# AN EFFICIENT TRUST BASED SECURED DATA AGGREGATION TECHNIQUE IN WSN

Anita Daniel D.
Research Scholar, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu
d.anitaedwin@yahoo.com

Emalda Roslin S.
Professor, Department of ECE, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu
roemi_mich@yahoo.co.in

**Abstract - The security of Wireless Sensor Network (WSN) in its applications face great challenges while satisfying energy constraints in green computing. WSN have different kinds of constraints such as lack of infrastructure, limited memory, low computation capability and reduced battery life, by those, security implied as supplemental demanding job. Since, there is much difference in reading values of sensor node and failure in nodes; it is difficult for accurate data extraction and aggregation in WSN. The principal purpose of data aggregation (DA) is to collect data in an energy efficient manner by which the network existence will be increased. This model investigates security linked issues, challenges and requirements in WSN. And also, a trust based framework for predicting the effectiveness of secured DA in WSN is presented. In this technique, a Trust rating function is developed to find the trust rating value of each sensor nodes and then form data aggregation tree (DAT) based on modified Cuckoo search algorithm (CSA). The sensor nodes with higher trust rating are selected as aggregators. Each sensor node encrypts data using watermarking techniques. Encrypted data is aggregated and transmitted to sink by aggregator. The simulation outcome depict that the intended model have superior than the existing one.**

***Keywords*:** Trust rating function, Base station, Data aggregation, Security in Wireless Sensor Networks

## 1. Introduction

The ongoing research in WSNs are based on security challenges because WSNs are exposed to varied attacks comprising of node compromising (capturing and reprogramming), jamming, passive eavesdropping, and inclusion of malicious nodes into the network [1]. Each sensor nodes (SN) are competent to environment sensing, local data processing and forwarding data to Cluster Heads (CH) and they turn into the Base Station (BS) in a WSN [2]. Transmitting data in an efficient manner is the major concern in WSNs. Since, there are restrictions in resources availability, data transmission must be minimized. By this way, the lifetime of the network and utilization of bandwidth will be increased [3]. The process of gathering information from different ways thereby minimizing the transmission count by redundancy will happen in the Cluster Head. By these, conservation of energy takes place in the system [4]. Cluster-based data transmission in WSNs extends the lifetime of the node and reduction in utilization of bandwidth with the help of local cooperation within sensor nodes [5]. In a cluster-based protocol, each cluster will have a head, called as CH. The leaf nodes collect the data and forward the aggregation result to the base station. The LEACH protocol [6] is an effective algorithm in which the consumption of the total energy will be minimal for Cluster based WSN. In order to defend the quick consumption of energy in the set of CHs, LEACH Protocol indiscriminately revolves CHs within the SNs in circular way, based on their energy [7]. LEACH shows advancements in its lifetime of the network. In LEACH protocols, the challenging issue is the security, due to its common key distributions. Like LEACH protocols, few more secure data transmission protocols are available but they apply symmetric key management for security. Symmetric Key Cryptography creates issues, while the pair wise key had not shared with other nodes in their predefined key structure [8].

GAB model [9] has presented with the focus of securing data and reducing the cost of energy when the exchanges of data done in WSN. This method is based on public-key cryptography. Here key management plays a major role. An efficient ECIPAP protocol [10] depends upon the homomorphic encryption algorithm is proposed with mechanism of checking the result instead of using secret sharing. Hence it requires more power even it provides confidentiality and integrity. Genetic Algorithm (GA) [2] depends on the genetic activity done by biological life form that help to solve problems while searching and optimization process. This model reduces overheads in transmission, consumption of energy and security assurance, but it depends on node connectivity. SET-IBS and SET-IBOOS methods [5] proposed mainly for security but SET-IBS depends on the Diffie-Hellman issue in the pairing domain and SET-IBOOS depends on the hardness state in the discrete

logarithm issue. SELADG model for WSN [11] method involves lesser overhead than that of the prevailing EEHA method. In ESCS (Energy-Aware Security Level Control Scheme) method [12], based on their energy nodes and are segregated as ES-mode and ER-mode; then for transmission it uses both symmetric-key and public-key method. LFTM based DA and transmission protocol for WSN [13] method depends on trust and reputation model for security assurance and accuracy in DA. These schemes suffer with node compromising attack but it provides more security with less energy consumption when compared with previous schemes. To achieve more security with extended network lifetime and to avoid attacks present in the network, it necessitates using asymmetric encryption technique with low memory usage and low communication overhead in the data aggregation process in WSN. Hence it necessitates the development of an efficient data transmission technique with high security in WSN.

This paper is organized in the following manner. Section 2 narrates the related works. Section 3 outlines the model of the system as the proposed work; Section 4 depicts the simulation results and Section 5 infers the paper by foreground width of our work.

