

Secure Data Transmission Framework for Internet of Things based on Oil Spill Detection Application

Abhijith H V¹

Department of Information Science and Engineering
Sai Vidya Institute of Technology, affiliated to
Visvesvaraya Technological University
Bangalore, India

Dr. H S Rameshbabu²

Department of Computer Science and Engineering
Sai Vidya Institute of Technology, affiliated to
Visvesvaraya Technological University
Bangalore, India

Abstract—Internet of Things (IoT) is a leading technology which can interlink anything to Internet and makes everything to intelligent and smart. IoT is not just a single technology. IoT is a combination of various technologies like communication, data analytics, sensors and actuators, cloud computing, artificial intelligence, machine learning, etc. Applications of IoT are spread across various domains. IoT is most suitable for remote applications like underwater networks. One such application is oil spill detection in ocean. Oil spill in an ocean is a critical challenge that causes damages to marine ecosystem. Detection of oil spills in a real time manner helps to resolve the problem quickly to minimize the damage. IoT can be used to detect the oil spill by making use of sensors deployed at various locations of ocean. With a massive amount of sensors deployed and the huge amount of data associated with it, there remain concerns about the data management. Also amount of data generated in IoT based remote sensing network is usually enormous for the servers to process and many times data generated are redundant. Hence there is a need for designing a framework which addresses both aggregation of data and security related issues at various aggregation points. In this paper we are proposing a secure data transmission framework for detecting oil spill through IoT, which avoids redundant data transmission through data aggregation and ensures secure data transmission through authentication and light weight encryption.

Keywords—Internet of things; wireless sensor networks; sensor nodes; data aggregation; authentication; light weight cryptography

I. INTRODUCTION

Internet of Things refers to connecting various things to the internet. IoT can be used in wide range of applications. IoT applications include remote applications also. Remote IoT applications include military applications such as surveillance, battle field monitoring etc. Underwater applications such as oil spill detection, analysis of aquatic animals lifecycle, etc. smart farming, forest applications such as fire monitoring etc.

The Application considered in this paper is oil spill detection. Oil spills are caused due to accidents in the ocean, leakage of oil, crude oil or gasoline pipelines. Oil spills are also caused due to negligence of offshore refineries or crude oil rigs. Irrespective of the cause of spill or slick, their effects are the same. Oil forms a separate film on the surface of water and stays there unless physically removed. The oil film causes harm to flora and fauna of the ocean. Detection of leakage in pipes or spillage of oil in accidents takes time and combating

the pollution takes even longer time. The longer the film of oil stays on water surface, the greater is the damage caused to aquatic eco system. Due to the vastness of oceanic surface, application of Internet of Things to sense oil spills is a very practical technological solution. There are underwater robotic submarines available that can be used to deploy sensor nodes at specific locations. Buoyant nodes sense surface conditions and communicate observations to middle level nodes that in turn communicate to nodes on the bed. Levels of hierarchical node deployment allow us to implement intelligent communication of sensed data. Just knowing that oil spill has occurred is of little practical use. Instead if we also know the extent of damage, area of region polluted, some corrective combating tasks can be initialized.

Oil Spill detection is a remote IoT application, which uses resource constrained networks [22]. It includes deployment of many low cost, low power sensing nodes which has capabilities to sense, process and communicate the data. Each sensor nodes has limited transmission range, limited energy, limited processing capabilities and limited memory.

As Sensor nodes are resource constrained devices many nodes are deployed in shorter region. This leads to the sensing of redundant information. Transmitting redundant data will leads to the wastage of energy and other resources. Redundant data transmission can be controlled by data aggregation techniques. There are different data aggregation approaches: In-network data aggregation, Tree based data aggregation, cluster based data aggregation, Grid based data aggregation and hybrid data aggregation. There can be single level or multiple levels of data aggregation [21].

Along with data aggregation we need to consider the importance of secured data transmission. As Oil spill detection uses wireless communication, there remains concern about security. Fault alarm causes lot of damages as oil spill needs to be addressed in real time manner. There is need for simple and strong authentication scheme to identify the nodes identity. Also there is a need of light weight encryption algorithm to be used to secure the data transmission [19].

