SECURE AND TRUSTABLE ROUTING IN WIRELESS SENSOR NETWORKS USING ACTIVE DETECTION ROUTING PROTOCOL

S. Karthikeyan[1],
Associate professor, Dept. of ECE
Sathyabama Institute of Science and Technology, Chennai
skarthi1879@gmail.com

Katikareddy Venkata Suhas Reddy[2],
Associate professor, Dept. of ECE
Sathyabama Institute of Science and Technology, Chennai

Katasani Venkata Bypu Reddy[3],
Associate professor, Dept. of ECE
Sathyabama Institute of Science and Technology, Chennai

T. Ravi[4]
Associate professor, Dept. of ECE
Sathyabama Institute of Science and Technology, Chennai

Abstract: A Wireless Sensor Network (WSN) contains gadgets that are self-sufficiently conveyed in space used to direct the physical and natural conditions with the assistance of sensors. They are primarily utilized as a part of security basic applications, for example, checking nature, following the environment and controlling regions. As a result of the asset impediment and computational limitations the WSNs are straightforward to different security assaults. Dark opening assault is a genuine assault which seriously influences the bundle exchange from source to goal. Here the Active Trust conspire is utilized to stay away from the Black opening assault. The Active Trust conspire keeps away from the dark openings through Active discovery directing and information steering which enhances the course security. Both complete hypothetical investigation and exploratory outcomes demonstrate that the execution of the Active Trust conspire is superior to anything that of past examinations. Dynamic Trust can fundamentally enhance the information course achievement likelihood and capacity against dark gap assaults and can enhance arrange lifetime.

Keywords: — Security, BHL, NL- Network lifetime, Trust, Wireless sensor networks(WSN).
1. INTRODUCTION

Wireless Sensor Networks are rising as a promising innovation as a result of their extensive variety of utilizations in modern, ecological checking, military and regular citizen areas. A remote sensor arrange is a self-sorting out system comprising of sensor hubs which can differ from hundreds to thousands in numbers. Every sensor hub has confined preparing, stockpiling limit, computational control. In remote sensor arrangements, each sensor hub speaks with other condition to think about its neighborhood condition and the information will send to any hub if any solicitations are coming. In remote sensor systems, it isn't much secure when vast zone of system contrasted with little zone of system [3]. Due to the innate qualities like memory constraints, open condition, control confinements and unattended nature, the security of a remote sensor arrange is traded off [11]. These feeble attributes makes the system effortlessly traded off by a foe to make assaults bringing about deplorable results. Dark Hole assault is one of the perilous assault which abuses a Dependability of a system by promising steering of information bundles to the goal realizing that it has a Most brief way yet as a general rule it drops all parcels and in addition specifically drops the parcels, and therefore undermines unwavering quality. As remote sensor systems are causing numerous security dangers, in this paper we are keeping away from the dark opening hub by proposing a procedure of information directing with no come up short. The dark gap assault gives the circumstance where an aggressor attempting to trade off some of hubs to track the data and hinder with the ordinary working of the WSN by consistently evolving, irritating, or breaking the usefulness of the hubs in the framework. This assaults will brings about producing the dark openings: zones inside which the enemy can either inactively catch or effectively piece data conveyance. The assailants can give numerous dark gaps because of the unattended idea of WSNs. By this assault enemy can upset typical information conveyance between sensor hubs and the sink, or even parcel the topology.

Be that as it may, the present trust-based course methodologies confront some trying issues [24]. (1) The center of a trust course lies in getting trust. In any case, getting the trust of a hub is exceptionally troublesome, and how it should be possible is as yet vague. (2) Energy productivity. Since vitality is extremely restricted in WSNs, in most research, the trust procurement and dispersion have high vitality utilization, which truly influences the system lifetime. (3) Security. Since it is hard to find noxious hubs, the security course is as yet a testing issue. In this way, there are still issues deserving of further investigation. Security and trust directing through a dynamic recognition course convention is proposed in this paper. The principle developments are as per the following.