## 2. Related Works

M. Mareli et al [14] developed three new CSAs depending upon switching increasing variables dynamically such as linear, exponential and power. The three new CSAs are checked for their accuracy on ten test functions which are based on mathematical calculations and the outputs are measured with persistent and dynamically decreasing linear frameworks. The CSEI method uses exponentially increasing switching parameter are identified as more effective than other CSAs.

Govind P. Gupta [15] proposed ICSCA method based on improved CSA for cluster formation. In this work, an improved CSA based meta-heuristic method used for the formation of energy balanced clustering and CHs selection is done by using the fitness function. Selection of energy efficient path from CH and BS will done using multi-hop routing algorithm, since, we need to move the aggregated data from CHs to the sink. This method performs much better compared to the other schemes based on CSAs with regard to complete usage of energy, network life time and residual energy.

Shirin Tahmasebi et al [16] developed Placement of Controllers based Cuckoo-PC technique in order to get a best solution in a minimal period. Therefore, the major concern to perform Cuckoo-PC apart from ILP method which is nothing but integer based linear programming that achieves results almost similar same like ILP and thus, it is clearly evident that Cuckoo-PC has highly measurable and it will be ideal for extensive networks.

Jing Cheng et al [17] presented a modified CSA for achieving most effective method of localizing nodes in the network. This model follows the alteration in step size to activate the population proceed towards the comprehensive solution rapidly, and the competence of the result is deployed to build mutation probability to keep away from local convergence. Besides to put a stop to the consumption of energy occurred by an insignificant search, this technique limits the population in the defined area.

Md. Akhtaruzzaman Adnan et al [18] developed an energy-aware hierarchical clustering algorithm based on CSA. Calculating the longer distant member nodes, which is taken as cost function and it is correlated to CH, and CH selection algorithm is done by the residual power of CH. This proposed framework provides superior life time in the network by generating better cluster formation and competent of providing more data to the base station with respect to existing clustering based approaches.

Mohammed DEMRI et al [19] carried out an enhanced routing methodology for energy-aware clustering protocol with CSA. A novel fitness function is used for multi-objective CHs selection, taken into account, the standard measurement namely distance and energy. It is evident from the output gained that the proposed framework works well than that of LEACH when compared to throughput, lifetime, stability time interval and number of dead nodes in the network.

Djallel Eddine Boubiche et al [20] developed a method for secure DA in WSN using watermarking based mechanisms. The mechanism offers a distributed verification called hop by hop for data integrity verification and authentication. The theoretical outputs had illustrated that SDAW can secure data aggregation in an energy efficient manner than Secure DAV mechanism, and the communication overhead gets averted by the communication links.

Djallel Eddine Boubiche et al [21] proposed a technique called watermarking based on a cross-layer framework and a dynamic embedding arrangement for providing more security. This CLWDA method considers the resource restrictions of the homogenous sensor node (SN) and effectiveness of the DA procedure on the heterogeneous aggregation nodes. It consumes reasonable memory space, reduced computation delay and increased aggregation accuracy when compared with CDAP protocol.

Arwa Alromih et al [22] developed a RWFS method based on Randomized Watermarking and Filtering Scheme that come up with filtering to take away any infused data at an initial phase of the transmission. Watermark is used in filtering, and that is generated from the authentic data and in randomly, directly embedded throughout the packet's payload. The results demonstrates the energy consumption of the system and the security enhanced as it alleviates the certain curbs in the present approaches.

Dr. Jamal Mohammed Kadhim et al [23] specifies a method to take care of data integrity and node authentication in WSNs when compared with previous methods by using the lightweight messages. The outcomes are measured in terms of WAR and WDR parameters.

Swathi.Y et al [25] proposed DA process in WSN by using fuzzy logic scheme is EAFSDA. The security is furnished using homomorphic data encryption and it gives a total solution for protected and effective DA, and that exhibits improvement in the discharged results in distinct with existing methods.

Zhengwang Ye et al [26] developed DTEM method for WSN. Trust is calculated by using dynamic weights. After merging the direct trust and indirect trust, an update mechanism takes place using a sliding window to increase flexibility. It carries out better in protecting from multiple malicious attacks.

## 3. Proposed Work

The design for the proposed TWDA method consists of three sections to have an energy efficient data transmission technique with high security WSN. Section I describes about Cluster formation. The steps followed in this section are the calculation of Trust rating value and selection of CH and Section II describes about the formation of clusters using modified CSA. Section III describes about secure DA using watermarking mechanism.

