European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 09, 2020

AN ENERGY-EFFICIENT TRUST BASED SECURE DATA SCHEME IN WIRELESS SENSOR NETWORKS

Dr.U.Palani[1], D.Raghuraman[2], Dr.D.StalinDavid[3], R.Parthiban[4], S.Usharani[5],D.Jayakumar [6], D.Saravanan[7]

Professor[1], Department of ECE, IFET College of Engineering, Villupuram,
Senior Assistant Professor[2],Department of CSE, IFET College of Engineering, Villupuram,
Assistant Professor[3], Department of CSE, IFET College of Engineering, Villupuram,
Associate Professor[4,5,6,7],Department of CSE, IFET College of Engineering, Villupuram,

Abstract: **WSN is a series of tiny nodes of sensors that have been deployed to sense the natural phenomena in different geographical locations and send them to the Base Station for further processing through multi-hop communication. Data Dissemination is the high-level application activity provided by the WSN to make nodes using reconfiguration and reprogramming to perform the intended services. Most of the existing systems of data dissemination fail to provide confidence for data dissemination among the nodes. Because of that, there are many vulnerabilities that can occur that can interrupt the process of data dissemination.A novel confidence-based data dissemination protocol has been proposed in this paper to efficiently provide energy-efficient secured data dissemination. In the NS2 simulator, the suggested protocol is checked and values are taken after repeated measurements. The feasibility of the proposed scheme is justified by the simulation performance.**

Keywords: **WSNs, class, multipath, bypass, NS2, data dissemination.**

I. INTRODUCTION

WSN is a distributed array of tiny sensor nodes that have been deployed to sense different physical parameters pertaining to this region in different geographical locations. Data Dissemination is a service carried out in WSNs for the purpose of administering and controlling, by means of reprogramming and reconfiguration, the intended services. Various data dissemination protocols have been suggested in the literature to carry out data dissemination. The two common state-of-the-art data dissemination protocols are Design Inquiry Protocol (DIP)[7] and Difference Detection, Horizontal Search and Vertical Search

(DHV)[19], among others. The lifetime and security of nodes during data propagation is a major concern due to the resource constraint existence of WSN. To deliver the data items to the sensor nodes, most of the data dissemination protocols use trickle algorithm gossiping. Gossiping results in the Redundant Broadcast Storm Problem along with the trickle algorithm (RBSP). In addition, Denial of Service (DoS) attacks are subject to any protocol that utilizes the trickle algorithm. In addition to the lifespan of nodes, protection during data dissemination is a major concern. The data for the distribution of data is vulnerable to even a slight shift in Data can corrupt the data and can make the nodes fail to perform the services expected.In addition, there are several potential risks that can make data malicious in the distribution of data. A novel energy-efficient trust-based secured data dissemination protocol has been provided in this paper, inspired by all these observations, to effectively provide energy-efficient secured data dissemination. WSNs are a very significant form of communication developed in the twenty-first century. The invention of the wireless micro sensor led to developments in the microelectronics method. In a systematic network, wireless sensor nodes are physically distributed, densely deployed and freely organized. One hundred or even thousands of such sensor nodes may be deployed due to their small scale.They can be used for military purposes, medical diagnosis, forest fire detection, surveillance of deep water, etc.

II. LITERATURE SURVEY

In two broad categories, namely reprogramming and reconfiguration, the current data distribution work is analyzed [10]. The distribution of data that is intended to alter the functional behavior of the sensor nodes is referred to as reprogramming. Reprogramming is used in data dissemination to update existing installed code with new code which provides new features and functionality. In sensor nodes, the current installed code can be buggy, which needs to be patched on the fly. Moreover, the configuration parameters and operations needed to be performed by the sensor nodes may have changed over time for various reasons.As a consequence, it may be necessary to dynamically assign a completely new function to the sensor nodes. It is evident from the literature that reprogramming is carried out by means of protocols for the dissemination of bulk data[11]. The approach used in bulk data delivery protocols is split into three classifications. The basis of the first group of reprogramming protocols is network topology. This form provides absolute reprogramming on the entire system, where remote methods are used to distribute large data files.In network programming (INP) and multi hop over air programming (MOAP)[1], the protocol that falls under this category is. The results from this category are that it uses the topology of the

network to distribute the data items to sensor nodes. The drawbacks of these protocols are that they do not guarantee protection and are easily abused by the nodes in these protocols.