(1) The ActiveTrust conspire is the principal directing plan that utilizes dynamic identification steering to address BLA. The most noteworthy distinction amongst ActiveTrust and past research is that we make numerous identification courses in locales with buildup vitality; in light of the fact that the aggressor doesn't know about location courses, it will assault these courses and, in this manner, be uncovered. Thusly, the assailant's conduct and area, and nodal trust, can be gotten and used to maintain a strategic distance from dark openings when preparing genuine information courses. To the best of our insight, this is the primary proposed dynamic discovery system in WSNs.

(2) The ActiveTrust course convention has better vitality proficiency. Vitality is valuable in WSNs, and there will be more vitality utilization if dynamic discovery is handled. Thusly, in past research, it was difficult to envision embracing such high-vitality utilization dynamic discovery courses. Be that as it may, we think that its conceivable after deliberately examining the vitality utilization in WSNs. Research has noticed that there is still up to 90% buildup vitality in WSNs when the system has kicked the bucket due to the "vitality opening" marvel. Subsequently, the ActiveTrust plot takes full preferred standpoint of the buildup vitality to make location courses. Those recognition courses can recognize the nodal trust without diminishing lifetime and along these lines enhance the
system security. As indicated by hypothetical investigation and test comes about, the vitality proficiency of the ActiveTrust conspire is enhanced in excess of 2 times contrasted with past directing plans, including most brief steering, multi-way directing.

(3) The ActiveTrust plot has better security execution. Contrasted and past research, nodal trust can be gotten in ActiveTrust. The course is made by the accompanying standard. To begin with, pick hubs with high trust to maintain a strategic distance from potential assault, and after that course along a fruitful discovery course. Through the above approach, the system security can be moved forward.

(4) Through our broad hypothetical examination and reproduction consider, the ActiveTrust directing plan proposed in this paper can enhance the achievement steering likelihood by 1.5 times to 6 times and the vitality productivity by in excess of 2 times contrasted and that of past.

2. RELATED WORKS

Anbuchelian. S et al proposed [1] a vitality sparing grouping calculation for identifying the assaults on bunch heads and therefore prompts the better vitality utilization in the remote sensor systems. Vipul Sharma et al [9] proposed a strategy for the discovery and concealment of dark opening assault in Leach based sensor systems. The go for this examination work is to propel an instrument that can distinguish and defeat the impact of dark opening assault in sensor arrange. The bad mark in this paper was it won't identify the sensor hubs as a dark gap hub.

Barleen Shinh proposed [2] a system to recognize and segregate the dark gap assault. The proposed instrument will recognize the vindictive hub and stop, it from the system. The system depends on the throughput of the system. At the point when the throughput of the system, will abatements to certain limit esteem, hubs in the system will go to head hub and identify the vindictive hub. Single-way steering is a simple directing convention however is immediately caught by the assailant. Regardless of whether there is an assault in one course, the bundle can safely achieve the goal.

Tao Shu propose [7] a randomized multi-way directing calculation to distinguish dark opening assault. Under the outline, the courses taken by the "offers" of various bundles change after some time. So the assailant can't track the courses passed by every parcel if the steering calculation ends up known to the aggressor. Wenjing Lou propose and explore a novel plan, [4] Security Protocol for REliable dAta Delivery (SPREAD), to improve the information privacy benefit in a system. The proposed SPREAD plan expects to give encourage security to mystery messages from being traded off when they are conveyed over the uncertain system D Loganathan likewise propose [5] a crossover multipath plot (H-SPREAD) to enhance both security and unwavering quality of this errand in a conceivably antagonistic and inconsistent remote sensor arrange. The new plan depends on a N-to-1 multipath convention which finds various ways from each hub to in one course revelation process. There are diverse multipath course development techniques.