In this paper we are proposing a secure data transmission framework for oil spill detection applications which involves intelligent data aggregation technique and security mechanism. Proposed approach aggregates the data as well as provides intelligence to nodes to detect whether to send the data or not.

Also our present work add features to detect the boundary of oil spill which helps in identifying intensity of damage. In this paper we are adding simple ID based authentication mechanism to prove the nodes identity. We can use any of the existing lightweight cryptographic algorithm to secure the data communication.

The paper is organized as follows: Related work is given in Section 2, proposed approach is described in Section 3, Section 4 describes the simulation and results, conclusion is provided in Section 5.

II. RELATED WORK

A lot of work has been carried out in detection of oil spills. Pangilinan et.al, have focused on determining the thickness of oil spill. Their hypothesis is that thicker the spill graver the effects of the pollution. They have determined the pixel intensity concerned with many competing parameters [1].

Reem Alattas has also worked on image analysis in oil spill detection. A threshold method is suggested to detect oil spill. SAR image processing is applied based on minimum cross-entropy with gamma distribution. A major drawback of the work is its intrinsic time lapse involved in data analysis. Oil spill like pollution must be combated as quickly as possible. Real time detection, if possible is most suitable for such problems. Additionally, the method proposed in [2] works with bi-modal images that have two classes of pixels only.

A.Gasul et.al [3] have proposed and tested a new method for SAR image analysis to detect oil spills. Their method works well with low resolution and distorted images as well. In spite of multi stages analysis algorithm implemented, ensuring error free end result is still difficult.

Kruti Vyas et.al in [4] have applied feature extraction of SAR images in oil spill detection. They have recognized three independent features for this purpose. They have performed a battery of experiments while considering types of images.

Mario Monteiro et.al, have made an extensive study of various aspects and challenges of detection of oil spills. Their work is particularly in connection with the seagull project. Their contribution is specifically in application of camera fitted unmanned aerial vehicles in combating water pollution. The author in [5] documents various challenges involved in detection of spills, with emphasis on time lapse between actual spill and its detection.

Unmanned surface vehicle is developed and analysed for performance in [6] by Deqing Liu et.al. Their work concentrates on frequent oil spills that happen at harbors, oil rigs and drilling platforms. They have designed a fluorosensor laser detector to achieve this aim. A feasibility analysis is also carried out by the authors.

Md. Shafi.K.T, et.al have developed a simple resonance based application to detect oil spill using planar microwave [7]. Proposed sensor is developed, deployed and tested in their work. The sensor designed is capable of detecting pollution beyond 5%.

There are different traditional data aggregation mechanisms, they are flat based [8][9][10] and hierarchical approaches.

In flat approach, the base station transmits a query requesting for a data from the sensing nodes within the area. The nodes which have relevant sensed information to the query sent will respond back. In this method base station performs excessive computations and communications. Because of this, if the base station fails, then network connection will be lost with the outer world.

Under hierarchical approach, many techniques have been proposed for energy efficiency and scalability. There are four types of hierarchical approach they are the cluster based data aggregation [11][12], tree based data aggregation [13], the grid based data aggregation [14], and the chain based data aggregation [15][16].

These traditional data aggregation schemes will just combine the data from multiple sources and forward it to next node. In majority of applications normal data aggregation is not sufficient. We need to add some intelligence to the data aggregation and data transmission process within the limits of constrained resources.

J. Chen, S. Kher, and A. Somani, et al. proposed a scheme in [15] which involves Majority Voting. This approach is a data outlier detection method based on spatial correlation. Here if a reading of local sensor node is different from majority of its neighbouring nodes, then it will be classified as abnormal.

Y. Sun, H. Luo, and S. K. Das et al. proposed a scheme in [16]. Here according to the trustworthiness ranked by comparison with historical data and neighbour data, Weight will be assigned to every sensor data. Then weighted mean value will be calculated at the aggregator. This will be considered as the aggregated data.