### 3.1. *Trust based Cluster Head Selection*

We select a CH [27] using a modified cuckoo search algorithm by considering the parameters like packet forwarding ratio [28,29], delay [30,31] and buffer overflow [33-36] to calculate the trust rating function. We design our formulae as below to calculate packet forwarding ratio by using the HELLO messages. In a network, each node interchanges its message with one-hop neighbor nodes. Then, each node takes down the received message about its neighbor nodes.

The probability of packet forwarding can be calculated between two nodes Pm by using the equation which is given below:

$$P_m = \frac{\xi r(t_{i-1}, t_i)}{\xi expected\ (t_{i-1}, t_i)} \tag{1}$$

where ξr is the entire amount of HELLO packets collected and ξ *expected* is the occurrence of the entire amount of HELLO packets throughout a specific interval ($t_{i-1}$, $t_i$).

If ($P_m$< $M_{th}$), $M_{th}$ is the minimum trust threshold then the particular node Id is found to be fault and that node may be isolated.

Delay can be calculated for $j^{th}$ node is given below:

$$D_j = \left( \frac{IniEne_j - \mathrm{Re}\, sEne_j}{IniEne_j} + P_m \right) \times d_{rt} \tag{2}$$

where $IniEne_j$ and $ResEne_j$ are the initial and residual energy of $j^{th}$ node and $d_{rt}$ is the round-trip delay of the node and $P_m$ is the probability of packet forwarding using equation 1 between two node respectively.

Buffer overflow can be calculated for $j^{th}$ forwarding node is given below:

The mean traffic load at $j^{th}$ node is calculated by considering $q_k$ be the queue length of the $k^{th}$ sample at present, and $Q_L$ be the complete amount of queue length samples collected at a certain time period.

$$L_T(j) = (1/Q_L) \times \sum_{k=1}^{n} q_k \tag{3}$$

The traffic load intensity at $j^{th}$ node is calculated by considering $q_{max}$ be jth node queue's maximum length.

$$L_{TI}(j) = (L_T(j) / q_{max}) \tag{4}$$

After that, the probability of favorable outcome of packet forwarding at node j with reference to possible queue overflows PQ can be defined by

$$PQ = 1 - L_{TI}(j) \tag{5}$$

Based on the above parameters we find the trust rating function.

$$f_{tr} = \frac{1}{3}\left[\sum_{j=1}^{T^p} P_m + \sum_{j=1}^{T^p} D_i + \sum_{j=1}^{T^p} PQ\right] \quad (6)$$

where $T^p$ is the amount of nodes in the particular path.

This trust rating value we give inside cuckoo search algorithm to identify cluster head.

### 3.2. *Modified Procedure for CSA*

In CSA, with fixed amount of host nests, the probability of the host bird located the cuckoo's egg is $P_{ce} \in (0, 1)$. Here, the host bird can either throws the egg apart or leaves a nest, and creates a totally new nest. Modified CSA should use a local and global random walk which can be derived by the variable $P_{ce}$. Here below we derive the local random walk

$$w_i^{t+1} = w_i^t + \varphi s \otimes \theta(P_{ce} - \delta) \otimes (w_j^t - w_k^t) \quad (7)$$

$w_i^t$ and $w_k^t$ selected using random permutation. And θ indicates Heaviside step function and $\delta$ is the random number which we taken from uniform distribution.

Given below is the global random walk equation

$$w_i^{t+1} = w_i^t + \varphi \oplus Levy(x, y) \quad (8)$$

where φ should be greater than 0 and it is the scaling factor for the step size as x. y is the Levy random variable.

**Algorithm for modified CSA**

Begin

Produce iteration number $t = 1$

Set with unknown vector estimates and parameters

Assess the trust rating of each node (nest) and find the leading one with the best trust rating value

While (maximum of criterion is not encountered or t < Maximum production)

Achieving a new set of solutions $[w_{new}, ...w_t^{t+1}, ...w_k^{t+1}]$

Levy flight by retaining the leading one of the last iteration

Evaluate its trust rating $f_{tr}$ for node p

Select a nest from q (assume, p) randomly

If ($f_{trq} < ft_{rp}$)

Replace new nest p instead of q

End If

A proportion ($P_{ce}$) of worst ones are rejected and new nests are constructed

Retain the leading nests with specific results

Rank the results and estimate the current leading one to choose an aggregator node

Change the generation count $t = t + 1$

End while

End

### *3.3 The secure DA using Watermarking Mechanism:*

In this paper, Trust based watermarking Data aggregation (TWDA) is proposed and DAT is built after the selection of aggregator nodes or Cluster Heads (CHs) by using the above modified CSA method. When DA, every node will generate a watermark and it will integrate dynamically in the data packet and forward the same to the higher node in the routing structure. Then the received parent node checks the unification of the data by executing a verification algorithm. In this network, the aggregator node uses watermarking technique with an asymmetric key distribution mechanism. The encoding random string of bits is shared between aggregators with the base station (BS) to assure the integrity of the Data aggregation.

