ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Comprehensive Review on Reduction of Malicious Nodes in Clustered Wireless Sensor Networks Using Different Trust Management Schemes

Sudha Rani S [#1], Edwin Prem Kumar G[*2], B. Juswin Thilak[#3]

[#1] PG Scholar, Dept of Information Technology, Karunya University, Karunya Nagar, Coimbatore, India

[*2]Assistant Professor, Dept of Information Technology, Karunya University, Karunya Nagar, Coimbatore, India

[#3] PG Scholar, Dept of Information Technology, 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. The three major operations in sensor network are data sensing, data aggregation and data forwarding. One such type of wireless sensor network is clustered wireless sensor network in which a set of sensor nodes are partitioned into a 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 cluster member and malicious cluster head is one of the key problem in clustering network. To reduce the effects of malicious or compromised nodes overhead in the network, we reviewed various Trust Mechanisms which calculates the trust value to identify the behaviour of malicious or compromised nodes. This paper is based on the survey of existing routing protocols related to clustering network and various existing trust management methods to provide enhanced security by preventing malicious nodes in clustering network.

Keywords – Sensor networks, Security, Attacks, Trust, Reputation, Trust models, Routing protocol, Trust techniques.

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 describes various trust methodologies. Section V deals with different routing protocols, Section VI describes about different trust techniques. Section VII concludes the paper with future scope.

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:

1. Bad Mouthing Attack: Propagate negative reputation information about good nodes [5], [6].
2. Good Mouthing attack: Propagate positive reputation information about bad nodes [5].
3. Energy Drain Attack: Radiate a large amount of traffic and require other nodes to respond [5], [6].
4. Homing Attack: The attacker investigates network traffic to interpret the geographical area of cluster heads or base station [4]
5. 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]
6. Sinkhole Attack: Attacks nearby network traffic through compromised node [5], [6]
7. 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].
8. Sniffing Attack: Overhear valuable data from the closeness nodes [5], [6]
9. Neglect and Greed Attack: Disturbs the behaviour of the adjoining nodes, which may not be able to receive or send messages [4].
10. Greyhole Attack: Drop certain types of packets [5], [6].
11. Whitewashing Attack: Re-enter the system with a new identity and a fresh reputation [5], [6].
12. Hello flood Attack: Establish the attacker as the data destined for the base station through it [5], [6].
13. Node outage: Halting the working of nodes [4].
14. Garnished Attack: Malicious nodes behave both good as well as bad with the aim of remaining undetected in the network.
15. DoS Attack: Prevent any part of WSNs from functioning correctly or in a timely manner [5], [6].
16. Conflicting Behaviour Attack: Attacker damages good node's recommendation of trust by performing differently to different nodes [24], [5].
17. Intelligent Attack: The compromised node provide services good or bad according to the threshold of trust values [5], [24].
18. Sybil Attack: The attacker is able to present multiple identity within the network to affect the data aggregation function [24], [45].
19. Selective forwarding Attack: When the attacker is in network, the decision to forward the data depends upon the attacker [45].

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].

In wireless sensor network, the two most important component is base station and sensor node also called as motes or smart dust motes. Motes are simply used to sense the physical phenomenon of the environment such as temperature, humidity, etc. and forward the sensed data to its neighbouring sensor node which 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 motes and stores it for later use based on the application [7]. Wireless communication taking place between 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 management system is required [5].

During routing process, sensor nodes might need to know which other nodes to trust for forwarding a 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 [25], [27]. Cryptographic measure includes Key management, secure routing and secure communication [26]. Along with cryptographic measures, it is mandatory to use trust management schemes also [7].

A. Concepts

*i) 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] [28]. Trust is the value based on the past behaviour of nodes [24]. When the trust value of nodes is known in the network, the nodes will take appropriate action against malicious nodes during operational decisions [29], [24]. 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

*i) Trust:*Trust is based on how the node would behave in the future [24].
*ii)Reputation:*Reputation is based on the performance of the node in the past [24].
*iii) Direct Interaction:*A value which is calculated by the node regarding its neighbours. It is also called as first-hand information [24], [8].
*iv)Indirect Interaction:*A calculated trust value provided by neighbouring node regarding its neighbouring nodes and it is also called as second-hand information [24], [8].
*v)Trust Value:*A value which is assigned between the ranges of 0-100. Values can also range from negative to positive [24].

