol 8, pp. 521-534, 2002.

[26] Chris Karlof, Naveen Sastry, David Wagner, "TinySEC: A Link Layer Security Architecture for Wireless Sensor Networks", SenSys 04, 2004.

[27] Sun YL, Han Z, Yu W, Liu KJR, "A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks", IEEE INFOCOM 06, pp. 1-13, 2006

[28] Boukerche A, Ren Y, "A trust based security system for ubiquitous and pervasive computing environments, Computer Communications, 31(18), pp.4343-51, 2008.

[29] Jaramillo J, Srikant R, Darwin: distributed and adaptive reputation mechanism for wireless adhoc networks. In: Proceedings of the 13th annual ACM international conference on mobile computing and networking, pp. 87-98, 2007.

[30] Papaioannou T, Stamoulis G, "Achieving honest ratings with reputation based fines in electronic markets, In: IEEE INFCOM, p. 1040-8, 2008.

[31] Hani Alzaid, Juan Gonazalez Nieto, Ernest Foo, "Secure data aggregation in wireless sensor network" in Proc. 6th Australian conference on Information security, vol. 81, 2011