S. Din, A. Ahmad, et al. proposed a scheme in [17], where the nodes closer to sink node performs direct communication and remains unclustered, the nodes which are one-hop away from the sink node perform multi-hop communication, and remains clustered.

Bo Yin et. al. in [18] specified a Tree based scheme which Involves construction of aggregation tree for complex queries. This ensures minimum communication cost.

S. Kumar and V. K. Chaurasiya et all in [20] proposes a scheme, where data Mining techniques are used to generate more accurate, consistent and useful information than that generated by any individual sensor node.

There exists different lightweight cryptographic techniques like AES [23], HEIGHT [24], PRESENT [25], DESLX [26], RSA [27] etc.

III. PROPOSED WORK

A. Architectural Setup and Assumptions

Following are the assumptions made in deployment of nodes in the test bed.

1) Grid based deployment of nodes: to specifically determine location of each individual node. This assumption is safe and valid as, there is a commercially available underwater robot capable of deploying nodes at specific coordinates of latitude and longitude.

2) Number of nodes per grid is fixed: this assumption helps us compute statistically significant results after data collection are done and analysis is to be performed.

3) Node density is uniform: non-uniform node deployment does not allow implementation of intelligence.

4) Each node in a grid represents a single unit area: data collected is representative of a fixed area under surveillance.

5) 4 unit squares form a cell: helps in aggregation of data across levels of nodal deployment.

6) Every cell has a cell-sink node: this is an architectural requirement of WSN.

7) Four cells combine to form a level 2-cell: helps implement the second layer of intelligence and additional aggregation.

8) One of the unit cell's cell-sink also works as a sink for four adjacent level-2 cells: based on energy levels, a suitable cell-sink is elected as the sink of adjacent cells.

9) All level-2 cells combine to form the region under observation: highest level of aggregation implemented under our scheme.

10) Each node will communicate the observation only if the quantity observed is above a fixed threshold.

B. Node Deployment Phase and Network Establishment

1) Four different levels of nodes are deployed.

- Ground level sensor nodes: They are capable of sensing the oil density at the preliminary level and intensity of light.
- High power node at the ground level: They act like grid head they can also sense the information.
- Anchor nodes at middle level: They act like second level grid head. They gather the data from multiple grids and transfer it to surface buoyant node.
- Surface buoyant node: They are at the surface level, they can sense the PH level of the water.

2) These nodes are deployed at the required locations using an underwater automatic vehicle (UWAV).

3) The area of interest is divided into equal sized grids. Ground level nodes and high power nodes are deployed at each grid. High power node will be the grid head of that particular grid.

4) Each High power node broadcast a beacon message to the ground level sensor node to indicate its presence in the grid.

5) Each ground level nodes respond back to their grid heads by sending the response beacon. Same Procedure is followed between grid heads and anchor nodes, Anchor nodes and surface buoyant nodes.

Fig. 1 shows the network architecture used in the proposed scheme.

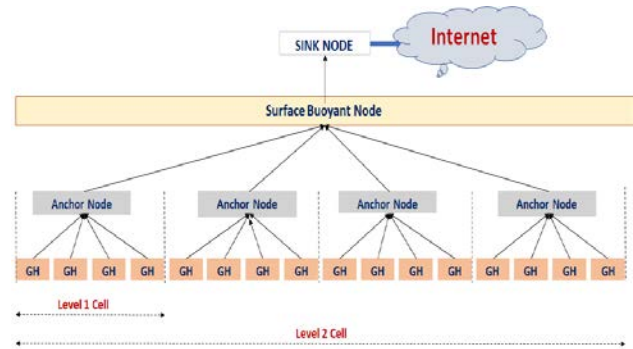


Fig. 1. Network Architecture.

C. Routing and Aggregation Phase

1) All the ground level sensor nodes sense the data and send the sensed data to its Grid head. Grid head aggregates the received data.