H.- M. Sun [8] proposes a multi dataflow topologies (MDT) way to deal with oppose the specific sending assault. In the event that one topology neglected to send the information, the goal will get the information through other topology.

Yuxin Liu, [10] proposed a dynamic put stock in conspire for secure and trustable directing in remote sensor systems. The paper proposes a dynamic identification directing of information for better security and trust. The primary objective of the plan is to guarantee that the nodal information securely achieve the sink and are not hindered by the dark gap. The identification course discovers high put stock in hub and in information directing, it
will chooses the course without dark gap hub and in this way enhance the achievement proportion of information achieving the sink. Indeed, even there is numerous examination on dark hub assault and evasion, there is still parts for additionally ponder. Single-way directing is a basic steering convention [12] however is effectively hindered by the aggressor. In this way, the most characteristic approach is by means of multi-way directing to the sink. Regardless of whether there is an assault in some course, the information can even now securely achieve the sink [9]. Multi-way directing conventions can be grouped into two classes relying upon whether the information bundle is isolated. One is multi-way steering without share division. The other is multi-way steering with share division, i.e., the parcel is separated into shares, and diverse offers achieve the goal by means of various courses [9].

(1) Non-share-based multi-way steering. There are diverse multi-way course development strategies. Ref. [25] proposes a multi dataflow topologies (MDT) way to deal with oppose the specific sending assault. In the MDT approach, the system is isolated into two dataflow topologies. Regardless of whether one topology has a pernicious hub, the sink can in any case acquire bundles from the other topology. In such conventions, the insufficiency is that if the parcel is steered through n courses all the while, the vitality utilization will be n times that of a solitary way course, which will truly influence the system lifetime; comparable research can be seen in multi-way DSR [25], the AOMDV [18] and AODMV [26].

(2) Share-based multi-way directing conventions. The SPREAD calculation in [27] is a commonplace offer based multi-way directing convention. The essential thought of the SPREAD calculation is to change a mystery message into different offers, which is known as a (T, M) edge mystery sharing plan [28]. The M shares are conveyed by different free ways to the sink with the end goal that, regardless of whether few offers are dropped, the mystery message overall can in any case be recuperated [9, 16, 28]. The benefit of this calculation is that through multi-way directing, every way courses just a single offer, and the aggressor must catch in any event T offers to reestablish nodal data, which builds the assault trouble [9]. Subsequently, the protection and security can be progressed. In the above research, the multi-way steering calculations are deterministic with the end goal that the arrangement of course ways is predefined under a similar system topology [9]. This shortcoming opens the entryway for different assaults if the directing calculation is acquired by the foe [9]. For the shortcoming said above, Ref. [29] proposed four irregular engendering methodologies: arbitrary spread (PRP), coordinated irregular proliferation (DRP), non-dreary arbitrary spread (NRRP), and multicast tree helped arbitrary spread (MTRP). The general procedure is as per the following. To begin with, partition the message into M shares, and the course way of each offer isn't foreordained. Along these lines, regardless of whether the enemy procures the directing calculation, it is hard to dispatch a pinpointed hub trade off or sticking assault. Since it is hard to catch more than T shares, the security is additionally made strides. In multi-to-one information gathering WSNs, we contend that for exemplary "cutting and collecting" or multi-way directing strategies, cut offers will converge in a similar way with high likelihood, and this way can be effectively assaulted by dark openings. Subsequently, in [16], a Security-and Energy-productive Disjoint Route (SEDR) plot is proposed to course cut offers to the sink with randomized disjoint multipath courses by using the accessible surplus vitality of sensor hubs. The creators exhibit that the security is expanded without decreasing the lifetime in the SEDR convention. Another strategy to keep away from assault and enhance course achievement likelihood is trust steering. Trust administration [20] is turning into another main impetus for explaining challenges in specially appointed systems [21], distributed systems [22], and WSNs [23, 24].