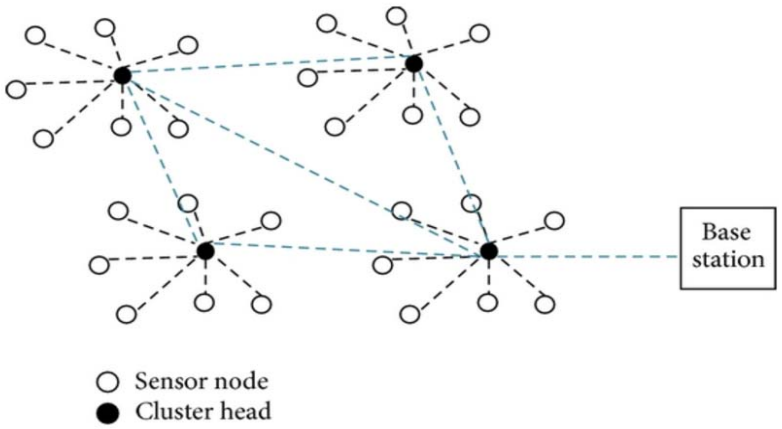


Fig.1. Distribution model

Following steps are used in the TWDA methods are

Step 1: Watermarking position is generated by using the XOR addition to merge the sensed data with MAC address.

Step 2: BS generates and exchanges the asymmetric encryption key with CH.

Step 3: CH encrypts data by utilizing Elliptic curve Diffie Hellman (EC-DH) algorithm.

Step 4: Each SN uses wakeup time of the one-hop node to compute and recognize the watermark location in the data packet.

Step 5: By using watermark extraction algorithm BS will extract the watermark after receiving the data packet.

Step 6: The extracted values are compared with newly generated watermarks. If both are identical, the data will be accepted otherwise it will be rejected.

## 4. Simulation results

This part gives out a performance evaluation based on several evaluation metrics used to evaluate the discharge of the proposed Trust based Watermarking DA (TWDA) model compared with the existing algorithm Dynamic Trust Evaluation Model (DTEM). The metrics used are the average delay, energy consumption, packet loss, packet delivery ratio, communication overhead and throughput. For this work, Network Simulator 2 (NS2) tool implemented in Ubuntu operating system, where the nodes of 200 numbers deployed randomly over a 2D area of 1000×1000 sq.m. Initially, simulations carried over with 50 nodes, and further they performed with 100 nodes,150 nodes and the last simulations are with 200 nodes. Initial energy of node is 10.1J. MAC protocol used is 802.11.

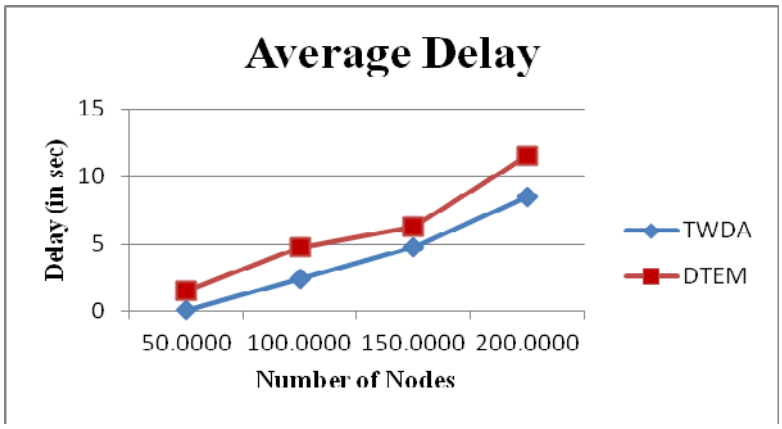


Fig. 2. Delay measured in Sec w.r.t. the varying node numbers

Figure 2 depicts the delay time measured in sec for TWDA and DTEM is shown for various node densities. The node densities are varied from 50 nodes to 200 nodes. The average delay is depicts the time desired for the transmitted data in the networks from the send off node to the receiver node. From the Figure 2, it is shown that the delay time of TWDA is less compared to the delay time of DTEM. Hence from the values calculated the delay time of the proposed TWDA is 48% lower with respect to the present DTEM.