IV. TRUST METHODOLOGIES

This section provides a brief description about various trust methodologies which uses mathematical measures and models related to trust and reputation in wireless sensor networks [5].

A. Bayesian Trust models

This trust model is used in [30] - [33]. It mainly consists of two directions: objective and subjective. In objective, trust analysis is based on the analysed data. In subjective, trust requires the level of confidence during decision making operation [5]. To calculate trust, model can take either continuous trust or binary trust or both [34]. This trust system mainly depends on the records of the relevant behaviours of other nodes so, it can utilize the prior probability of an event to update it with relevant behaviours of other nodes [5].

B. Subjective Logic Trust Model

This model is used for analysing trust network and a Bayesian network which is derived from dampster-shafer theory of evidence. It is used for obtaining subjective beliefs about the degree of uncertainty truth propositions [35]. To deal with uncertainty of truth and anomaly detection, Subjective Logic Anomaly Detection (SLAD) Framework is used. Based on the abnormal or anomalous data, SLAD also uses Extended Subjective Logic Based algorithm (ESLB) [36]. It deals with four tuple such as belief, disbelief, uncertainty and base rate [5].

C. Entropy trust model

Entropy trust model is mainly used in the field of thermodynamics. Trust evaluation in adhoc network makes use of Bayesian based trust propagation model and entropy based trust model [30]. Entropy trust model is considered to be compatible with Bayesian theory model [37]. Entropy mainly deals with how much uncertainty is present in a signal or random event [38], [40].

D. Fuzzy trust model

Fuzzy logic provides an approximate trust value rather than exact trust value. Fuzzylogic will be in the form of multi-valued logic which is derived from fuzzyset theory. Fuzzy logic integrates a series of IF-THEN rules to solve a problem in the system [5]. The important steps used in Fuzzy logic are as follows [39],

1. Initially, fuzzy sets and principles.
2. Initialize the input variables to the fuzzy engine.
3. Apply fuzzy rules to determine the output data.
4. Evaluate the results and finally return the feedbacks to balanced criteria.

E. Game theory trust model

[41] – [43] trust management systems use game theory to avoid the uncooperative nodes in the network. This model mathematically captures the behaviour of nodes based on the behaviour of other nodes. Game model uses two modes of operation to detect the behaviour of nodes: the deterministic mode and the random mode. In deterministic mode, the network is analysed. In random mode, a generic algorithm predicts the finest responses in every game [43]. Game theory is not a predictive tool to identify the behaviour of nodes rather it suggests how nodes need to behave [5]. Game theory performs a bidirectional behaviour in sensor network [5].

V. ANALYSIS OF DIFFERENT ROUTING SCHEMES RELATED TO CLUSTERED WSN

A. LEACH: Low Energy Adaptive Clustering Hierarchy

[1], [2], [10] LEACH is one of the cluster based protocol which minimizes energy dissipation in sensor networks. In LEACH, cluster heads are randomly selected from sensor nodes [1]. When communication takes place between sensor node and base station, energy is spread to all the sensor nodes in the network. The operation of LEACH deals with two important phases, set-up phase and steady phase [10]. During the set-up phase, a random number between 0 and 1 will be selected by sensor nodes [1]. The sensor node becomes cluster head, only if random number is less than the threshold T (n) [1]. T (n) is calculated as,

$$\mathrm{T\ (n)} = \begin{cases} \dfrac{\mathrm{P}}{1-\mathrm{P}[\mathrm{r}\ \mathrm{mod}\left(\frac{1}{\mathrm{P}}\right)]} \\ 0 \end{cases}$$

Condition apply, if n € G, otherwise 0. Where P is desired percentage to become a cluster head, r is the current round, G is set of nodes not being selected as a cluster head in the last 1/P rounds [1].