Zhan et al proposed a trust-mindful directing structure convention (TARF), utilizing trust and vitality cost for course choices, to keep vindictive hubs from deceiving system movement [30]. Ref. [31] proposes the Sec-CBSN calculation, which creates distinctive trust computation strategies in light of nodal parts. Ref. [32] builds up an assault safe and lightweight trust administration convention named ReTrust, which can oppose assaults through a trust administration approach for medicinal sensor systems (MSNs). Ref. [33] presents a proposition named TRIP, which means to rapidly and precisely distinguish malevolent or childish hubs spreading false data in vehicular...
impromptu systems (VANETs). Ref. [34] additionally proposes a flexible confidence display, SensorTrust, for various leveled WSNs. Ref. [24] presents the idea of property closeness in finding possibly agreeable hubs among outsiders.

3. EXISTING SYSTEM

Blockhole assaults is a standout amongst the most run of the mill assaults and fills in as takes after. The enemy bargains a hub and drops all parcels that are directed by means of this hub, bringing about touchy information being disposed of or unfit to be sent to the sink. Since the system settles on choices relying upon the hubs' detected information, the outcome is that the system will totally come up short and, all the more truly, settle on erroneous choices. In this manner, how to distinguish and maintain a strategic distance from BLA is of awesome criticalness for security in WSNs. There is much research on dark opening assaults. In any case, the present trust-based course systems confront some trying issues. (1) The center of a trust course lies in getting trust. Be that as it may, getting the trust of a hub is exceptionally troublesome, and how it should be possible is as yet vague. (2) Energy proficiency. Since vitality is exceptionally restricted in WSNs, in most research, the trust obtaining and dissemination have high vitality utilization, which genuinely influences the system lifetime. (3) Security. Since it is hard to find malignant hubs, the security course is as yet a testing issue.

3.1 DISADVANTAGES OF EXISTING SYSTEM

The arrange settles on choices relying upon the hubs' detected information, the result is that the system will totally come up short and, all the more truly, settle on mistaken choices

4. PROPOSED SYSTEM

In this paper we propose security and trust directing through a dynamic recognition course convention. The most gigantic refinement among ActiveTrust and past research is that we make various area courses in zones with store essentialness; in light of the way that the attacker doesn't think about recognizable proof courses, it will ambush these courses and, in this way, be revealed. Thusly, the attacker's direct and territory, and furthermore nodal trust, can be procured and used to avoid dull openings while getting ready honest to goodness data courses. To the best of our understanding, this is the foremost proposed dynamic acknowledgment segment in WSNs.

4.1 ADVANTAGES OF PROPOSED SYSTEM:

- The ActiveTrust conspire is the main directing plan that utilizes dynamic identification steering to address Blockhole assaults (BLA)
The ActiveTrust course convention has better vitality effectiveness
The ActiveTrust plot has better security execution

4.2 MODULES DESCRIPTION:

4.2.1 DETECTION ROUTE

An identification course alludes to a course without information parcels whose objective is to persuade the enemy to dispatch an assault so the framework can distinguish the assault conduct and after that stamp the dark opening area.

4.2.2 DATA ROUTING

The information directing alludes to the procedure of nodal information steering to the sink. The directing convention is like regular steering conventions in WSNs; the distinction is that the course will choose a hub with high trust for the following jump to keep away from dark openings and in this manner enhance the achievement proportion of achieving the sink.

5. WORKING PRINCIPLE

In this paper, we have proposed a novel security and trust directing plan in light of dynamic discovery, and it has the accompanying superb properties: High fruitful steering,
- The Active Trust plan can rapidly identify the nodal trust and afterward maintain a strategic distance from suspicious hubs to rapidly accomplish an almost 100% fruitful directing likelihood High vitality proficiency.
- The Active Trust plot completely utilizes buildup vitality to develop different discovery courses.
- The hypothetical examination and exploratory outcomes have demonstrated that our plan enhances the effective steering likelihood by in excess of 3 times, up to 10 times at times.