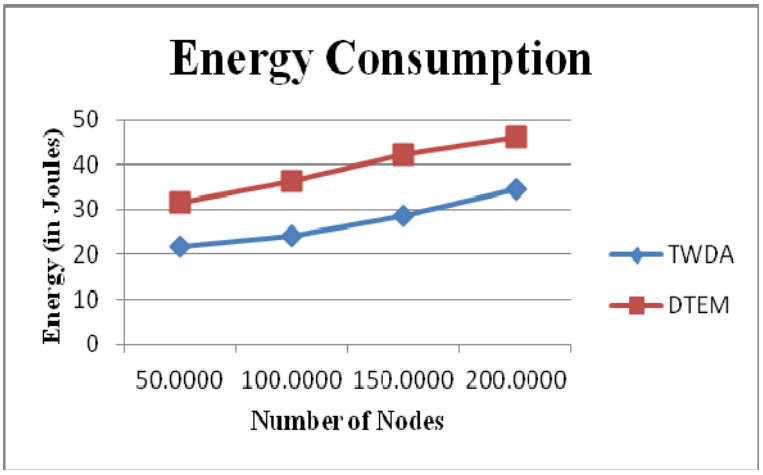


Fig. 3. Energy consumption measured in Joules w.r.t. the varying node numbers

Fig. 3 exhibits the performance of the TWDA and DTEM with regards to the energy consumption which is studied by varying number of nodes such as 50, 100, 150 and 200. It can be calculated by adding the receiving energy based on nodes numbers and the transmitted energy. This will be observed from the Fig.3 that TWDA is 31% lesser and outperforms the present system DTEM with regards to energy consumption.

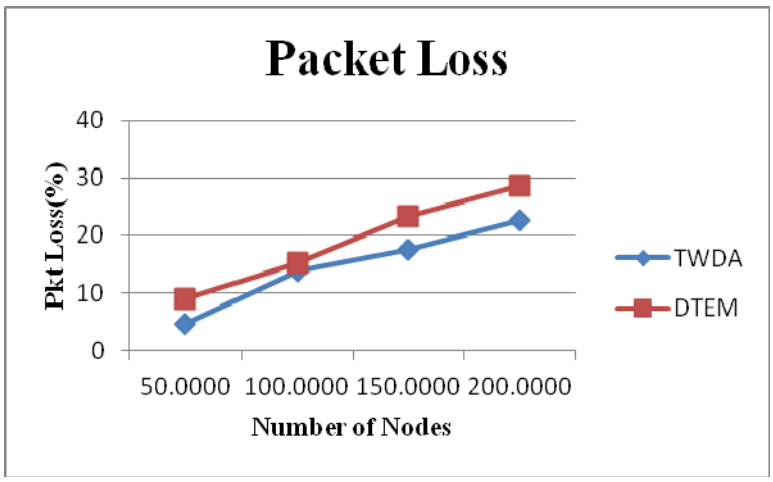


Fig. 4. Packet loss measured in percentage w.r.t. the varying node numbers

Packet loss is the number of packets that are omitted in the course of their transmission to reach at their destination. It can be viewed from the Fig.4 that TWDA is 26% lesser and outperforms the available scheme DTEM in terms of packet loss.

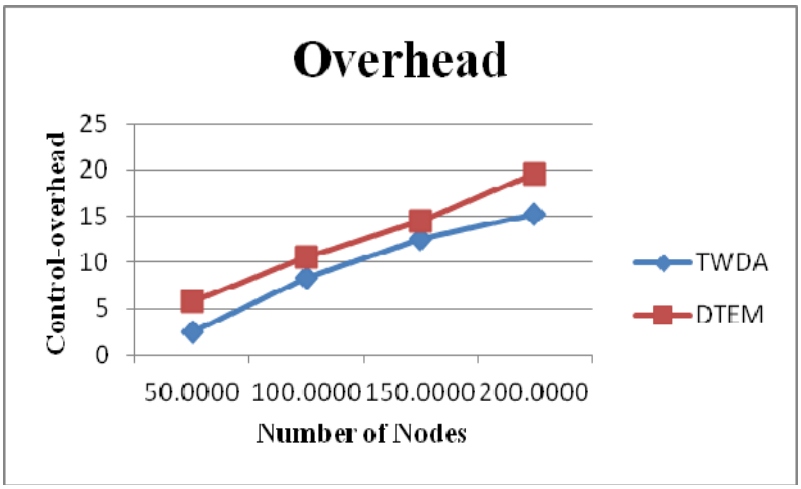


Fig. 5. Overhead w.r.t. the varying node numbers

Communication overhead mainly depends on packet size and it considered for network lifetime. It is the number of packets has to be transmitted from one node to another. It can be viewed from the Fig.5 that TWDA is 29% lesser and outperforms the available scheme DTEM in terms of overhead.

Packet delivery ratio is the relative size of data packets received and the data packets transmitted in the system. To achieve efficiency in transmission, there should be high packet delivery ratio. When the packet delivery ratio is high, then the data received at the receiver will have fewer drops. Hence from fig.6, the values calculated for Packet delivery ratio of the existing DTEM exhibits poor performance than that of proposed TWDA.

