iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Energy Preserving Reliable Trust Management Model for Wireless Sensor Networks

Mr. Kantamani Prasanna Kumar[1], Dr. Yamuna Devi C R[2]
[1] Department of Telecommunication Engineering, Dr. Ambedkar institute of Technology, Bangalore.
[2] Department of Telecommunication Engineering, Dr. Ambedkar institute of Technology, Bangalore.

***Abstract**: trust models offer defense process for wireless sensor networks. Research is being performed on trust models. Present research is being considered only for communication conduct for calculating belief values and it is not sufficient for evaluation of belief vales. An existing system is efficient distributed trust model (edtm) for wireless sensor networks. Direct trust and recommendation trust are calculated on the basis of received packets of the nodes in the network. To calculate direct, communication, energy and data trust are taken into consideration. Precision of recommendation trust is improved by defining trust efficiency and familiarity. In this paper, the newly proposed system is energy efficient cluster-tree (eect) for wireless sensor networks. Grouping of deployed nodes in the network into clusters, forming and electing a cluster head with large average residual energy compared to its neighboring nodes, received signal strength and threshold value. After electing a cluster, the cluster head is bridged to sink node through multi-hop interaction approach in inter cluster interactions. It improves the energy efficiency, throughput, packet delivery ratio and overhead factor.*

***Keywords**: EDTM, EECT, WSN, SN, CH*

I. INTRODUCTION

Wireless Sensor Networks are normally used to relay the information to central site, and also to regulate the physical conditions like temperature, pressure, sound, etc. They are bi-directional in nature. They regulate sensor activity. They are applicative in military purposes like battlefield vigilance. They also find applicative for industries and consumer purposes i.e., machine health regulation and monitoring of industrial and controlling process. WSN is constructed with the help of nodes. Every node in the network is linked to one or many sensors. Sensor node in a network has various parts such as an internal antenna connected to radio transceiver, a microcontroller, sensors interfaced with electronic circuit and a battery which acts as a energy source. The size of sensor node varies. And so does its cost.

A. Explication of Trust and its Properties

1)Trust: Many concepts are considered while defining trust. those are quality of services, availability, reliability, risk, utility and few other concepts. in simple words trust is nothing but a level of belief. trust is the belief that a sensor node has on other sensor node in the network for a purposeful operation. and that purposeful action depends on the previous behaviors. This trust value reflects how the sensor node acts and behaves. Whether it behaves normally or not. The range of trust value is from 0 to 1. Here value 1 indicates completely trustworthy and value 0 indicates the opposite [2].

2) Direct trust: Considering direct communication behaviors direct trust value is calculated. Relationship of two neighboring/ nearby nodes is reflected using this direct trust value.

3) Recommendation trust- filtered reliable recommendations are considered for calculation of recommendation trust. So a proper effective mechanism is chosen to filter out recommendation information. Since it is known that recommendations from the third parties are not always secure.

4) Indirect trust: Indirect trust comes into picture when subject node cannot communicate directly with object node. That is when indirect trust has to be established. Gain of indirect trust value depends upon recommendation from others nodes in the network.

The properties of trust are as follows: 1) Asymmetry means that node A believes node B that doesn't mean node B believes node A. 2) Transitivity indicates the belief level passed along the node length. If node A believes node B & node B believes node C, this indicates that node A believes node C to some extent. This transitivity property is used for calculating trust values between two non-neighbor nodes. 3) Composability indicates Integrated trust value obtained using composability property is sum total of trust values from different multiple paths [3].

Sensors are distributed spatially to monitor parameters such as sound, pressure, temperature, etc. These sensors collect the data through the network and pass to a destination. One crucial aspect that needs to be remembered is the security. Purpose of security in

WSNs is to protect the data and network connections of the sensor nodes. There are certain requirements for data security. And they are confidentiality, integrity and substantiate. Protection of accessing to communication channel is needed by considering of the network. Protection against malevolent resource consumption, node capturing, denial of service attacks and node injection is needed. Guarding against the malicious nodes is required by the applications of secure routing.

II. LITERATURE SURVEY

Development of trust models has been growing trend among researchers. The first proposed trust model is Reputation based framework. Watchdog and prominence system are the two very important building blocks of RFSN system. Monitoring of communication behaviors is the responsibility of watchdog. Preserving the popularity of the node is the responsibility of prominence system. Considering prominence value system calculates the trust value. Considering only direct trust and ignoring recommendation trust is drawback of the reputation based framework system.

The next presented trust model system is the PLUS model. The management scheme is based on parameterized & localized trust. It is mainly focused on solving network security issues by taking the help of trust management mechanism. To make security stronger, uncomplicated and highly efficient deriving of trustworthiness is required statistically. Important features of PLUS are as follows:

Parameter database is maintained to describe operational environment, status of the network, types of applications and local information of the nodes.

Providing common general resources to other components by constructing of a shared library.

Four of the designed logical components are network I/O, trust estimator, routing operator and security responser. Network input/output is dealt with traffic in the network. Packet handles are provided by the routing operator. Trustiness of the nodes are estimated using Trust estimator and security responser from point of security perspectives.

Recommendations & references are used to establish trust relationship between nodes in PLUS [6]. The judge nodes received packet from suspect node needs to undergo the integrity check of the packet. The suspect nodes trust value gets reduced if there is a fail in integrity check. No matter whether the suspect node is indulged in malignant behavior or not. This results in suspect node getting biased penalty.