2) Grid Head adopts Spatial aggregation: based on the percentage of area generating similar readings. Each unit cell has a designated high power node acting as cell-sink. Communicate reading only if at least three out of four nodes report similar readings.

3) Grid Head sends data to Anchor node. Anchor node aggregates the data. Anchor node also adopts spatial Aggregation.

4) Anchor nodes send the aggregated data to surface buoyant node. Surface buoyant node aggregates and sends the data received as well as PH information to sink.

5) Surface buoyant node adopts Boundary value aggregation: region under observation has a sink node that acts as a data aggregator. Radial survey is made periodically at three lengths of radii- minimum, nominal and maximum. Minimum is close to the sink, maximum is distance from sink to boundary of region under observation, and nominal is an intermediate distance.

D. Boundary Detection

In the proposed system, a coordinate table is created. This table is a list data structure that stores coordinates of each node in the IOT infrastructure. Each entry consists of x, y and x coordinate values stored in an indexed linear linked list. An additional field stored data communicated from the sensor node.

Aggregation as well as intelligence is applied at middle level nodes and at bed nodes respectively. Boundary determination is implemented in the following steps:

1) Search the list of nodes and segregate nodes that have updated sensed data.

2) Perform a sequential search among the segregated nodes to determine nodes with maximum positive and negative coordinates of x, y and x.

3) Step 2 gives probable boundary nodes, compare their observed data with neighbor nodes to determine actual boundary nodes.

4) Communicate boundary coordinates.

5) Rate of spread is determined by calculating $(a_2 - a_1)/t$, where a_2 is the new area of oil spill after elapse of time unit t , a_1 is the previously computed area of oil spread, i.e. before the elapse of time t .

E. Security

Assumptions

1) Grid Head, Anchor node, Surface buoyant nodes are considered as aggregator nodes.

2) Ground level sensor nodes are subordinate nodes for Grid heads, Grid heads are subordinate nodes for anchor node and anchor nodes are subordinate nodes for surface buoyant nodes.

3) Every ground level sensor node and other subordinate nodes maintains the following in its memory.

a) A pre shared Secret key shared with its aggregator node (Grid Head, Anchor node, Surface buoyant node).

b) A pre shared secret information (used for Authentication) shared with aggregator node.

4) Every aggregator node maintains the following in its memory.

- a) Subordinate node ID.
- b) Pre Shared Secret Key for encryption and decryption.
- c) Pre shared Secret Info for authentication.

Table I shows the Secret information repository format maintained by nodes. Fig. 2 shows the security architectural setup followed in the network.

TABLE I. SECRET INFORMATION REPOSITORY

Node ID	Key (Secret key shared with subordinate node)	Secret Info (Pre Shared Secret Information used for authentication)

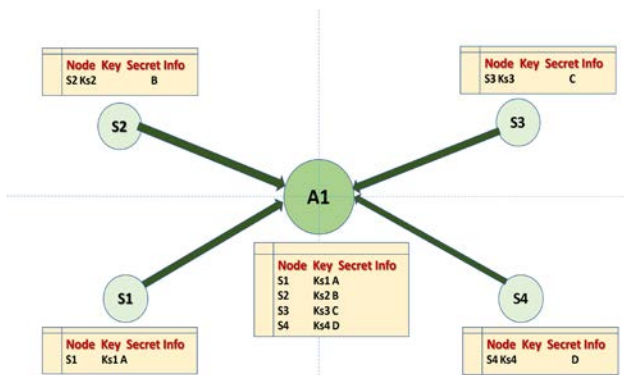


Fig. 2. Security Architectural Setup.

Authentication Scheme:

Sender Side:

Fig. 3 shows the authentication and encryption procedure adopted by sender node.