Reliability based data dissemination protocols are the next category. This type aims to provide the entire device with complete reprogramming with reliability as the basic criteria. Deluge[2], Slegue[3] and L-R Slegue[4] are the protocols that fall under this classification. The findings from these protocols are that to achieve reliability, they use the flooding mechanism to disseminate data objects. The drawbacks of these protocols are that they use a single broadcast channel to maximize the packet distribution transmission time.

The next disadvantage is the loss of packets because of volatile inferences triggered by possible collisions due to node flooding. The next weakness is the idle listing of these protocols and the issue of too many senders that consume a lot of energy during data dissemination. Finally, these protocols are epidemic in nature and a single node will weaken the system as a whole. The next reprogramming type is the data dissemination protocol based on structure. The optimal structure for disseminating the data items to the neighbor nodes is generated in this formSprinkler[5] and cord[6] are the protocols which fall under this category. The findings from these protocols are that they concentrate primarily on the latency and number of packets transmitted over the network, effectively minimizing the retransmission of packets. The drawbacks of the protocol are that the energy consumed depends on the scale of the network and the topology of the network. The drawbacks of these protocols are that the repeated use of core nodes results in rapid energy depletion, leading to core node failure. In addition, this protocol is not flexible and the network cannot be joined dynamically by new nodes.The results on full reprogramming are that it needs a significant amount of information to be disseminated, which is normally costly. The energy needed to transmit large data items across large-scale sensor networks depletes the sensor nodes' battery power and results in extreme node inconsistency that degrades the output of the network. Therefore, to perform data dissemination, light weight protocols are required to disseminate small files.

The next kind of dissemination of data is reconfiguration. Reconfiguration is the dissemination of configuration parameters, the object of which is to allow minor adjustments in the functional behavior of the nodes. Protocols for the dissemination of light weight data will perform both reprogramming and reconfiguration depending on the situation. The observation from the literature is that protocols for reconfiguration can disseminate data more efficiently than protocols for reprogramming. The most widely used technique for reconfiguration is the trickle algorithm.In order to minimize the amount of traffic by

minimizing the redundant transmission of data objects, the Trickle algorithm[16] is based on friendly gossip with routing protocols. The main purpose of this algorithm is to ensure that whatever information is available on the network is easily propagated to other network nodes. If there is no change, the overhead contact should be kept as low as possible. Design Relay Inquiry Protocol (DIP)[7], Difference Identification, Horizontal Search and Vertical Search (DHV)[19], Protected Design Relay Inquiry Protocol (Se-DRIP)[8] and Distributed Design Relay Inquiry Protocol (Di-DRIP)[8] are the protocols that use the trickle algorithm to perform data dissemination. The results from these protocols are that all other information dissemination protocols use a centralized approach, apart from Di-DRIP. A single point of failure is the unified solution. When the connection between the Base Station (BS) and the sensor nodes is broken, data dissemination is not possible. When BS is either not available or targeted by attackers, data dissemination becomes impossible.

In addition, both protocols use a trickle algorithm based on gossip that results in a DoS attack and a problem with RBSP. BS is a tempting target for the attacker to make it even worse, and it is vulnerable to multiple protection attacks that can be triggered anywhere during communication paths.Di DRIP differs from others in that it is based on a decentralized approach[13][14][15]. In this method, other nodes, including BS, perform the propagation service. The observation from this method is that other nodes also participate in the propagation service in Di-DRIP by using the trickle algorithm in addition to the base station. The Di-DRIP protocol thus decreases the BS load and removes a single failure point. The results from the literature survey are that most of the current data dissemination protocols fail to provide safe data dissemination based on energy-efficient confidence.A novel energy-efficient trust-based protected data dissemination is proposed in this paper, inspired by all these observations, to make data dissemination safe and reliable.