The researchers came up with another trust model called as Node Behavioral strategies banding belief theory of the trust evaluation algorithm (NBBTE) [6]. This algorithm is explained on the basis of the theory called behavior arrangement banding D-S trust theory. Establishing of different trust factors based on communication behaviors among sensor nodes is done with the help of NBBTE algorithm. Measuring of direct trust values of nodes is possible by incorporating fuzzy set logic.

Obtaining integrated trust value by adopting method called D-S evidence theory on considering of recommendation from neighbor nodes. Thus this NBBTE algorithm establishes different trust factors based on communication behaviors and assess in the trustworthiness among sensor nodes. And then another trust model was proposed known as EDTM i.e., an efficient distributed trust model. This trust model assess faithful relationship among nodes accurately and effectively and also prevents the security disputes. And EDTM is chosen as a comparing algorithm.

III.PROPOSED SYSTEM

The newly presented system is energy efficient cluster tree for Wireless Sensor Networks. The main objective of cluster tree is to bring down the energy consumption, delay and ameliorate the potential of Wireless Sensor Networks. Grouping of nodes into clusters and electing a cluster head considering remaining energy parameter when compared to nearby nodes, received signal intensity & threshold value. Further the cluster head is bridged to a sink using multihop interaction methods incorporating inter cluster communication. Parameters such as energy efficiency, throughput, packet conveyance proportion and over head variable.

To find cluster head (CH), the residual energy & distance parameter are taken into consideration. Distance between cluster head & sink is indicated by the distance parameter. While cluster formation, cluster members receive advertisement (ADV) message from their corresponding cluster head. This indicates the members joining with corresponding cluster heads. This kind of interactions between cluster head & cluster members are called intra cluster communication.

In this way , the information is aggregated by cluster head from its cluster members. Interaction between cluster heads will occur for the information to reach destination. Now do load all the cluster heads into routing table and data gets generated at the source. Once the data gets generated, source cluster head checks for the nearest cluster head, if the cluster head is involved in interaction, it choses some other cluster head & relays the information to its particular cluster head. Cluster head sends acknowledgement (ACK) packet to previous cluster head (CH). This kind of interaction between cluster heads of different clusters and sink is called inter cluster communication. Later, the complete cluster head is bridged to sink using direct hop or through multi hop interaction methods in

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

inter cluster communications.

Fig 1 shows intra cluster interaction & inter cluster interaction. Thus the information reaches the destination, once information reaches sink, its gives ACK packet to previous transmitted CH.

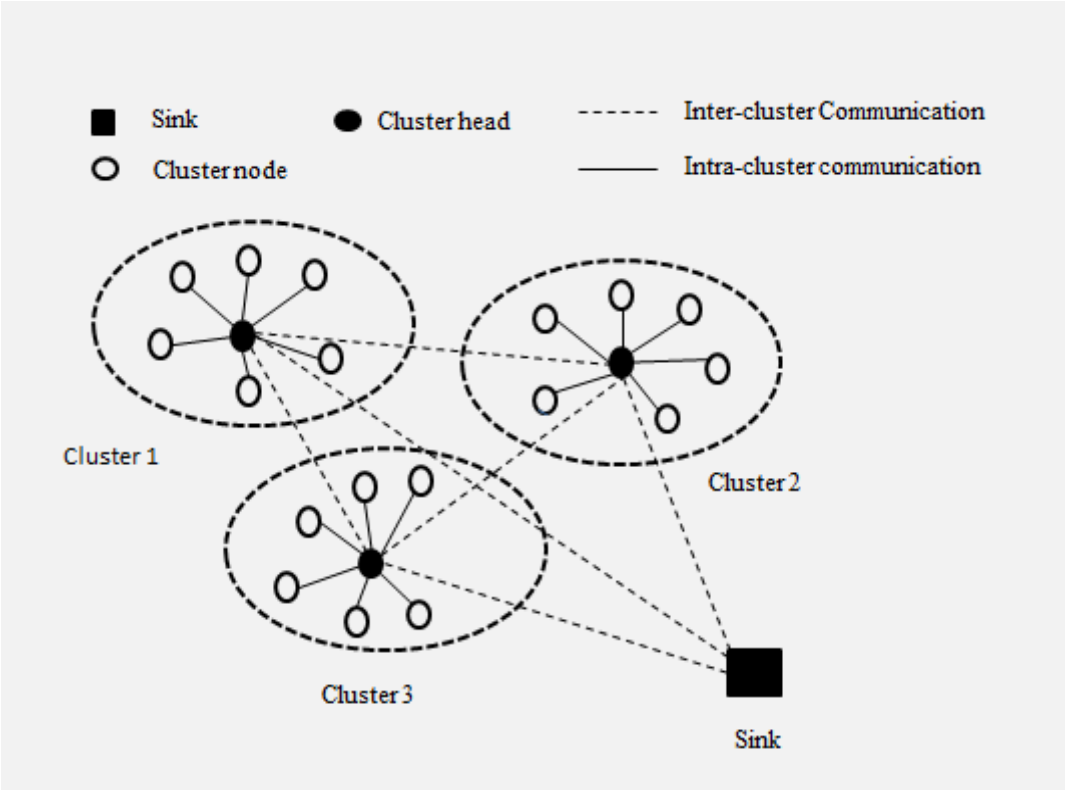


Fig. 1: Inter-cluster interaction & intra-cluster interaction.