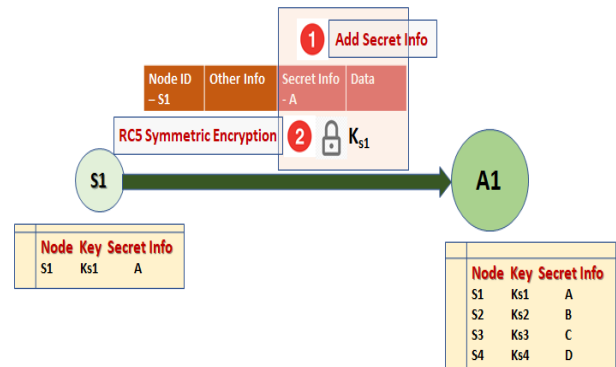


Fig. 3. Sender Side Authentication Procedure.

Pre shared secret info A will be prefixed to the data.

Secret Info and the Data will be encrypted using pre shared secret key.

Receiver Side:

Fig. 4 shows the authentication and encryption procedure adopted by receiver node.

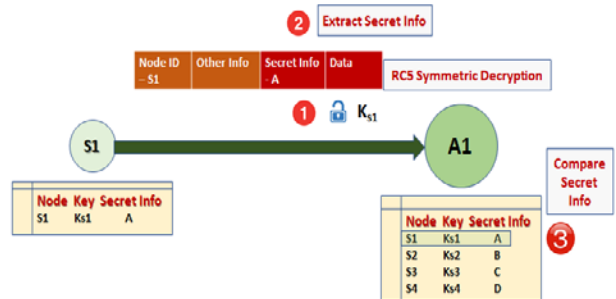


Fig. 4. Receiver Side Authentication Procedure.

Received packet will be decrypted using Pre share secret key.

Secret information A will be taken from the header

Node ID and Secret information will be compared with the key repository stored at the aggregator node to prove the authenticity.

Encryption Scheme:

Any Light weight cryptographic scheme can be used to encrypt the data and secret Info at sender side. The list of popular light weight cryptographic algorithms and its comparisons are given in Table II [28]:

TABLE II. LIGHT WEIGHT CRYPTOGRAPHY TECHNIQUES

Light weight Cryptographic scheme	No. of Rounds	Block Size (bits)	Key Size (bits)	Structure
AES	10/ 12/ 14	128	128/192/256	SPN
HEIGHT	32	64	128	GFS
PRESENT	31	64	80/128	SPN
LEA	24/28/32	128	128/192/256	Feistel
TEA	64	64	128	Feistel
RC5	1-255	32/64/128	0-2040	Feistel
DESL	16	64	54	Feistel
Hummingbird	4	16	256	SPN

IV. SIMULATION AND RESULTS

MATLAB is used as the simulation tool to check the efficiency of proposed work. Initially area of interest with dimensions 800m (length) x 800m (breadth) x 800m (depth) is considered. Then the volume under consideration is divided into equal sized grids of size 50m each at ground level. Table III shows the various parameters used in simulation. Fig. 5 depicts the 3 dimension test bed created through simulation and Fig. 6 shows Grid layout in 2 Dimension. Here blue color nodes represent nodes deployed at ground level. Red color nodes represent anchor nodes and the magenta color nodes indicate nodes that are buoyant on oceanic surface.

TABLE III. SIMULATION PARAMETERS

Parameter Type	Parameter Value
Area of application region	800 X 800 m ²
Sea Depth	800 m
Grid range	100 m
Number of Ground level node in each grid	4
Number of High power nodes in each grids	2
Number of Anchor node in each group of grids	1
Number of Surface buoyant nodes in each group of grids	1
Simulation Time	150sec
Payload length	512 Bytes
Parameters of Ground level node	
Initial Energy	4J
Transmission range	20m
Data rate	4kbps
Parameters of High power node	
Initial Energy	7J
Transmission range	25m
Data rate	6kbps
Parameters of Anchor node	
Initial Energy	10J
Transmission range	30m
Data rate	8kbps
Parameters of Surface buoyant node	
Initial Energy	14J
Transmission range	35m
Data rate	12kbps