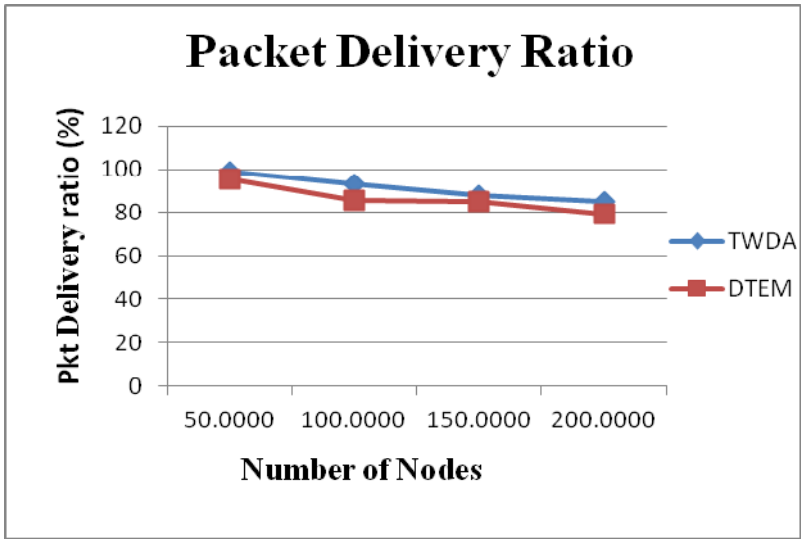


Fig. 6. Packet delivery ratio measured in percentage w.r.t. the varying node numbers

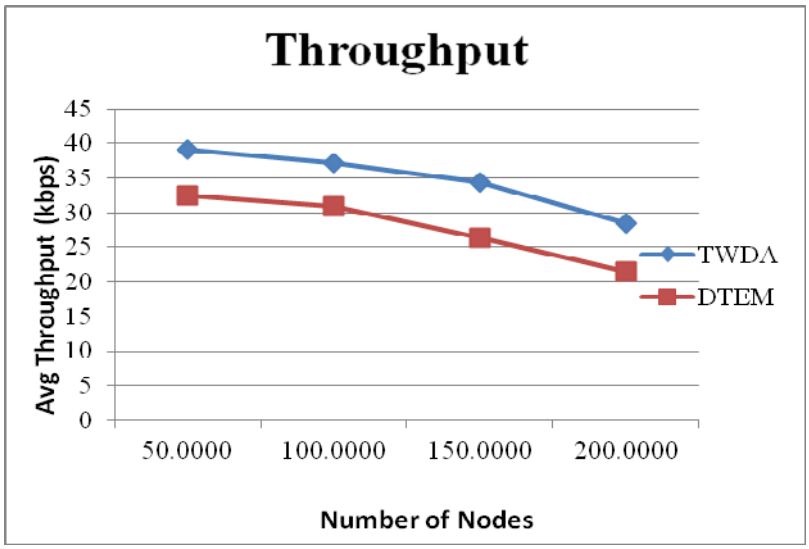


Fig. 7. Throughput is measured in kbps w.r.t. the varying node numbers

Throughput is a ratio of number of packets in the structure will be processed in an available time period. While taking the proposed TWDA from fig.7, throughput is 26% higher when compared with the existing DTEM algorithm.

Table 1. Evaluation metrics of the proposed TWDA method and EETM method

| Metrics | TWDA | | | | DTEM | | | |
|---|---|---|---|---|---|---|---|---|
| Node density | 50 | 100 | 150 | 200 | 50 | 100 | 150 | 200 |
| Average Delay (sec) | 0.1235 | 2.4231 | 4.7123 | 8.5122 | 1.5123 | 4.7561 | 6.2899 | 11.5129 |
| Energy consumption (Joules) | 21.64 | 24.01 | 28.44 | 34.42 | 31.49 | 36.28 | 42.38 | 46.01 |
| Packet loss % | 4.51 | 13.89 | 17.53 | 22.53 | 9.04 | 15.21 | 23.23 | 28.61 |
| Communication overhead ( bytes) | 2.51 | 8.31 | 12.52 | 15.30 | 5.76 | 10.59 | 14.55 | 19.60 |
| Packet delivery ratio (%) | 99.12 | 93.22 | 88.01 | 85.21 | 95.21 | 85.86 | 84.88 | 79.21 |
| Throughput(kbps) | 39.04 | 37.21 | 34.44 | 28.42 | 32.49 | 30.88 | 26.38 | 21.50 |

The delay, overhead, packet loss and energy consumption of TWDA is 48%, 29%, 26% and 31% lower with respect to the present DTEM. TWDA throughput is 26% higher when compared with the existing DTEM algorithm. Packet delivery ratio of the existing DTEM exhibits poor performance than that of proposed TWDA. The comparison of DTEM and TWDA based on the average values of the performance metrics shown in table 2.