In the current years, the fast innovative advances in miniaturized scale electro-mechanical systems, less power and very coordinated computerized hardware, littles scale energy streams, small chip & less power, minimal effort & many functional Wireless Sensor Networks, capable of monitoring physical parameters of environment. R=The sensor is battery driven having low capacity, modest micro-chip, radio handset, arrangement of transducers used to obtain information and monitor the surroundings. The rise of minimal effort, little sized wireless devices has persuaded escalated examine in almost recent times tending to the ability of coordinated effort of sensors in data aggregation, which prompted the development of Wireless Sensor Networks.

IV. TRUST COMPUTATION

A. Computation of Direct Trust

Computation of direct trust requires many other different trusts to be taken into consideration. Other trusts such as communication trust i.e., trust calculated based on the communication behaviors, information trust i.e., belief level of the data that is being communicated and energy trust. To accomplish the tasks the sensor components of wireless sensor networks normally liaise and communicate to its neighboring nodes. The interaction demeanor with the neighboring nodes are examined to asses sensor node's performance. There is loss in communication units called packets. There is also unstable communications in sensor nodes. The major reason behind this loss is due to the behavior of wireless channels through which communication is happening.

1) *Computation of Communication trust:* The preliminary conduct of data on the senor node is the most vital facet of communication trust. As the communication channel betwixt sensor nodes is unreliable, insecure and boisterous, therefore examining the node's behavior in Wireless Sensor Networks based on precursory behavior of communication channel include large amount of uncertainty. A Subjective framework is adopted to mitigate the uncertainty, trust value in Sequential Logic framework is a triad with T = {b, d, u}, here b corresponds to belief, d corresponds to disbelief, u corresponds to uncertainty in the channel and b, d, u $\in$ [0, 1], b +d +u = 1. The communication trust T_{com} evaluated on the basis of successful (s) and

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

unsuccessful (f) interaction data components:

$$T_{com} = \frac{2b+u}{2} \quad (1)$$

Where, $b = \frac{s}{s+f+1}$, $u = \frac{1}{s+f+1}$

2) Computation of energy trust: The vitality of a senor node in Wireless Sensor Network is a vital parameter because the sensor components called nodes are fixated in quantity of energy that are possessed. Example, the malignant nodes has large amount of energy consumption than the normal sensor components, while the nodes which are not involved in any communication has less energy consumption.

Defining of parameter called energy threshold is important and is denoted by θ. The sensor node's remaining energy denoted by E_{res} is lower than defined threshold parameter. Because of which sensor nodes are incapable of performing its intended tasks due to insufficient energy. That is why vitality trust of node is considered as 0. Or else, the evaluation of vitality is dependent upon consumption of vitality by the node p_{ene}, $p_{ene} \in$ [0,1]. If the rate of consumption of energy is large is, then lesser unconsumed energy will be remaining, that eventually leads to lesser potential of nodes to accomplish the tasks intended. Therefore, the trust values for the sensor nodes should be considerably smaller. Computation of energy trust is done as follows:

$$T_{ene} = \{1 - p_{ene}, \text{if } E_{res} \geq \theta, 0 \text{ else.} \quad (2)$$

Where, p_{ene} is computed based on Ray Projection method.

3) Computation of Data Trust: The data trust of data on the sensor node has an affect on the trust of communication nodes that generated and misrepresented data, and contrariwise. The information packet has spatial correlation, i.e. the information containing packets transmitted amid neighboring nodes are inevitably alike in all of the same regions. Normal distribution is followed by the rate of data packets. Modeling of the information as the normal distribution simplifies sensor network. For some data set, the PDF i.e., probability density function is given by:

$$f(x) = (1/\sigma\sqrt{2\pi})\, e^{-(x-\mu)^2/2\sigma^2} \quad (3)$$

here x is the characteristic value v_d of information object, μ is mean of data and σ is variance of data. Because mean μ of data set is representative value which reflects similarity of value to a data object, the mean value is required to be the exorbitant value of trust [18]. If information rate is nearer to the mean, then the belief value for this data set is comparatively large, and the contrariwise. The elucidation of information trust rate is as described:

$$T_{data} = 2(0.5 - \int_{\mu}^{v_d} f(x)\, dx = 2\int_{v_d}^{\infty} f(x)\, dx \quad (4)$$

Considering the interaction trust T_{com}, the vitality trust T_{ene} and the information trust T_{data}, the trust between neighboring nodes can be obtained as follows:

$$T_{n-direct} = w_{com} T_{com} + w_{ene} T_{ene} + w_{data} T_{data} \quad (5)$$

where w_{com} is weight of communication trust, w_{ene} is energy trust's weight value w_{data} is information trust's weighted value , $w_{com} \in$ [0, 1], $w_{ene} \in$ [0, 1], $w_{data} \in$ [0, 1] and $w_{com} + w_{ene} + w_{data} = 1$.

B. Computing Recommendation Trust

Recommended trust is a kind of direct trust. But there is no any direct interaction between source node and destination node; recommender's recommendations are utilized for calculating trust. In previous works done, the true & false recommendations are usually not renowned. The detection of false recommendation is vital because it has greater influence on calculation of trust.