Be that as it may, the present trust-based course methodologies look in getting trust. Be that as it may, acquiring the trust of a hub is exceptionally troublesome, and how it should be possible is as yet hazy. Vitality proficiency. Since vitality is extremely restricted in WSNs, in most research, the trust securing and dispersion have high vitality utilization, which truly influences the system lifetime. (3) Security. Since it is hard to find noxious hubs, the security course is as yet a testing issue. Accordingly, there are still issues deserving of further investigation. Security and trust steering through a dynamic discovery course convention is proposed in this paper.

The essential advancements are according to the accompanying. The Active Trust plot is showed up in the principle coordinating arrangement that uses dynamic acknowledgment directing to address BLA. The most immense differentiation between Active Trust and past research is that we make distinctive disclosure courses in districts with development imperativeness; in light of the fact that the attacker doesn't think about acknowledgment courses, it will ambush these courses and, in this way, be revealed. Thusly, the assailant's direct and territory, and furthermore nodal trust, can be gained and used to avoid dim openings while getting ready certified data courses. To the best of our understanding, this is the central proposed dynamic acknowledgment instrument in WSNs.

The Active Trust course convention has better vitality proficiency. Vitality is valuable in WSNs, and there will be more vitality utilization if dynamic identification is prepared. Accordingly, in past research, it was difficult to envision embracing such high-vitality utilization dynamic location courses. Nonetheless, we think that its conceivable after precisely examining the vitality utilization in WSNs. Research has noticed that there is still up to 90% buildup vitality in WSNs when the system has passed on due to the "vitality gap" wonder. Thusly, the Active Trust plot takes full favorable position of the deposit vitality to make identification courses and endeavors to
diminish vitality utilization in hotspots (to enhance arrange lifetime). Those location courses can identify the nodal trust without diminishing lifetime and consequently enhance the system security. As indicated by hypothetical examination and test comes about, the vitality effectiveness of the Active Trust conspire is enhanced in excess of 2 times contrasted with past directing plans, including briefest steering, multi-way directing. The Active Trust conspire has better security execution. Contrasted and past research, nodal trust can be acquired in Active Trust. The course is made by the accompanying standard.

Table 1. Performance of algorithm

| Algorithm | Malicious node is in the middle of the route | Destination node is a malicious node | Malicious node is identified but with major loss of packets | Malicious node is identified and change of route occurs (proposed system) |
|-----------|-------------------------------------------|------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------|
| Packets sent | 155                                      | 155                               | 155                                                      | 155                                                                 |
| Packets Received | 57                                       | 0                                 | 95                                                       | 134                                                                 |
| Packet Loss | 98                                       | 155                               | 57                                                       | 21                                                                  |
| PDF       | 36.77                                     | 0.00                              | 63.22                                                    | 86.45                                                               |
| End to End Delay(s) | 1.290                                   | 2.025                            | 0.861                                                    | 0.637                                                               |

To start with, pick hubs with high trust to stay away from potential assault, and afterward course along an effective identification course. Through the above approach, the system security can be made strides. Through our broad hypothetical investigation and recreation examine, the Active Trust steering plan proposed in this paper can enhance the achievement directing likelihood by 1.5 times to 6 times and the vitality productivity by in excess of 2 times contrasted and that of past looks into.

Figure 2. Malicious node

The above graph refers to the first row of the table, in this case, the malicious node is in between the source and destination nodes. The malicious node drops packets very frequently and sometimes send to its neighbour node after the storage of the node capacity.
Figure 3. Malicious Send
The above graph refers to the second row of the table, in this case, the malicious sends the request to the source node and source node sends all the data packets to the fake destination.

Figure 4. Malicious source node
The above graph refers to the third row of the table, in this case, the malicious node is identified by the source node and takes another path to the destination node, but there will be so much of delay in the route selection, so some of the packets will be dropped.