Once the cluster heads are selected, cluster head will advertise other sensor nodes that they are the new cluster head in the network [2]. When senor node receives the advertisement (ADV) message from cluster head, sensor node decides to which cluster they belong based on the signal strength of ADV message [10]. Once the cluster is being selected by sensor nodes, they will become the member of appropriate cluster head. Then using TDMA approach, cluster head will assign time on which sensor nodes can send data to the cluster heads [2], [10].

During the steady phase, sensor nodes starts sensing and transmitting data to the cluster heads [1]. Now cluster heads will aggregate the data received from the members of network before transmitting it to the base station [10], [1]. After certain amount of time spent in steady phase, the network enters the set up phase again to select another round of cluster heads [1].

B. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks

Directed diffusion is a data-centric routing protocol where sink node broadcasts the interest [1] [2]. The three main operation of directed diffusion is local determination of interest, data propagation and data aggregation. Directed diffusion consists of certain elements such as data interests, data messages, gradients and task descriptors [1], [11]. Task descriptors allows sink to send out the interest. Data descriptors are named by assigning attribute-value pairs which describes the sensing tasks. Each sensor node stores the entry of data interests in its cache [1]. The data interest entry consists of timestamp field and certain gradient fields [1], [2]. When the data interest is propagated throughout the network, the gradients are sent from source back to the sink [1]. If source has data for interest, it can send data along with the gradient interest path to the sink [11]. When sink starts receiving data from source, sink will make a new interest and strengthen the interest.

C. REAR: Reliable Energy Aware Routing

REAR is on demand, distributed and reactive routing protocol used purposely to provide reliable data or packet delivery transmission [12], [14]. The main operation of REAR is local node selection, path reservation, path request broadcasting delay. All the three operations are performed together to reduce retransmissions of data caused by unstable paths [12]. It requires limited energy and uses available memory resources of sensor nodes to perform the desired operations. It prior attempts to protect nodes against errors, rather finding a solution after the error takes place [12]. REAR makes use of three types of sensor nodes: Sink node, Intermediate node and target node [14]. The four important parts of REAR are: Service Discovery, Backup Path Discovery, Reliable Transmission and Reserved Energy Release. It establishes an energy efficient special path from source to destination and then distributes the traffic load uniformly in the network [14].

D. CHEF: Cluster Head Election mechanism using Fuzzy logic in Wireless Sensor Network

CHEF is a centralized clustering approach in which clustering decisions are made at base station [14]. The main objective of CHEF is to reduce the energy consumption and enhance the lifetime of the network [13]. In each round of clustering, base station will elect the cluster-head using three fuzzy descriptors: node concentration, node centrality and residual energy level. Each node of the cluster communicates with base station because base station is more powerful, have sufficient memory, storage and has the global knowledge about the network [14]. Base station will elect cluster-head based on 27 fuzzy if-then rules [14]. Thus, energy is utilized to transmit the location information of all the nodes to the base station [13].

TABLE I
Evaluation of Routing Protocols

Protocol	Routing Technique	Application
LEACH[1],[2], [10]	Cluster based hierarchical routing	Health Monitoring
Directed Diffusion [1] [2] [11]	Data centric flat routing protocol	Environmental Monitoring
REAR [12] [14]	On demand, distributed, reactive routing protocol	Mapping, Task Scheduling related to biological monitoring
CHEF [13] [14]	Centralized cluster routing protocol	HVAC

VI. TRUST TECHNIQUES

A. Based on Reputation Systems

SaurabhGaneriwal et al [15] 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,

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

Srinivasan et al [16] 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 [20] 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 [19] 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 [18] 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 [17] 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 [21] proposed a LDTS: A Lightweight andDependable 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 [22] 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,

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

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:

$$E_{N\,b} = E_{N \rightarrow b} + E_{b}$$

$E_{N\,b}$ is node's energy cost, the average energy cost of successfully delivered data packet is $E_{N \rightarrow b}$, 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 [23] 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.

VII. CONCLUSION AND FUTURE WORK

We conclude that there are different trust management schemes available and applicable to a variety of applications related to wireless sensor networks. Some approaches are applicable in static environment and some are in dynamic environment. Sensor networks has wide range of future applications so better trust management approaches can also be incorporated to provide enhanced security. Better trust management mechanism in clustered sensor networks need to be addressed in future to prevent the malicious nodes behaviour on the resource constrained sensor environment. They are many more different categories of trust methodologies related to wireless sensor networks where detailed study of those trust schemes can be addressed in future work.