In fig 4.1, destination node B sends recommendations to source node A, source node A examines record of belief values & choses a pair of neighboring nodes source node A & destination node B are considered as recommenders which are having trust values greater than calculated threshold 0.5.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

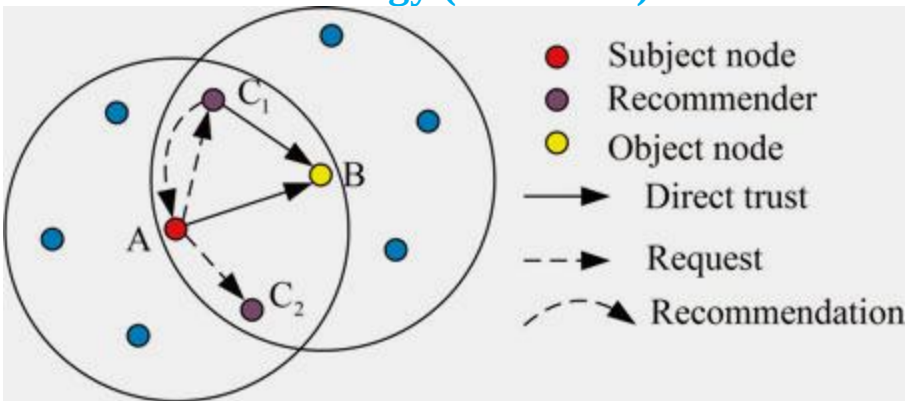


Fig. 2: Computation of recommendation belief.

1) *Computation of Recommendation Reliability:* Consider an elementary checking technique amid numerous recommendations by describing recommendation reliability T_{rel}. T_{rel} Which is computed as follows:

$$T_{rel}=1-\left|T_{C_i}^{B}-T_{ave}^{B}\right| \quad (6)$$

Where, $T_{C_i}^{B}$- Suggested value of destination B accounted through recommender C_i

T_{ave}^{B} – Average of all suggestions.

2) *Computation of Suggestion similarity:* The recommendation is most vital if the trust value from the recommender is higher. However, a question may arise that whether honest recommendations are provided only by the nodes with larger trust value. A notion of relationship awareness or familiarity is introduced, based on age of relationship amid two sensor nodes. This notion enables the nodes to permit importance to recommendations relayed from long-term neighboring sensor nodes than short-term neighboring sensor nodes. Familiarity amid the nodes is described as:

$$T_{fam}=\frac{num_{C_i}^{B}}{num_{C_i}}*\alpha^{\frac{1}{num_{C_i}^{B}}} \quad (7)$$

Where, $num_{C_i}^{B}$- Successful communication times amid recommender C_i and destination node B.

num_{C_i}- Overall successful communication times of the recommender.

α - Regulatory factor and $\alpha \in (0,1)$.

Recommendation trust is computed by:

$$T_{n-recom}=\frac{\sum_{i=1}^{n}0.5+\left(T_{C_i}^{B}-0.5\right)*T_{rel}*T_{fam}}{n} \quad (8)$$

n- Number of recommenders.

C. Computation of Indirect Trust

In Fig. 4.2, based on details about the sensor node placement, three ways of implementations can be perceived for selecting recommenders:

1) Locating recommender nearer to destination node to limit consumption of energy.
2) Locating recommender having high trust value which guarantees efficiency and capability of the Trust chain.
3) Locating a Trust chain by taking into account the information about distance and also trust value.

The first step helps in finding the smallest Trust chain, so that the communication overhear is minimized. But the indirect trust computation is inaccurate due to the presence of malignant nodes. The second step elects the believable chain of trust but it is energy inefficient. The third step is the most suitable and best step for selecting recommenders.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

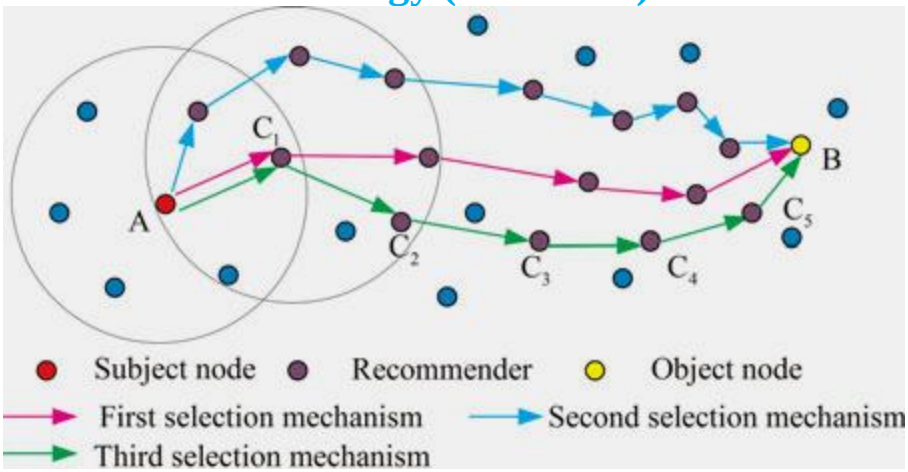


Fig. 3: Computation of indirect belief.