Table 2. Comparative Metrics

| Model | Average Delay (sec) | Energy consumption (Joules) | Packet loss (%) | Communication overhead (bytes) | Packet delivery ratio (%) | Throughput (kbps) |
|---|---|---|---|---|---|---|
| DTEM | 6 | 39 | 19 | 12.6 | 86 | 28 |
| TWDA | 3.9 | 27 | 14.6 | 9.7 | 91 | 35 |

In table 2 it is evident that the network lifetime increased because delay, energy consumption, percentage on packet loss and communication overhead of the proposed TWDA are less when compared with the existing DTEM. The Packet delivery ratio and Throughput of the proposed TWDA are higher when compared with the existing DTEM.

## 5. Conclusion

In sensor network, the security of data is a vital issue. The tiny sensor devices had their own limitations and they will have disastrous effects to the attacks that are mounted against the routing service in WSN. However, since there is a high demand in resources, the standard techniques that have been used are not able to safeguard against these classical routing attacks. This work implements trust rating function which is used in modified CSA to form the DAT along with watermarking techniques leads a new exposure to evolve a security system with energy efficiency by deploying the available resources in WSNs. Hence in this proposed work, an efficient data transmission technique with high security in WSN is designed and compared with the existing method. Further, the TWDA technique will be enlarged by including various characteristics considering more indicators.

## References

[1] Reza Soosahabi, Dmitri Perkins, “Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks” IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, march 2014.
[2] Lathies Bhasker, “Genetically derived secure cluster-based data aggregation in wireless sensor networks”, Published in IET Information Security doi: 10.1049/iet-ifs.2013.0133.
[3] Patil, N.S., Patil, P.R., “Data aggregation in wireless sensor network”, IEEE Int. Conf. Computational Intelligence and Computing Research, 2010.
[4] Kumar, D., Aseri, T.C., Patel, R.B.: ‘EECDA: energy efficient clustering and data aggregation protocol for heterogeneous wireless sensor networks’, Int. J. Comput. Commun. Control, 2011, VI, (1), pp. 113–124.
[5] Huang Lu, Jie Li, Mohsen Guizani, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, march 2014.
[6] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks,” IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
[7] S. Sharma and S.K. Jena, “A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks,” Proc. International Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
[8] Mareli. M and Twala, B, An adaptive Cuckoo search algorithm for optimisation, “Applied Computing and Informatics”, September 2017.
[9] Tristan Daladier Engouang, Yun Liu, and Zhenjiang Zhang, “GABs: A Game-based Secure and Energy Efficient Data Aggregation for Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, Volume 2015, Article ID 658543.
[10] Liehuang Zhu, Zhen Yang, Jingfeng Xue, and Cong Guo, “An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks”, International Journal of Distributed Sensor Networks Volume 2014, Article ID 565480.
[11] M. Roseline Juliana, S.Srinivasan, “ SELADG: Secure Energy Efficient Location Aware Data Gathering Approach For Wireless Sensor Networks”, International journal on smart sensing and intelligent systems vol. 8, no. 3, september 2015
[12] Jong Min Kim, Hong Sub Lee, Junmin Yee and Minho Park, “Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks”, Journal of Sensors, Volume 2016 (2016), Article ID 2678269
[13] Mukesh Kumar and Kamlesh Dutta, “LDAT: LFTM based data aggregation and transmission protocol for wireless sensor networks”, Journal of Trust Management, 2016.