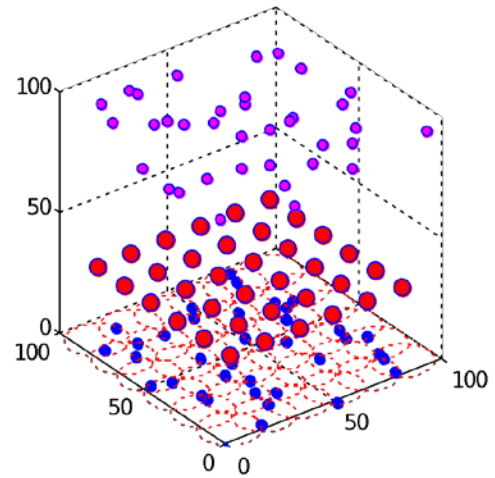


Fig. 5. 3-Dimension Test Bed.

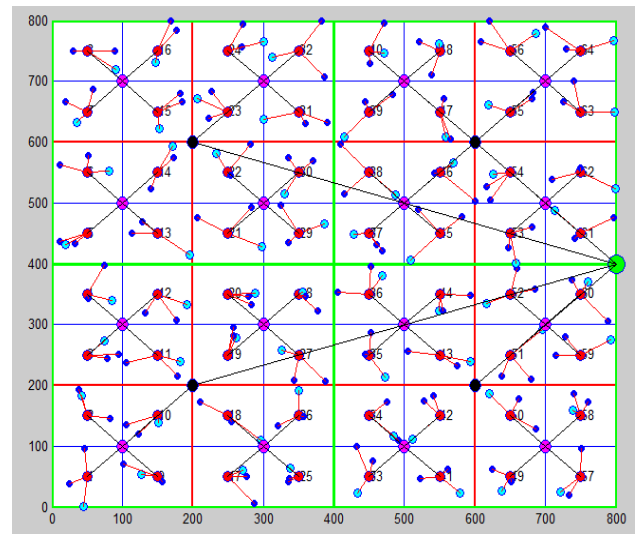


Fig. 6. Grid Layout.

Fig. 7 shows amount of time required to detect the oil spill versus the oil spread area. Time required to detect spills of larger area is evidently greater. From this we can analyse the spreading rate of oil in the water and intensity of oil leakage. As underwater communication is slower than normal environment redundant information transmission can be reduced to ensure the timely delivery of information and to avoid collision in the network Figure 8 helps us understand that the number of redundant transmission in various techniques compared with proposed work are much greater. Proposed method requires lesser number of packet transmissions compared to without aggregation deployment, in-network architecture and cluster based approach. It is clear that proposed work reduces redundant data transmission significantly.

The performance of various lightweight cryptographic techniques is shown in Table IV. Based on this suitable technique can be adopted [28].

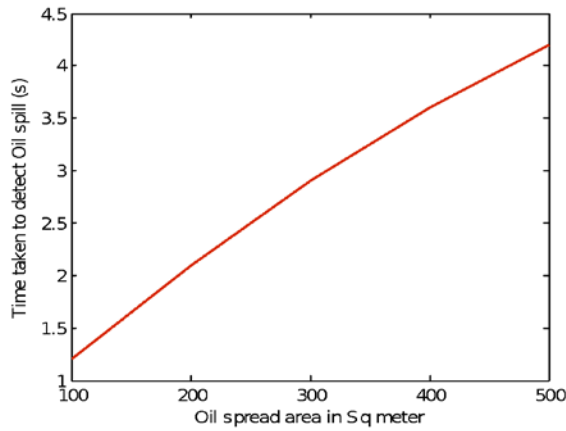


Fig. 7. Time Required for Detecting the Spreading of Oil Leakage.

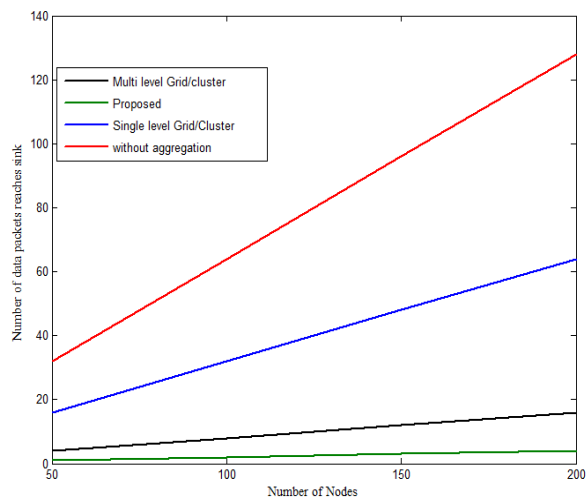


Fig. 8. Number of Redundant Transmission in Various Approaches.