III. NETWORK MODEL AND ASSUMPTIONS

For the development of this protocol in the wireless sensor network, the following network assumptions will be made.

- All the sensor nodes deployed are static and do not have any mobility.
- Node energy spending varies depending on the transmission and reception of both data packets and control packets, as well as the spending of energy on idle time and sleep.
- The nodes' initial energy is 100JJ.
- While nodes are inherently resource-constrained, they can still measure trust and perform simple cryptographic operations over a lifetime.

IV. SECURED DATA Distribution PROTOCOL TRUST BASED

A new secured data dissemination protocol based on light weight trust is proposed that can effectively provide energy-efficient trust-based secured data dissemination. The confidence-based secure data dissemination protocol consists of three phases: the key generation phase, the confidence calculation phase, the transmission of packets and the reception phase.

A. Phase of Key Generation

In the proposed system, the first stage is the key generation phase. The elliptical curve discrete logarithm problem (ECDLP) is used in the proposed system to generate keys for secure data transmission. As follows, the steps for generating the keys are explained.

1. Define the elliptical curve E over the finite field Fq, a point of order n p € E(Fq) and a point Q = rP where 0≤ r ≤ n-11
2. The Base Station (BS) generates the Base Station key (KBS1) after the construction of the elliptical curve by selecting a random integer Ru and computing the point Gu = Ru P = (Gxu, Gyu) over an elliptical curve
3. By choosing a random integer Su, BS generated (KBS2) calculates the point Su = r u p = (Sxu, syu) over an elliptical curve.
4. By selecting a random integer Su, 4.BS generated (KBS3) computes the point by selecting a random integer Hu and calculates the point Hu = r u p = (Hxu, Hyu) over an elliptical curve.
5. {KBS1, KBS2, KBS3 } is the private PK key.
6. The {Ru, Su, Hu}is public key.

For the pre-deployment process, both public keys and private keys are installed in the nodes.

B. Phasis of trust calculation

The corresponding nodes calculate the trust values in the trust score calculation phase and send them to BS. Direct trust and indirect trust are the trust metrics for the trust score calculation.

Direct calculation of trust

Direct trust is calculated based on the observations of the nodes themselves. Node A counts, in direct trust, the number of packets forwarded by node B. Equation (1) [23] calculates the packet forwarding ratio from Node B to its neighboring nodes.

FPKT/(FPKT+DPKT): PFR AB= (1)

Where PFR AB is the ratio of packet forwarding, FPKT is the number of packets forwarded to its neighboring nodes by node B at time T and DPKT is the number of packets dropped to time T by node B.

In direct trust, the consistency of the behavior of nodes can be determined using the equation (5)

$$\text{Node Consistency} = \frac{\text{Present forwarding ratio for packets}}{Past\ packet\ forwarding\ ratio} \quad (2)$$

Let FR reflect the rate of fluctuations in node behavior from time T to T-1 in terms of packet forwarding ratio. Let PF be the punishment factor for the degradation of performance in the packet forwarding ratio and EF is the incentive factor for the increase in packet forwarding ratio performance. If the punishment factor is greater than the stimulus factor, then the rate of fluctuations is FR € (0,1).

1. Check if the previous rate of fluctuations is greater than the current rate of fluctuations. The FR increases and the node consistency decreases.

   If FRAB(t) (T-1) > FRAB(t) (T-1) (T)

   Then

   FR = FR(T-1) - PF * (FRAB(T) - FRAB(T-1) - (T-1)

2. Check that the previous rate of fluctuations is lower than the current rate of fluctuations, the FR decreases, and node consistency increases.

   If FRAB(t) (T-1) < FRAB(t)(T-1) (T)

   FR = FR(T-1) - EF * (FRAB(T) - FRAB(T-1) - (T-1)

3. Verify that the previous rate of fluctuations is equal to the current rate of fluctuations, then FR and node consistency remain constant.