[14] Ms.Anuja.S.Joshi, Mr. Omkar Kulkarni, Dr. Kakandikar G. M., Dr. Nandedkar V.M, "Cuckoo Search Optimization- A Review", International Conference on Advancements in Aeromechanical Materials for Manufacturing (ICAAMM-2016).
[15] Govind P. Gupta, "Improved Cuckoo Search-based Clustering Protocol for Wireless Sensor Networks", 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017.
[16] Shirin Tahmasebi, Mohadeseh Safi, Somayeh Zolfi, Mohammad Reza Maghsoudi, Hamid Reza Faragardi and Hossein Fotouhi, "Cuckoo-PC: An Evolutionary Synchronization-Aware Placement of SDN Controllers for Optimizing the Network Performance in WSNs", Sensors 2020.
[17] Jing Cheng and Linyuan Xia, "An Effective Cuckoo Search Algorithm for Node Localization in Wireless Sensor Network", Sensors 2016.
[18] Md. Akhtaruzzaman Adnan, M.A. Razzaque, Md. Anowarul Abedin, S.M. Salim Reza and Molla Rashied Hussein, "A Novel Cuckoo Search Based Clustering Algorithm for Wireless Sensor Networks", Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering.
[19] Mohammed DEMRI, Mohamed Elsadiq BARMATI, Hanane YOUCEFI, "Enhanced Cuckoo Search-based Clustering Protocol for Wireless Sensor Networks", IEEE 2018.
[20] Djallel Eddine Boubiche, Sabrina Boubiche, Homero Toral-Cruz, Al-Sakib Khan Pathan, Azzedine Bilami and Samir Athmani. "SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs", Telecommunication System, 2015.
[21] Djallel Eddine Boubiche, Sabrina Boubiche, and Azeddine Bilami, "A Cross-layer Watermarking-based Mechanism for Data Aggregation Integrity in Heterogeneous WSNs", IEEE Communications Letters, February, 2015.
[22] Arwa Alromih, Mznah Al-Rodhaan and Yuan Tian, "A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications", Sensors 2018.
[23] Dr. Jamal Mohammed Kadhim and Enas Faris Yahya, "Watermark Authentication for Secure Data Aggregation in WSN Based on Secure Hash Algorithm and Node Identifier", International Research Journal of Advanced Engineering and Science, Volume 4, Issue 4, pp. 80-85, 2019.
[24] Sabrina Boubiche, Djallel Eddine Boubiche, Azzedine Bilami and Homero Toral-Cruz, "An Outline of Data Aggregation Security in Heterogeneous Wireless Sensor Networks", Sensors 2016.
[25] Swathi.Y, Sanjay Chitnis, "Energy Aware Fuzzy Logic Secure Data Aggregation (EA-FSDA) technique for Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-6, August 2019.
[26] Zhengwang Ye, Tao Wen, Zhenyu Liu, Xiaoying Song, and Chongguo Fu, "An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks", Journal of Sensors Volume 2017, Article ID 7864671.
[27] Kashif Naseer Qureshi, Muhammad Umair Bashir, Jaime Lloret and Antonio Leon, "Optimized Cluster-Based Dynamic Energy-Aware Routing Protocol for Wireless Sensor Networks in Agriculture Precision", Journal of Sensors, Volume 2020.
[28] R. Mahaveerakannan, Dr. C. Suresh Gnana Dhas, Dr.V.Ganesan, "Exploration on Increasing Packet delivery rate in WSN using Cluster Approach", EAI Endorsed Transactions on Energy Web and Information Technologies, Volume 5, September 2018.
[29] Mohammed Al-Medhwahi, Fazirulhisyam Hashim, Borhanuddin Mohd Ali, and A.Sali, "Impact of Packet Size in Adaptive Cognitive Radio Sensor Network", Wireless Communications and Mobile Computing Volume 2018.
[30] Gita Babazadeh Eslamlu, Masoud Sabaei, and Mehdi Fereydooni, "A New Delay Constraint Topology Control Algorithm in WSN", International Conference on Innovations in Information Technology (IIT), 2012.
[31] Minrui Wu, Yanhui Wu, Chuyao Liu, Zhiping Cai, Neal N. Xiong, Anfeng Liu and Ming Ma, "An Effective Delay Reduction Approach through a Portion of Nodes with a Larger Duty Cycle for Industrial WSNs", Sensors 2018.
[32] Vikas Srivastava, Sachin Tripathi, Karan Singh and Le Hoang Son, "Energy efficient optimized rate based congestion control routing in wireless sensor network", Journal of Ambient Intelligence and Humanized Computing, August 2019.
[33] Ranida Hamidouche, Zibouda Aliouat, Ado Adamou Abba Ari and Mourad Gueroui, "An efficient clustering strategy avoiding buffer overflow in IoT sensors: a bio-inspired based approach", Journal of IEEE ACCESS, Volume. , No. , August 2019.
[34] P. Jayarajan, G. R. Kanagachidambaresan, T. V. P. Sundararajan, K. Sakthipandi, R.Maheswar, A. Karthikeyan "An energy-aware buffer management (EABM) routing protocol for WSN", The Journal of Supercomputing, September 2018.
[35] Adwan Alanazi and Khaled Elleithy, "Buffer-overflow and Noise-handling Model: Guaranteeing Quality of Service Routing for Wireless Multimedia Sensor Networks", Asian Journal of Scientific Research, September 15, 2016.
[36] Wojciech M. Kempa, "Buffer Overflow Duration in a Model of WSN Mode with Power Saving Mechanism Based on SV Policy", Springer International Publishing AG 2017 (0975 – 8887),Volume 167 – No.7, 2017.