After establishment of Belief chain, the recommenders must indulge in trust propagation process. The source A initially relays suggestion request to its very next recommender & awaits a reply from the recommender. When the recommender receives request message from the source A, it check if it has the data that is required by the source A & checks if destination is its neighboring. If destination B is not the neighbor of the recommender, it continuously relays the information to its next node; else replies request message along with a recommendation value. Through the recommendation value denoted by $T_{C_i}^{B}$ and the belief value of the recommender is denoted by T_{C_i} , indirect belief value is computed by:

$$T_{n-indirect}\left(\begin{matrix}B\\C_1\end{matrix}\right) = \begin{cases} T_{C_1} * T_{C_1}^{B}, & \text{if } T_{C_1}^{B} < 0.5 \\ 0.5 + \left(T_{C_1} - 0.5\right) * T_{C_1}^{B}, & \text{else} \end{cases} \quad (9)$$

$$T_{n-indirect}\left(\begin{matrix}B\\C_{i+1}\end{matrix}\right) = \begin{cases} T_{C_{i+1}} * T_{n-indirect}\left(\begin{matrix}B\\C_1\end{matrix}\right), & \text{if } T_{n-indirect}\left(\begin{matrix}B\\C_1\end{matrix}\right) < 0.5 \\ 0.5 + \left(T_{C_{i+1}} - 0.5\right) * T_{n-indirect}\left(\begin{matrix}B\\C_1\end{matrix}\right), & \text{else} \end{cases} \quad (10)$$

i = 1, . . . , n,

D. Update of Belief Value

Because of dynamic conduct of Wireless Sensor Networks like attaching or detaching from the communication network, trust values must be regularly upgraded. Initially the values must not be upgraded very often, because it leads to wastage of energy and evaluation will be afflicted through different conditions of traffic like data congestion and the delay in the network. To evaluate a node's trustworthiness, past calculated trust values must be available. If cycle time is very large, the current conduct of destination node will not be efficient. To mitigate the problems faced, a sliding window time concept is utilized to upgrade trust values.

The sliding time window contains many time slots for upgrading the thrust value. Every time period is a time series. In every time series, the source assess the belief of destination node denoted as T (i), where i = 1, . . .,m, here m is total time period. In the subsequent iteration, the calculated value is upgraded to $T(i+1)_{new} = w_i\, T(i) + w_{i+1}\, T(i+1)$, i = 1,….,m, $w_i + w_{i+1} = 1. w_i \; and \; w_{i+1}$ are values of weight of previously calculated trust values and the prevailing trust value. The trust value calculated recently must be given more importance than the previously calculated values. An aging aspect or factor β is defined to compute attenuation of trust value: $= e^{t_i - t_{i+1}}$, , where t_i- Trust computational time of T (i), and t_{i+1}- Trust computational time of T(i+1). The weight value is given by $w_i = \beta,\ w_{i+1} = 1 - \beta$.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. SIMULATION RESULTS & ANALYSIS

Experiments are performed using network simulator 2(version 2.35). Implemented two different set of simulations. One for EDTM and the other one for EECT. Evaluation of performance of EDTM and EECT is done based on different simulation parameters. Then comparison of results of existing system and proposed system is done and is as shown as follows:

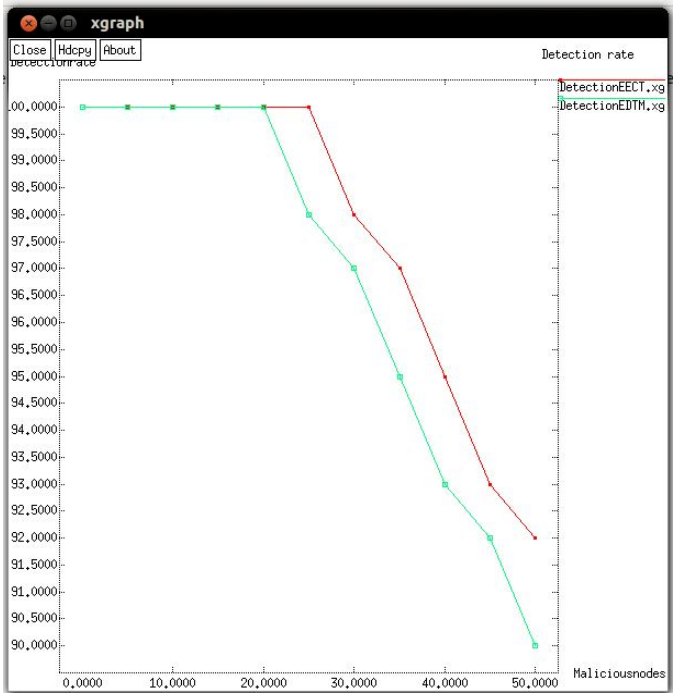


Fig. 4: Comparison of the Detection rate.

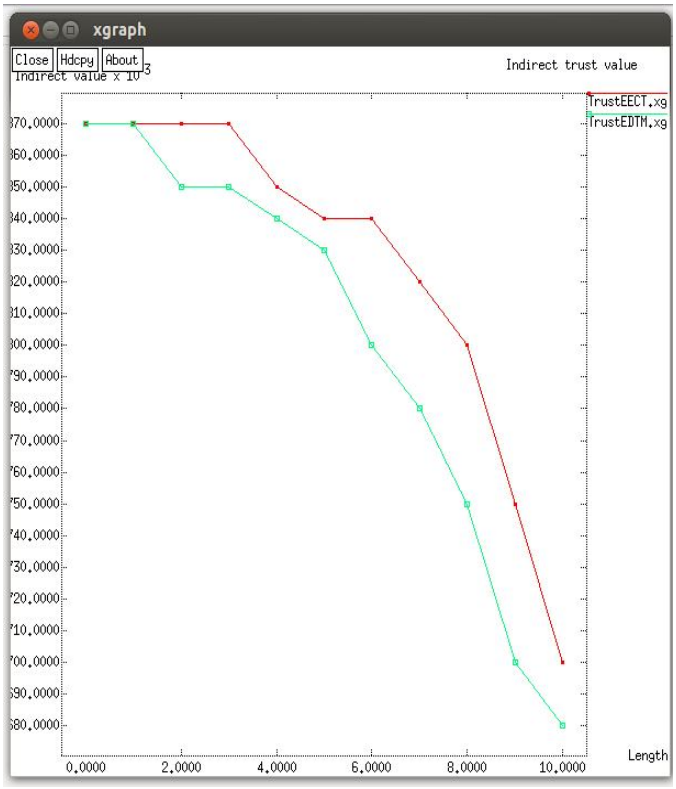


Fig. 5: Comparison of Indirect trust value.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

EECT outperforms EDTM in terms of indirect trust value calculation.