   FR = FR FR (T-1)

Based on the above observations, the direct trust is calculated by using the equation (3)

$$(FRAB(T) * \cos(\pi/2 * FR) = DTAB(t) \quad (3)$$

Indirect trust calculation

A node calculates the recommendation credibility of the neighbor node in the indirect trust calculation by calculating the indirect trust between them. This Root Mean Square (RMS) error is used in indirect trust to differentiate neighbor evaluation between nodes. Let X be the common set of node A and node B neighbors. The node X evaluation error for node A and node B is calculated in equation 4.

$$Eerr_A^B(t) = \sqrt{\frac{\sum_{x \epsilon X_{AB}} (DT_A^x(t) - DT_B^x(t))^2}{|X_{AB}|}} \quad (4)$$

The similarity parameter SAB(t) is referred to in ITAB(t) as the similarity between node A and node B, to the extent that node A and node B are the same in terms of confidence. Based on a threshold value (γ), the similarity parameter increases or decreases. The parameters N and φ decide the rise and decrease of SAB (t). In equation 5, the SAB(t) is computed

S_A^B (t) =S_A^B (t-1) + 1- S_A^B (t-1)Eerr_A^B (t)< γ(5)

S_A^B (t-1) - S_A^B (t-1) / φ Otherwise

TheIT_A^B (t)is calculated by using the equation 6

ITAB(t)=1-log(SAB(t)/log(n)SAB(t)>0-log(SAB(t)/log(n)(6)

The BS calculates the total trust score using the equation after computing the direct trust and indirect trust for each node of the corresponding group (7). Each node's trust value is installed prior to the pre-deployment stage.

Total confidence score = Direct confidence + Indirect confidence (7)

C. Phase of Packet Transmission and Reception

The next stage is the transmission of packets and the reception phase. The BS finds the optimum routing path between source nodes and destination nodes based on trust score, link quality and residual energy prior to the packet transmission phase. The method for finding the optimum routing path is explained as follows.

- BS requests all the sensor nodes that are present in the network for the trust score and residual energy.
- For all sensor nodes,
- BS identifies the possible paths requested for data dissemination between source nodes and target nodes.
- For each path between source nodes and destination nodes,
- BS calculates the average confidence score of each route present in path i.
- BS calculates the average residual energy of all paths to target nodes from the source node.
- BS calculates the quality of links based on ETX metrics for all paths.
- After calculating the confidence score, the quality and energy of all path I nodes from source to destination are linked.

- BS discovers the best optimal path based on trust score, residual energy and quality of connections.
- The paths are prioritized on the basis of confidence score, residual energy and quality of the link.
- BS selects one of the best possible paths for effective dissemination of data.

In packet transmission, BS constructs the data dissemination packets after identifying the optimal path and encrypts them with its public key and transmits them via multi-hop communication to the target nodes. The recipient is the target nodes that are in need of data dissemination packets in the packet reception phase. The target node decrypts and checks that the received packets are authenticated using their private keys. The node updates its code if the received packets are valid, otherwise the packets will be discarded.

D. Implementation setup

With the NS2 Simulator, the proposed protocol is checked and implemented. Table 1 gives theparameters of the simulation used in the proposed system.

Table I: Proposed system simulation parameters

Network simulator	NS2
Simulation area	1000*1000m
Density of nodes	1000 to 1500
Transmission range	25-30ms
Physical layer	Phy/wirelessphy-mica2
Radio Propagation model	Two ray model
Environment	Urban
Nodeinitial energy	150J
Transmission power (tx)	1.5J per packet
Receiving power (rx)	0.48J per packet

Simulation duration	50 minutes
No of trails	65
Packet size	30bytes

E. Results and discussions:

With other existing protocols based on Average Energy Dissipated (ADE), Dissemination Ratio (DR), Nodes life time, End to end delay, the proposed protocol is assessed.

Dissipated average energy (DAE)

A comparison of the ADE of the proposed scheme with DI-DRIP and SEL-DRIP is provided in Figure 1. Compared to other existing systems, the proposed system has better average energy dissipated from the graph because the proposed system provides confidence-based secure data dissemination and discovers the optimal path based on confidence score, quality of the link and residual energy. If, as in the current system, during data dissemination, it does not provide optimal security and floods data to sensor nodes.