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, TaiebZnati, "Wireless sensor networks: technology, protocols and *applications"*. First edition, 2012

[3] Edwin premkumar, BaskaranKaliapermal, 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] AashimaSingla, RatikaSachdeva, *"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] YanliYu,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, BabilKumari, "*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, IssacAgudo, Carmen Fernandez-Gago, "*Trust management systems for wireless sensor networks:Bestpractises-",* 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] Intanagonwiwat, R. Govindan, D. Estrin, "*Directed Diffusion: A scalable and Robust Communication Paradigm for sensor Networks,* Proc. Sixth Ann. *ACM/IEEE Int'l Conf. Mobile Computing and Networking (MOBICOM),* pp. 56-67, Aug. 2000.

[12] H. Hassanein, Jing Luo, "Reliable *Energy Aware Routing In Wireless Sensor Networks Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on* In Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop, pp. 54-64, April 2006

[13] Jong-Myoung, Kim, Seon-Ho Park, Young-Ju Han, Tai Myoung Chung "*CHEF: Cluster Head Election mechanism using Fuzzy logic in Wireless Sensor Networks*" Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference Vol**1**, pp. 654 – 659, 2008

[14] 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.

[15] 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.

[16] 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.

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

[18] 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

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

[20] 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.

[21] 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

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

[23] Christhu Raj M. R, Edwin Prem Kumar.G, KartheekKusampudi", 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.

[24] 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.

[25] SudipMisra, AnkurVaish, "Reputation based role assignment for role based access control in wireless sensor networks", Computer Communications, Vol 34, pp. 281-294, 2011

[26] 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

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

[28] 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.

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

[30] 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

[31] Nielsen M, Krukow K, Sassone V, "A Bayesian model for event-based trust", Electronic Notes on Theoretical Computer Science (ENTCS), Vol. 172, pp. 499-521, 2007

[32] Qi J-J, Li Z-Z, Wei L. A trust model based on Bayesian approach. Advances in Web Intelligence (AWIC), pp. 374-379, 2005.

[33] Quercia D, Hailes S, Capra L, B-trust: Bayesian trust framework for pervasive computing in: Trust management Proceedings of the fourth international conference, Trust 2006, Pisa, Italy, 2006

[34] Mohammad Momani, Subhash Challa, Rami Alhmouz, "Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks", Journal of Networks, Vol.5, No.7, 2010.

[35] Josang A, Hayward R, Pope S, "Trust network analysis with subjective logic. In: Proceedings of the Australian computer science conference (ACS'06), Horbat, pp. 139-161, 2006

[36] JinhuiYaun, Hongwei Zhou, Hong Chen, "SLAD: Subjective Logic Anomaly Detection Framework in wireless sensor networks", International Journal of Distributed Sensor Networks,pp. 1-21, 2011

[37] Caticha A, Giffin A, "Updating probabilities, In: The 26th International workshop on Bayesian inference and maximum entropy methods, Vol. 872, Paris, France, pp. 31-42, 2006

[38] Dai Hongjun, JiaZhiping, Dong Xiaona, "An Entropy-based Trust Modelling and Evaluation for Wireless Sensor Networks", in International Conference on Embedded Software and systems, ICESS2008, pp. 27-34, 2008.

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

[40] Hong Luo, Jiaming Tao, Yan Sun, "Entropy based trust management for data collection in wireless sensor networks", IEEE Wireless Communications networking and mobile computing, pp.1-4, 2009.

[41] 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.

[42] King-Casas B, Tomlin D, Anen C, Camerer CF, Quartz SR, Montague PR, Getting to know you: reputation and trust in a two person economic exchange. Science, 308(5718), pp. 78-83, 2005

[43] Komathyk K, Narayanasamy P, "Trust based evolutionary game model assisting AODV routing against selfishness", Journal of Network and computer application, vol.31, No.4, pp.446-71, 2008

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

[45] 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