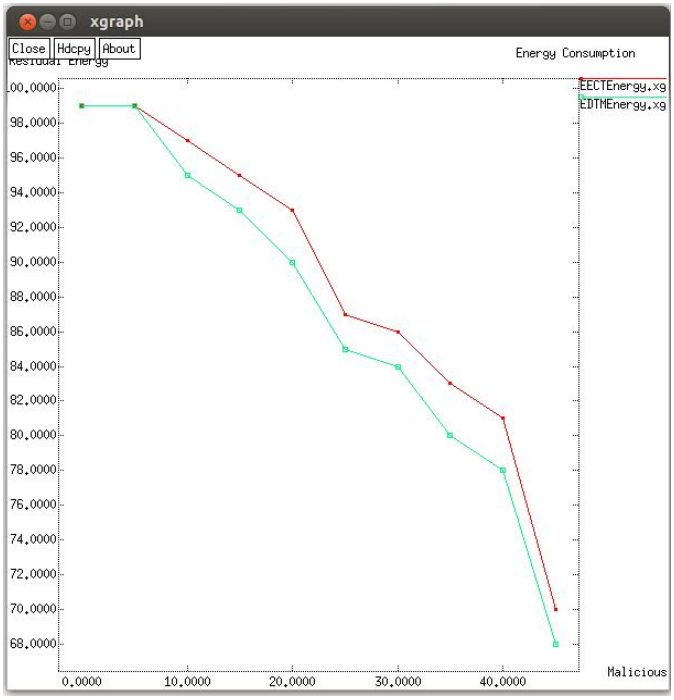


Fig. 6: Comparison of the energy consumption.

EECT is much more energy efficient then EDTM, because in EDTM all the nodes are participating in the transmission of data to the destination. Whereas in case of EECT only nodes with high average residual energy are involved in transmission.

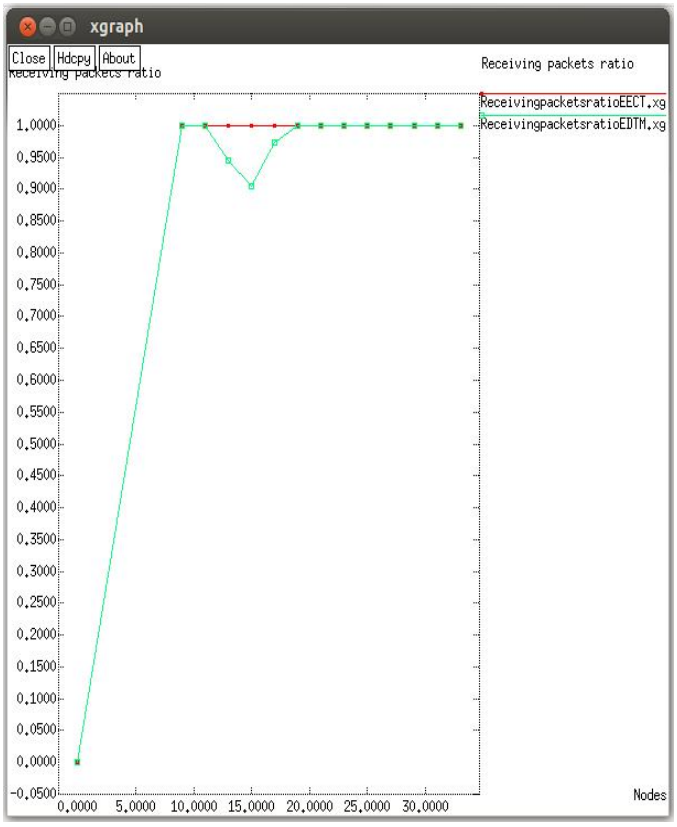


Fig. 7: Receiving packet ratio versus Number of nodes.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

EECT is able to achieve better performance than EDTM in terms of receiving packet ratio. EECT reduces packet overhead of cluster head.

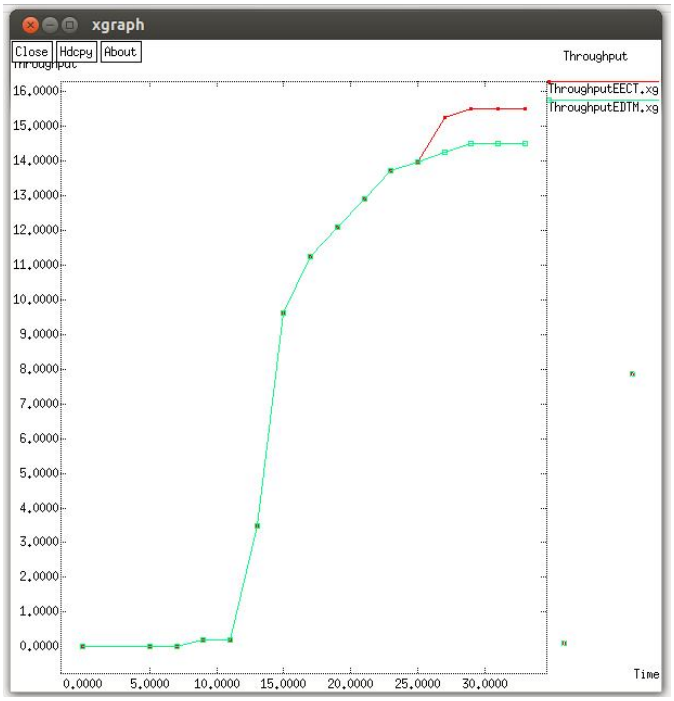


Fig 8: Throughput versus Number of nodes.