Figure 5. Malicious source identify
The above graph refers to the fourth row of the table. In this case, the malicious node is identified by the source node and takes another path to the destination node, it also checks the trust on the neighbour node to which it has to send the data packets.

Figure 6. Comparison of nodes

The above graph gives the comparison between the existing systems and our proposed system. The yellow color represents the proposed system, it shows that the packet delivery fraction is high and the end to end delay is very less i.e., 0.637 sec (approx.).

6. CONCLUSION

In this paper, we have proposed a novel security and trust directing plan in view of dynamic identification, and it has the accompanying superb properties: high fruitful steering likelihood, security and adaptability. The Active Trust plan can rapidly distinguish the nodal trust and afterward maintain a strategic distance from suspicious hubs to rapidly accomplish an almost 100% fruitful directing likelihood. High vitality proficiency. The Active Trust conspire completely utilizes deposit vitality to develop different identification courses. The hypothetical examination and trial comes about have demonstrated that our plan enhances the fruitful steering likelihood by in excess of 3 times, up to 10 times sometimes. Further, our plan enhances both the vitality productivity and the system security execution. It has imperative importance for remote sensor arrange security.

REFERENCES

[1] Anbuchelian, Selvamani. K, Chandarasekar. A “An EnergyEfficient Multipath Routing Scheme by Preventing Threats in Wireless Sensor Networks”, Electrical and Computer Engineering (CCECE), IEEE 27th Canadian Conference, 2014.
[2] Kumar, M.K., Surya, J., Kumar, V.G.S., Karthikeyan, S."Online prediction of driver distraction based on brain waves activity patterns", International Journal of Pure and Applied Mathematics, Volume 117 No. 21 2017, PP: 139-146
[3] Larisha Rayen, B., Monica, B., Karthikeyan, S., Sivakumar, V.G.," Multi-band circularly polarized antenna for 2.4/5.3/5.8 ghz WLAN and 3.5 ghz WI-MAX applications", Journal of Advanced Research in Dynamical and Control Systems, 2017, vol. No:16, PP: 1311-1322
[3] Liu A, M. Dong, K. Ota, and J. Long, "PHACK: An efficient scheme for selective forwarding attack detection in WSNs," Sensors, vol. 15, no. 12, pp. 30942–30963, 2015.
[4] Lou W, W. Liu, Y. Fang, “SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004
[5] Savitha.G and S.Karthikeyan, "Effective cellular transmission in software defined radio", ARPN journal of Engineering and Applied Science, Vol.11, no.22, November 2016, PP: 12675-12680.
[6] Merin Mary Koshy and S. Karthikeyan, "A survey on advanced technology for communication between deaf/dumb people using eye blink sensor & flex sensor", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIECS), IEEE Explorer conference PP:

[7] Balaji and S. Karthikeyan, "A survey on moving object tracking system using Image Processing", 11th international conference on Intelligent systems and control, IEEE explorer conference, vol., Jan 2017, PP: 11-16.

[8] Mayan J.A, Arifa S, Pavithra R, "Semantic based multi lexical ranking technique for an effective search in protected cloud", 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumarakoil, 2016, pp. 570-576.

[9] Gopika. S. Kumar, S. Karthikeyan and N. Ambily, “A Metaphorical Scrutiny in Banishing Salt and Pepper Noise”, BIO SCIENCES BIOTECHNOLOGY RESEARCH ASIA, December 2014 Vol. 11(3).

[10] G. Karudaiyar, S. Karthikeyan and B. Sainath, “Encryption and Decryption Scheme by Using Finite State Machine”, BIO SCIENCES BIOTECHNOLOGY RESEARCH ASIA, December 2014 Vol. 11(3), 1867-1872.

[11] S. Karthikeyan, S. Jayashri, “Energy Utilization Strategies using Novel Approach in Wireless Sensor Networks”, International Conference on Software Engineering and Mobile Application Modelling and Development, Dec 2012, pp: 1-5.

[12] S. Karthikeyan, S. Jayashri, “Energy Efficient System for Heterogeneous Wireless sensor Networks”, European Journal of Scientific Research, Volume 72, No 4 march 2012, PP: 599-607. ISSN: 1450-216X.

[13] S. Karthikeyan, S. Shanmugapriya and S. Jayashri, "Sub-head Transmission of Heterogeneous Data by Cloned Agent to Android Mobile", Research Journal of Applied Sciences, Engineering and Technology, 8(1):pp.24-34, 2014

[14] S. Pavithra, S. Karthikeyan, V. J. K. KishorSonti, S. Jayashri, "Competent Realization of Co-operative spectrum sensing in cognitive radio systems", International journal of Engineering systems modeling and simulation, Inder science publishers, Vol. 7, No. 2,pp 103-110 2015. (FREE JOURNAL)

[15] K. Bharathi, S. Karthikeyan, “A Novel Implementation of Image Segmentation for Extracting Abnormal Images in Medical Image Applications”, Indian Journal of Science and Technology, Vol. 8(8S), 333–340, April 2015.

[16] Asha P, Albert Mayan J, Canessane A (2018), "Efficient Mining of Positive and Negative Itemsets Using K-Means Clustering to Access the Risk of Cancer Patients", Communications in Computer and Information Science, ICSCS 2018, Kollam, 2018, pp:373-382.

[17] S. Karthikeyan, “Ontogeny Smart Bulletin Board”, ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, Vol. 10, No. 5, pp. 2148-2151, March 2015.

[18] R. Themnozhi, S. Karthikeyan, “An Efficient Parallel Architecture in Design and Implementation of Adaptive LMS Algorithm”, ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, Vol. 10, NO. 7, pp 3150-3153, April 2015.

[19] J. Nandhini, K. Shabatini, S. Karthikeyan, “Wireless Colour Sensing Arm Robot”, International Conference on Robotics, Automation, Control and Embedded Systems – RACE, ISBN: 978-81-925974-3–0, PP: 1065-1071, February 2015.

[20] Albert Mayan J, Anto Praveena M D, Telkar Bharath Rao, Uravakonda Uday Sagar (2018), "Optimized test data generation over suspicious implementation of oracle problem", IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSE-2017), pp:2559-2563.

[21] D. Angeline Deborah Monica, S. Karthikeyan and V. Brindini, "Source and destination anonymity using end-to-end anonymous addressing scheme in wsn", ARPN Journal of Engineering and Applied Sciences, August 2015, Vol 10, No 14, PP: 5778-5783.

[22] R. Ananth S. Karthikeyan, "Dual Cluster Head Algorithm For Proficient Routing In Wireless Sensor Networks", Indian Journal of Science and Technology, Vol 9(43), November 2016, PP: 1-7.

[23] M. Tamilselvi, S. Karthikeyan, "A Literature Survey In Face Recognition Techniques", International Journal of Pure and Applied Mathematics Volume 118 No. 16 2018, PP: 831-849
[24] Bagavath sri and S. Karthikeyan, "Secure Elliptic Curve Cryptography Based RFID Schemes for Internet of Things", Indian Journal of Science and Technology Vol 9(42), November 2016 PP: 1-5.
[25] Brij Bhushan Ojha, S.Karthikeyan ,"Design of an interconnection network using VLSI photonics: Issues and challenges " International Journal of Pure and Applied Mathematics, Volume 118 No. 17 2018, PP: 211-224
[26] S. Vimalsree and S. Karthikeyan, "A Low Power Multibit Flip Flop Merging Technique Using WSN Nodes", ARPN, vol. no:11, No.15, August 2016, Page no: 9358-9363.
[27] Usha Nandini , Saravanan M , Albert Mayan J , Murari Devakannan Kamlesh , Mohana Prasad K (2018) , " Automatic traffic control system using PCA based approach", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017),pp.2387-2392.