TABLE IV. PERFORMANCE OF VARIOUS LIGHT WEIGHT CRYPTOGRAPHY TECHNIQUES

Light weight Cryptographic scheme	Flash Memory (in Bytes)	Cycles (Encryption)	Cycles (Decryption)
AES	3410	3766	4558
HEIGHT	5672	2449	2449
TEA	1140	6271	6299
DESL	3098	8365	7885

V. CONCLUSION

Adding intelligence to oil spill detection makes detection real-time and provides insight in to combating the pollution in the future. Collecting raw data triggered by an event gives minimal insight into crucial facts like thickness of oil film, expanse of oil spill and also reduces number of redundant transmissions. By detecting the boundary of oil spill we can easily predict the intensity of oil spread in the sea. This enables faster remedial actions. Also proposed methods eliminate the redundant data transmission through the spatial and boundary value aggregation. Proposed method secures the data transmission by adopting simple ID based authentication and

existing light weight cryptography techniques. Adding intelligence to sensor nodes to make decision on oil spill can be considered for future enhancement.

REFERENCES

- [1] M. N. Pangilinan, R. Anacan and R. Garcia, "Design and Development of an Oil Spill detection and Transmission System Using Artificial Illumination Using LEDs," 2016 7th International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Bangkok, 2016, pp. 407-412, doi: 10.1109/ISMS.2016.61.
- [2] Reem Alattas, "Oil Spill Detection in SAR Images Using Minimum Cross-Entropy Thresholding", 7th International Congress on Image and Signal Processing, IEEE 2017.
- [3] A. Gasull, X. Fábregas, J. Jiménez, F. Marqués, V. Moreno and M. A. Herrero, "Oil spills detection in SAR images using mathematical morphology," 2002 11th European Signal Processing Conference, Toulouse, France, 2002, pp. 1-4.
- [4] Kruti Vyas, Pooja Shah, Usha Patel, Tanish Zaveri, Rajkumar, "Oil spill detection from SAR image data for remote monitoring of marine pollution using light weight imageJ implementation", 5th Nirma University International Conference on Engineering (NUiCONE), IEEE 2015.
- [5] M. M. Marques et al., "Oil spills detection: Challenges addressed in the scope of the SEAGULL project," OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, USA, 2016, pp. 1-6, doi: 10.1109/OCEANS.2016.7761019.
- [6] Deqing Liu, Xiaoning Luan, Feng Zhang, Jiucui Jin, Jinjia Guo, Ronger Zheng, "An USV-based Laser Fluorosensor for Oil Spill Detection", Tenth International Conference on Sensing Technology, IEEE 2016.
- [7] Muhammed Shafi K. T., Nilesh Kumar Tiwari, Abhishek Kumar Jha, and M. Jaleel Akhtar, " Microwave Planar Resonant Sensor for Detection of Oil spills", IEEE, 2016J.Kulik.W.R.Heinzlman & H.Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", WirelessNetwork, Vol 8, Mar-2002, pp.169-185.
- [8] C.Intanagonwivat,R.Govindan and D.Estrin, "Directed Diffusion: A Scalable and robust communication paradigm for sensor networks", 6th annual international conference on mobile-computing and networking, Aug-2000.
- [9] B.Krishnamachari and J.Heidemann, "Application specific modeling of information routing in wireless sensor networks", IEEE international performance, computing, communications conference, Vol-23, pp.717-722, 2004.
- [10] W.R Heinzelman, "Application-specific protocol architectures for wireless networks", PhD-Thesis, MIT, June-2000.
- [11] O.Younis and S.Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks" IEEE transactions on mobile computing, Vol-3, Dec-2004,pp.366-79.
- [12] Lindsey,S, Raghavendra,C, "PEGASIS Power-efficient Gathering in sensor Information system", IEEE Aerospace Conference 2002, pp-1125- 1130.
- [13] Y. Sun, H. Luo, and S. K. Das, "A Trust-based Framework for FaultTolerant Data Aggregation in Wireless Multimedia Sensor Networks," IEEE Trans. Depend. Sec. Comput., 2017.
- [14] J. Chen, S. Kher, and A. Somani, "Distributed Fault Detection of Wireless Sensor Networks" ACM Workshop on Dependability Issues in Wireless Ad-hoc Sensor Netw. 2017.
- [15] Kuong-Ho-Chen, Jyh-Ming-Huang, Chieh-Chuan-Hsiao "CHIRON: An Energy-Efficient Chain-Based Hierarchical Routing Protocol in Wireless Sensor Networks", IEEE. 2009.
- [16] Liyang-Yu, Neng-Wang, Wei-Zhang, Chunlei-Zheng, "GROUP: a Gridclustering Routing Protocol for Wireless Sensor Networks", 2006 IEEE International conference on wireless-communication networking & mobile-computing, china 2006.
- [17] S. Din, A. Ahmad, A. Paul, M. M. U. Rathore, and J. Gwanggil, "A cluster based data fusion technique to analyze big data in wireless multi-sensor system," IEEE Access, vol. 5, pp. 50690 5083, 2017.

- [18] Bo Yin et. all. "Communication-Efficient Data Aggregation Tree Construction for Complex Queries in IoT Applications", IEEE INTERNET OF THINGS JOURNAL, 2018.
- [19] Xiong Li et. all. "Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications", IEEE INTERNET OF THINGS JOURNAL, 2018.
- [20] S. Kumar and V. K. Chaurasiya, "A Strategy for Elimination of Data Redundancy in Internet of Things (IoT) Based Wireless Sensor Network (WSN)," in IEEE Systems Journal 2018.
- [21] Abhijith H V, & Sindhu M P. (2015). Energy efficient multilevel hierarchical data aggregation mechanism for wireless sensor networks. 2015 IEEE International Advance Computing Conference (IACC). doi:10.1109/iadcc.2015.7154688.
- [22] H.V., Abhijith and Raj, S. Deepak and Babu, H. S. Ramesh, Intelligent Boundary Determination of Oil Spill Detection Using IOT (April 21, 2018). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018, Available at SSRN: <https://ssrn.com/abstract=3167315> or <http://dx.doi.org/10.2139/ssrn.3167315>.
- [23] Ahmed, E.G., Shaaban, E. and Hashem, M. "Lightweight mix columns implementation for AES." In Proceedings of the 9th WSEAS international conference on Applied informatics and communications, pp. 253- 258. 2009.
- [24] Leander, G., Paar, C., Poschmann, A. and Schramm, K. "New lightweight DES variants." In International Workshop on Fast Software Encryption, pp. 196-210. Springer, Berlin, Heidelberg, 2007.
- [25] Jana, S., Bhaumik, J. and Maiti, M.K. "Survey on lightweight block cipher." International Journal of Soft Computing and Engineering 3 (2013): 183-187.
- [26] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C. "PRESENT: An ultra-lightweight.
- [27] Tawalbeh, L. A. A., & Sweidan, S. (2010). Hardware design and implementation of ElGamal public-key cryptography algorithm. Information Security Journal: A Global Perspective, 19(5), 243-252.
- [28] Sohel Rana, Saddam Hossain, Hasan Imam Shoun and Dr. Mohammad Abul Kashem, "An Effective Lightweight Cryptographic Algorithm to Secure Resource-Constrained Devices" International Journal of Advanced Computer Science and Applications(IJACSA), 9(11), 2018. <http://dx.doi.org/10.14569/IJACSA.2018.091137>.