EECT algorithm is able to achieve better throughput than existing system. The total number of nodes in each cluster is also maintained in every round.

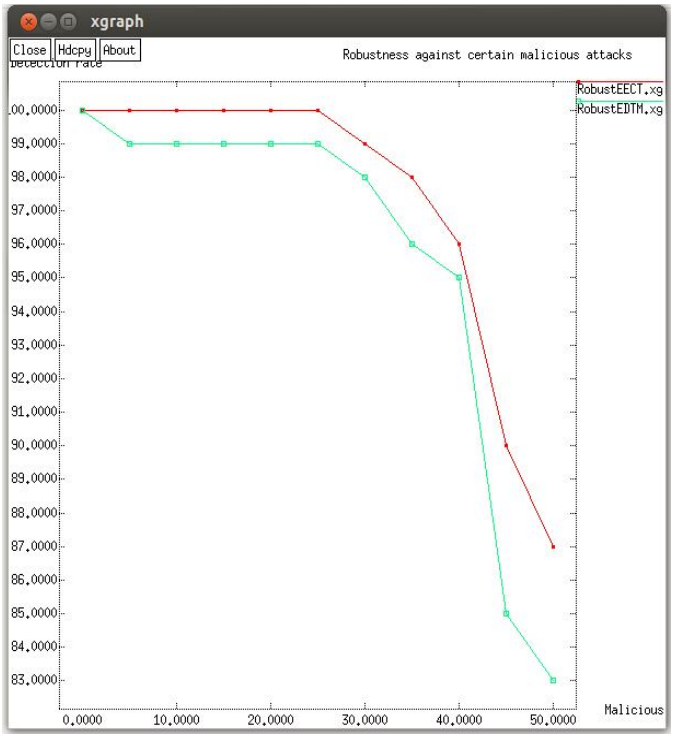


Fig 9: Comparison of robustness against certain Malicious attacks.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Both EECT and EDTM are robust against malicious attacks but EECT works better.

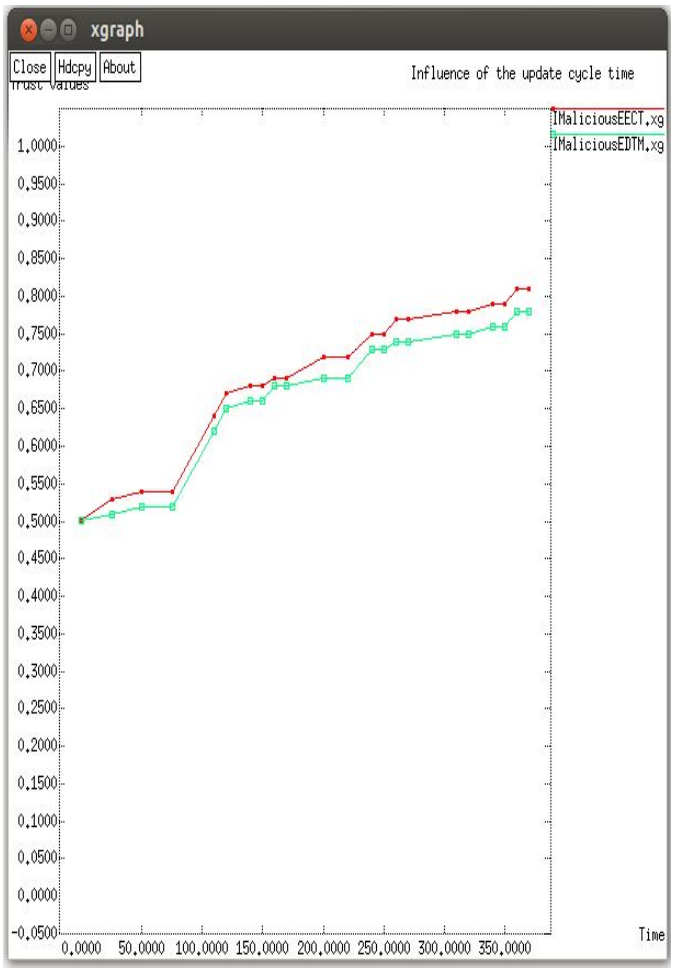


Fig. 10: Influence of update cycle time.

In order to save energy consumption, a longer update time period can be used for trust evaluation. But shorter update time periods should be used for appropriate trust values calculated with malicious nodes.