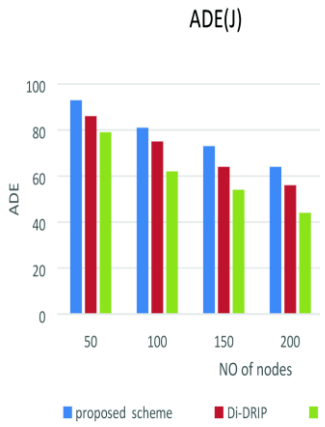

Figure 1. Average immoral Energy

- **Dissemination Ratio**

The dissemination ratio of the proposed scheme with the protocols DI-DRIP and SEL-DRIP is given in Figure 2. It is clear from the graph that the proposed scheme has a better dissemination ratio because the system proposed reduces the transmission and retransmission of data and discovers the optimal routing path for the dissemination of data items. Hence, compared to other existing protocols, the proposed system has a better dissemination ratio.

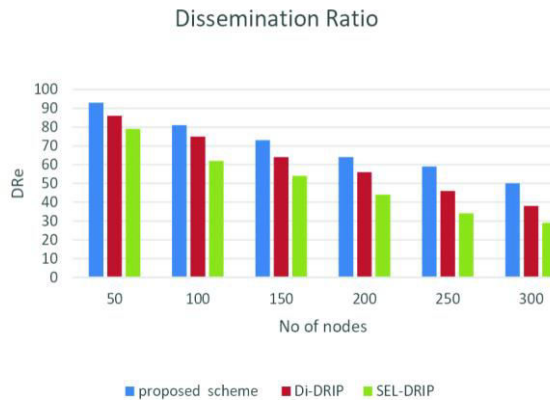

Figure 2. Broadcasting Ratio

Figure 3 provides the lifespan of the nodes between the proposed system and existing systems. It is clear from the graph that the nodes have better life time in the proposed scheme compared to other existing systems because the proposed scheme uses confidence-based secure data transmission and discovers the optimal routing path for transmitting data items. Where, as in current data dissemination protocols, flooding is used to transmit data items. Therefore, compared to existing systems, the proposed scheme has a better node lifetime.

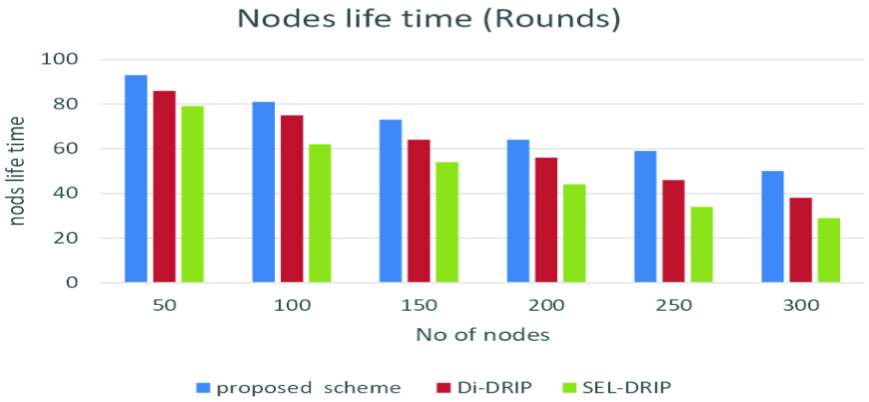

Figure 3. Bulges life time

- **Residual Energy**

  The residual energy comparison of the proposed scheme with existing systems is shown in Figure 4. It is clear from the graph that, compared to other existing protocols, the proposed system has better residual energy because the proposed protocol consumes optimal energy for transmission of packets and reception of packets. Hence, compared to other existing protocols, it has better residual energy.

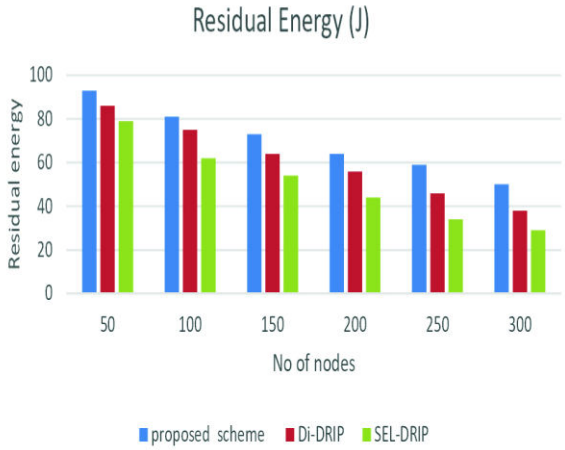

Table 1 provides a comparison of the proposed EETBSDDP protocol to the existing Bypass routing protocol and the Multipath routing protocol. From the perspective of power utilization, reliability, scalability and QoS, this table provides a comparison. In comparison to the Multipath routing protocol and the Bypass routing protocol, the proposed EETBSDDP protocol offers the highest QoS. EETBSDDP power consumption is lower and has good scalability and high reliability.

TABLE II. Comparison Of EETBSDDP With Existing Protocols

Routing Protocols	*Power Usage*	*Reliability*	*Scalability*	*QoS*
Bypass Routing Protocol	Lowest	Less	Good	Ok
Multipath Routing Protocol	High	Highest	Good	Ok
EETBSDDP	Low	High	Good	Ok

V. COMPARISON OF EETBSDDP WITH EXISTING PROTOCOLS

Table II provides a comparison of the proposed EETBSDDP protocol with the current Bypass routing protocol and the Multipath routing protocol. This table compares the power usage, reliability, scalability and QoS aspects of the protocol. In comparison to the Multipath routing protocol and the Bypass routing protocol, the proposed EETBSDDP protocol offers

the highest QoS. EETBSDDP power usage is smaller and has good scalability and high reliability.

VI. CONCLUSION AND FUTURE WORK

A trust-based secured dissemination protocol is proposed in this paper that offers energy-efficient secured dissemination of data by providing trust-based dissemination of energy-efficient data. The proposed protocol uses the NS2 simulator to implement it. The results of the simulation show that efficient data dissemination can be provided by the proposed protocol. The future work of the proposed scheme is aimed at improving its capacity to provide security and energy efficiency. WSNs for many applications now have the most hopeful future. Numbers of changes were introduced by different authors in the multipath routing protocols using different methods, but the concept of the class of the proposed work enhances the reliability and energy efficiency. Advance reliable and effective protocol for dissemination of data does not alter the size of the message or packet and does not use any additional resources. It can easily be applied to the current system. Due to memory and hardware limitations, it is very difficult for large and complex routing algorithms to be implanted. Due to limited sensor resources on wireless sensor networks, overall security is also difficult. We are continuing our research into our project for efficiency and reliability in wireless sensor networks along with future security.

References:

1. L. Wang, “MNP: Multihop network reprogramming service for sensor networks”, in: Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems, USA, 2004.
2. J.W.Hui, D.Culler,“The dynamic behavior of a data dissemination protocol for network programming at scale” In: Proceedings of the 2nd international conference on Embedded networked sensor systems (Sensys 04), New York, NY, USA, ACM (2004) 81-94
3. S. Hyun, P. Ning, A. Liu, and W. Du, “Seluge: secure and DoS resistant code dissemination in wireless sensor networks” , in Proc. 2008, ACM/IEEE IPSN, pp. 445-456.
4. Rui Zhang, Yanchao Zhang “LR-Seluge: Loss-Resilient and Secure Code Dissemination in Wireless Sensor Networks”In: International Conference on

Distributed Computing Systems, proc.2011,IEE computer society, page number 497-506.

5. V. Naik, A. Arora, P. Sinha, H. Zhang, “Sprinkler: a reliable and energy efficient data dissemination service for wireless embedded devices”,in: Proceedings of the 26th IEEE International Real-Time SystemsSymposium (RTSS), 2005.
6. L. Huang, S. Setia, “CORD: energy-efficient reliable bulk data dissemination in sensor networks”, in: Proceedings of INFOCOM, 2008.
7. K. Lin, P.Levis,“Data discovery and dissemination with dip”, In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC, USA, IEEE Computer Society (2008) 433-444.
8. Daojing He, Sammy Chan, Shaohua Tang, and Mohsen Guizani, “Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", IEEE transactions on wireless communications, vol. 12, no. 9, september 2013.
9. Daojing He, Sammy Chan, Shaohua Tang, and Mohsen Guizani, "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", ieee transactions on wireless communications, vol. 26, issue no: 4 pp : 1129 - 1139, April 2015.
10. D. Stalin David, A. Jayachandran, 2018, “Textures and intensity histogram based retinal image classification using hybrid color structure descriptor”, Biomedical and Pharmacology Journal, Vol.11 issue 1, pp.577-582.
11. D. Stalin David, 2019, “Parasagittal Meningiomia Brain Tumor Classification System based on MRI Images and Multi Phase level set Formulation”, Biomedical and Pharmacology Journal, Vol.12, issue 2, pp.939-946.
12. D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-6, doi: 10.1109/CESYS.2016.7889823.
13. Stalin David, D., Jayachandran, A. A new expert system based on hybrid colour and structure descriptor and machine learning algorithms for early glaucoma diagnosis. Multimed Tools Appl 79, 5213–5224 (2020). https://doi.org/10.1007/s11042-018-6265-1.
14. De P, Liu Y, Das S K. Remo,“An energy efficient reprogramming protocol for mobile sensor networks”, In Proc. the 6th IEEE PerCom, Mar. 2008, pp.60-69.

15. PantaR K, Khalil I, Bagchi S. Stream,"Low overhead wireless reprogramming for sensor networks", In Proc. the 26th IEEE INFOCOM, May 2007, pp.928–936.
16. Q. Wang ,Y. Zhu, L. Cheng ,"Reprogramming wireless sensor networks: Challenges and approaches", IEEE Network, 2006, 20(3): 48-55.
17. D Stalin David, A Jayachandran, 2018, Robust Classification of Brain Tumor in MRI Images using Salient Structure Descriptor and RBF Kernel-SVM, TAGA Journal of Graphic Technology, Volume 14, Issue 64, pp.718-737.
18. D Stalin David, 2016, Robust Middleware based Framework for the Classification of Cardiac Arrhythmia Diseases by Analyzing Big Data, International Journal on Recent Researches In Science, Engineering & Technology, 2018, Volume 4, Issue 9, pp.118-127.
19. D Stalin David, 2020, 'Diagnosis of Alzheimer's Disease Using Principal Component Analysis and Support Vector Machine, International Journal of Pharmaceutical Research, Volume 12, Issue 2, PP.713-724.
20. D Stalin David, 2020, 'An Intellectual Individual Performance Abnormality Discovery System in Civic Surroundings' International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 5, PP.2196-2206.
21. Geoss. [Online].Available: http://www.epa.gov/geoss/
22. NOPP. [Online].Available: http://www.nopp.org/
23. ORION[Online].Available:http://www.joiscience.org/oceanobserving/advisors
24. P.Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A self-regulating algorithm for code maintenance and propagation in wirelesssensor networks", in Proc. 1st Conf. Symp. Netw. Syst. Design Implementation, 2004, pp. 15–28
25. Daojing He, "Accountable and Privacy-Enhanced AccessControl in Wireless Sensor Networks", IEEE transactions on wireless communications", vol. 14, no. 1, january 2015,387-3
26. S.Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained accesscontrol in wireless sensor networks," in Proc. IEEE IPDPS, 2011,pp. 352–362
27. T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistency maintenance protocol for multi-hop wireless sensor networks," inProc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp.327–342.20
28. D Stalin David, 2020, 'Machine learning for the prelude diagnosis of dementia', International Journal of Pharmaceutical Research, Volume 13, Issue 3, PP.2329-2335.

29. Stalin David D, Saravanan D, 'Multi-perspective DOS Attack Detection Framework for Reliable Data Transmission in Wireless Sensor Networks based on Trust', International Journal of Future Generation Communication and Networking , Volume 13, Issue 4, 2020, PP.1522–1539.
30. J. K. S and D. S. David, "A Novel Based 3D Facial Expression Detection Using Recurrent Neural Network," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-6, doi: 10.1109/ICSCAN49426.2020.9262287.
31. Stalin David D, Saravanan M, "Enhanced Glaucoma Detection Using Ensemble based CNN and Spatially Based Ellipse Fitting Curve Model", Solid State Technology, Volume 63, Issue 6, PP.3581-3598.
32. Stalin David D, Saravanan M, Jayachandran A, "Deep Convolutional Neural Network based Early Diagnosis of multi class brain tumour classification", Solid State Technology, Volume 63, Issue 6, PP.3599-3623.
33. R.Parthiban, Dr.K.Santhosh Kumar, Dr.R.Sathya, D.Saravanan," A Secure Data Transmission And Effective Heart Disease Monitoring Scheme Using Mecc And Dlmnn In The Cloud With The Help Of Iot", International Journal of Grid and Distributed Computing, ISSN: 2005 – 4262, Vol. 13, No. 2, (2020), pp. 834 – 856.
34. R.Bhavya, G.I.Archanaa, D.Karthika, D.Saravanan," Reflex Recognition of Tb Via Shade Duplicate Separation Built on Geometric Routine", International Journal of Pure and Applied Mathematics 119 (14), 831-836.
35. D Saravanan, R Bhavya, GI Archanaa, D Karthika, R Subban," Research on Detection of Mycobacterium Tuberculosis from Microscopic Sputum Smear Images Using Image Segmentation", 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).
36. D Saravanan, R Parthiban," Automatic Detection of Tuberculosis Using Color Image Segmentation and Statistical Methods", International Journal of Advance Research in Science and Engineering, Volume 6, Issue 10.
37. U.Palani, D.Saravanan, R.Parthiban, S.Usharani," Lossy Node Elimination Based on Link Stability Algorithm in Wireless Sensor Network", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6S5.
38. S.G.Sandhya, D.Saravanan, U.Palani, S.Usharani," Handover Priority to the Data at Knob Level in Vanet", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6S5.

39. D.Saravanan R.Parthiban, U.Palani S.G.Sandhya," Sheltered and Efficent Statistics Discrimnation for Cluster Based Wireless Antenna Networks", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6S5.
40. D.Saravanan[1], Dr. K.Santhosh Kumar[2],, R.Sathya[3], U.Palani[4], "An Iot Based Air Quality Monitoring And Air Pollutant Level Prediction System Using Machine Learning Approach – Dlmnn", International Journal of Future Generation Communication and Networking, Vol. 13, No. 4, (2020), pp. 925–945.
41. Raghu Raman D, Saravanan D, Nivedha R,"An Efficacious E-Portal for Rancher to Buy
42. Seeds and Humus", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-1S5, June 2019.
43. M.Sudha, D.Saravanan,cS.Usharani," Security Improvement of Dropper Elimination Scheme for IoT Based Wireless Networks", International Journal of Engineering Trends and Technology (IJETT) ,Volume-45 Number3 -March 2017.
44. K. Gayathri, D.Saravanan," An Innovative IOT security Enhancing Schema Based Gamed Theory Decryption Percentage", International Journal of Advanced Research in Science and Technology, Volume 6, Issue2, 2017, pp. 666-671.
45. E.Kowsalya, D.Saravanan, R.Parthiban," Energy Aware Resource Allocation for Throughput Maximized IOT Network", International Journal of Computer Trends and Technology (IJCTT) – Volume 45 Issue 2- March 2017.
46. Santhosh Kumar SVN, Yogesh P, "Privacy Preserving with Enhanced Access Control for Distributed Data Dissemination in WSN," Asian Journal of Research in Social Sciences and Humanities, Vol. 6, No. 12, December 2016, pp. 561-577
47. E.goldenjulie, S.tamilselvi, "CDS-fuzzy opportunistic routing protocol for WSN," wireless personal communication, 2016.
48. Santhosh Kumar SVN, Yogesh Palanichamy, "Energy Efficient and secured distributed data dissemination using hop by hop authentication in WSN", Wireless Networks, 2017.
49. VijenderBusireddy,SarmaVenkataraman,"Communication and data trust for Wireless Sensor networks using D-S theory," IEEE Sensor Journal, Vol. 17, No. 12, 2017.