VI. CONCLUSIONS

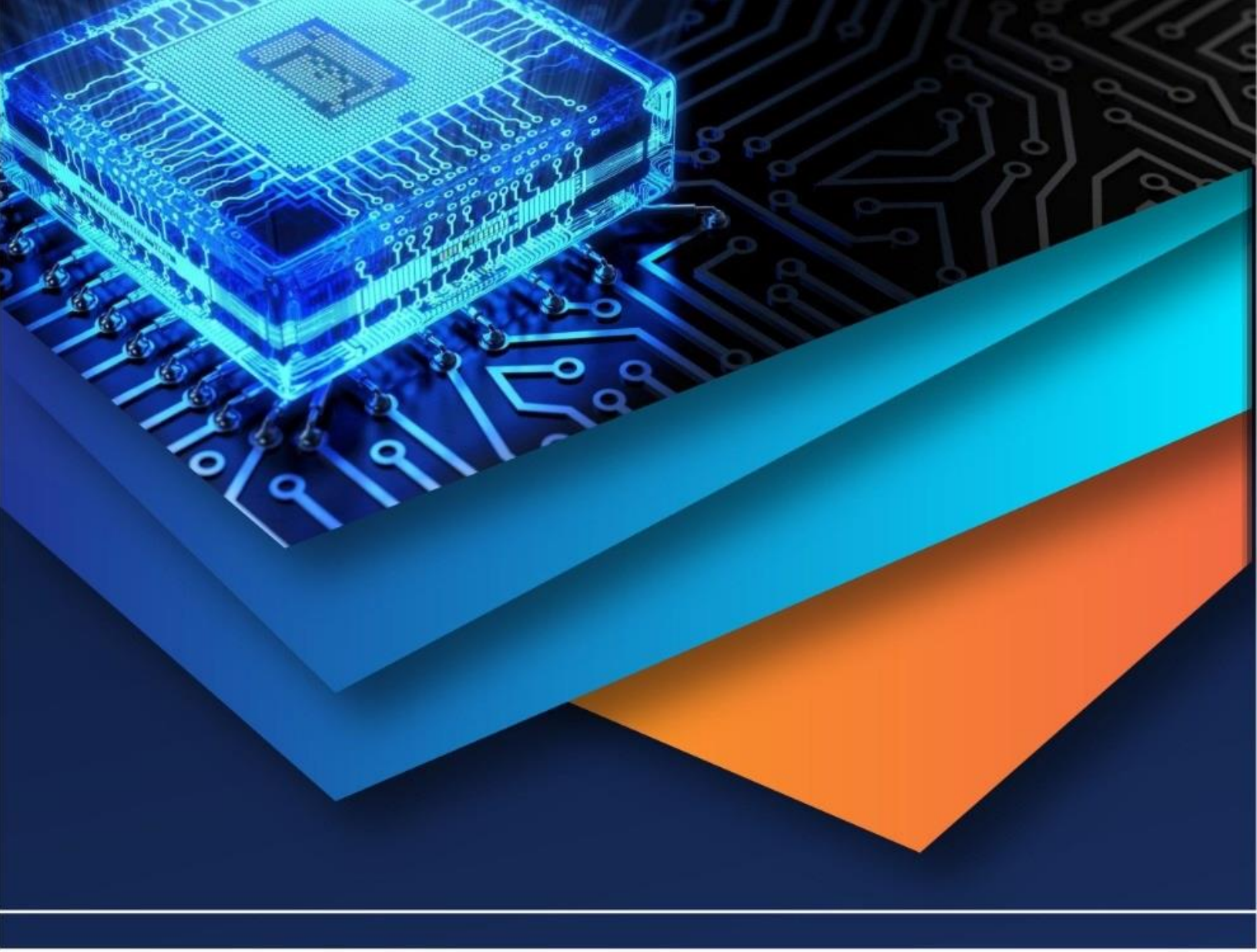
The trust model has become important for malignant nodes prediction in WSNs. It can assist in many applications such as protective routing, protective information collection, and trusted key interchange. In this paper, an existing system is an efficient distributed trust model (EDTM),in which the calculation of direct trust, recommendation trust and indirect trust are discussed. And a newly proposed system is energy efficient cluster tree (EECT). Evaluation of performance of EDTM and EECT is done based on different simulation parameters. Then comparison of results of existing system and proposed system is done.

REFERENCES

[1] H. Chan and A Perrig, “Security and privacy in sensor networks,” Comput., vol. 36, no. 10, pp. 103–105, Oct. 2003.
[2] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, “Pervasive, secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 7, pp. 400– 411, May 2009.
[3] V. C. Gungor, L. Bin, and G. P. Hancke, “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
[4] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, “Managements and applications of trust in wireless sensor networks: A Survey,” J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.
[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation based framework for high integrity sensor networks,” in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 66–77.
[6] Z. Yao, D. Kim, and Y. Doh, “PLUS: Parameterized and localized trust management scheme for sensor networks security,” in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., 2008, pp. 437–446.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

[7] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory," Sensors, vol. 11, pp. 1345–1360, 2011.
[8] G. Han, Y. Dong, H. Guo, L. Shu, and D. Wu, "Cross-layer optimized routing in WSN with duty-cycle and energy harvesting," Wireless Commun. Mobile Comput., 3 Feb. 2014, DOI: 10.1002/ wcm.2468.
[9] G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti, "The insights of localization through mobile anchor nodes in wireless sensor networks with irregular radio," KSII Trans. Internet Inf. Syst., vol. 6, pp. 2992–3007, 2012.
[10] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279–298, 2nd Quarter 2012.
[11] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and distrust values," IEEE Commun. Surveys Tuts., vol. 321, pp. 157– 171, 2010.
[12] A. Josang, "An algebra for assessing trust in certification chains," in Proc. Netw. Distrib. Syst. Security Symp., 1999, pp. 1–10.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY