Journal of Theoretical and Applied Information Technology
15th February 2022. Vol.100. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MALICIOUS ATTACK ALLEVIATION USING IMPROVED TIME-BASED DIMENSIONAL TRAFFIC PATTERN GENERATION IN UWSN

T. SARAVANAN[1], S. SARAVANAKUMAR[2], GOPAL RATHINAM[3], M. NARAYANAN[4], T. POONGOTHAI[5], P. SANTOSH KUMAR PATRA[6], SUDHAKAR SENGAN[7]

[1,2]Associate Professor, St.Martin's Engineering College, Department Of Cse, Secunderabad, India

[3]Professor, University Of Buraimai, Department Of Information And Communication Engineering, Al Buraimi, Oman

[4,5,6]Professor, St.Martin's Engineering College, Department Of Cse, Secunderabad, India

[7]Professor, Psn College Of Engineering And Technology, Department Of Cse, Tirunelveli, India

E-mail: [1]tsaravcse@gmail.com, [2]saravanakumarme85@gmail.com, [3]gopal.r@uob.edu.om, [4]narayanan_baba@yahoo.com, [5]poongothait@gmail.com, [6]drpskpatra@gmail.com, [7]sudhasengan@gmail.com

ABSTRACT

A group of permanent and movable submarine electromagnetic clusters make up the submarine network components. The architecture may change back and forth through time depending on the methodological perspective and the diverse application demands. The majority of researchers have been using constellation architectural networks in current history. In such a networks, the cluster head gathers and delivers intra-cluster and cross - functional and cross data packets. Clustering leaders are chosen energy is a measure of the remaining node, the ideal quantity of Member Nodes, and electricity usage. The choice of cluster head minimizes power consumption and extends the longevity of the lifespan connection. Any form of show's primary issue is protection. Demand of Service (DoS) attacks can impact underwater wireless sensing (UWSNs) despite if they are implemented using modern techniques. As an outcome of these attacks, collaboration connectivity nodes are disrupted, and the program's capacity is reduced. Destructive attacks, often known as denial-of-service (DoS) operations, can be carried in a variety of methods that are not available in plenty of other communications links. These can be initiated at any point in the transport ward's hierarchy. Even if UWSNs are all well by encryption techniques, Attacks can always be a hazard. In this regard, we propose the primary goal of Improved Time-based Dimensional Malicious Alleviation (ITDMA) to safeguard against DoS attacks when directing at the protocol stack. We used the Deep Insight approach to convert numerical features into standard regarding in this investigation. The input data was then classified as malicious actions using these properties in a proposed bi-level classification system. This research would focus on the gateway node and risk based approach, with a good output in terms of classification accuracies, false positive rate, and capacity.

Keywords: *UWSN, Foraging motion, Alleviation, ITDMA, Network trace and False alarm*

1. INTRODUCTION

WSN (wireless sensor network) is a cutting-edge method of information collecting via dispersed and autonomously nodes. This industry has gained gained increasing attention than ever, owing to its dominance in terms of task scope and affordability. [1] A WSN typically consists of a large number of low-cost, low-power, narrow, number of co various sensors with relatively brief wireless network technologies. The sinker, also known as the access point, has a large production capability, as well as more memory, caching, and analytical power. All information from of the network is sent to the sink through mobile communications channel, and the process is completely self-contained. A predictable UWSN is projected in Fig. 1.

The Underwater Wireless Sensor Network (UWSN) is made up of submerging sensing devices that may be used for activities that aren't possible with current cable

submarine measurement techniques. The established submersible system model classic ways of communicating such as wire for deployments; however, the UWSN has a lot of notable advantages in comparison channel, including marginalisation, ease of application, data relevance, believability, and mass implementation reportage [2]. UWSN has various potential uses, including wave energy measurement, instruments surveillance, and evaporative emissions, owing to its advantages over wired below pumping stations.

The most crucial responsibility for any wireless connection connectivity is to provide cybersecurity. In comparison to traditional home networks, providing wireless networking security is difficult, specifically in devices with low. Because of the substantial BER (bit error rate) throughout broadcast, huge and uneven network latency, and insufficient capacity of ultrasonic sensors and acoustically (sounds) channels, underwater acoustic sensor networks are highly vulnerable to hacking attacks [3]. The exclusive features of the under-water sonar and sound communication channels, and the variances among underwater sensor networks and their water-based peers necessitate the development of proficient and trustworthy security mechanisms.

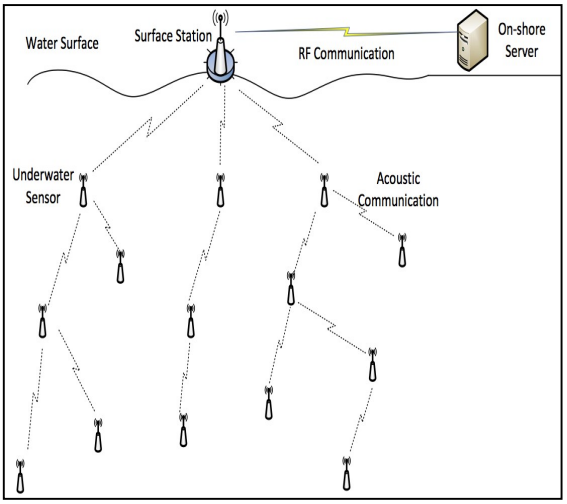

Figure 1: Conceptual view of UWSN

Though the malicious attack can be identified with the help of Time-based dimensional traffic pattern generation in UWSN by various researchers as articulated the various limitations, the literature review explains the ways of possibilities to detect and demolish the malicious attack and the various algorithms and protocols used on the wireless sensor networks.

The proposed an Intrusion Detection System (IDS) using detection of malicious attacks with increased resilientback-propagation. The reported work utilized only the training dataset, performed testing on 70% data, validated 15% data, and tested 15% data. The performance is decreased for testing on unlabeled data.

2. REVIEW OF LITERATURE

Each detector link is connected with the others in the neighborhood via a radio range. One essential need for UWSN is transmission bandwidth, which affects the number of nodes, implementation efficiency, and original planning of the specified monitored region. Submersible IoT systems include two communication modes: acoustic and optical connectivity. Because it is available and necessitates connection over greater distances, underwater sensor wireless systems has been one of most often utilised technologies. Ultrasound waves, on the other contrary, have a number of drawbacks, including diffraction, significant delay due to low propagation velocity, significant components, bandwidths, and negative **impacts on underwater organisms. In order to** improve the volume of auditory transmission, orbital total velocity has recently emerged as a viable multiplexed technique for encrypting data onto vortex streams [4]. Due to the limits of wireless signals, optically waves provide another option. So according [5] contemporary underwater optical communications development is focused on increasing high bandwidth and transmission distance. Laser wavelengths provide a greater data throughput, lower latency, and are more thermally efficient, but they have shorter transmission ranges.

Long-term maritime checking can also be accomplished through the use of a variety of additives and communication channels. For data gathering reasons, the study's authors [6] used Autonomous Surface Vehicles (ASVs), highly mobile imitation fish, and synthetic snails in Biograd Na Moru, Croatia. All detectors are permanent and fixed in the precise field of view, either tethered to air floats or moored on the sea floor, for both the fixed segmentation process. The position of cluster members may be determined using a variety of methods. Based on the hardness theory, a new technique [7] advocated the use of conventional ray calculations to handle the occurrence of uncertainty in the node density site.

WSN deployments and different attacks (such as active and passive attacks) were described by the experts in [8]. They also talk about the necessity of information transmission trust and openness from sender to receiver. [9] proposes a safe routing mechanism that includes a shortest path selection and deterministic algorithms to normalize vitality utilization, as well as multiple routing approaches to data encryption. However, because the capacity of the network, which is the major restriction in WSNs, is not taken into account, this technique may fail. The professionals in [10] proposed a methodology in which the WSN is secured using the Rivest cypher 6 (RC6) technique and dynamically cross prioritization (DMP) for packet sequencing with lossless encoding categorization.

It was described how to build a heterogeneous robotic swarm for long-term autonomous monitoring of marine environments.The capabilities and duties of two different agent kinds, as well as the various interactions between them, were described in detail. The surface and underwater means of communication that were established to allow the swarm to engage in advanced behaviours were examined.A dual network topology was established on the surface, consisting of a mesh network and a system of access points.By using an acoustic communication protocol based on Time Division Multiple Access, affordable acoustic modems have proven to be reliable in enabling critical information exchange during underwater research.

Experiments in real-world environments and conditions confirmed the robotic swarm's individual and collective capabilities. Advanced underwater positioning methods will be implemented as part of the swarm's continued development. Current algorithms and behaviors will be thoroughly tested for scalability. The swarm's collaborative behaviors will combine high-level evolutionary decision-making, task allocation, and scheduling algorithms, extending the range and efficiency of its autonomous exploration and monitoring capabilities.

3. IMPROVED TIME BASED DIMENSIONAL TRAFFIC PATTERN ORIENTED MALICIOUS ALLEVIATION

Different forms of DoS attacks and the accompanying protective methods are discussed briefly in accordance with the UWSN paradigm. The submerged wireless network, on the other hand, is made up of five layers, as illustrated in the diagram. Figure 2. This research looked at prospective DoS attacks at all tiers as well as sophisticated DoS prevention systems. All tiers are prone to Hacking, which are detailed following.

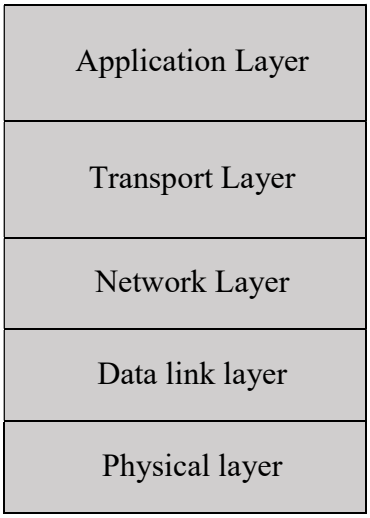

Figure 2: Layers in communication medium of underwater

The very first layer is the main layer, which is in charge of all hardware interactions. Conflict attempts, weariness operations, buzzing attacks, and denials of sleep attacks are all conceivable DoS violence on the second layer, which is the cabling, which comprises all potential algorithms executed over the networks. These are the probable data link layer attacks. The third layer is the network architecture, which is crucial for the proper interconnection and intraconnection. Wormhole, hello-flooding, and homing attacks are examples of probable dos attacks. The final tier is the transmission control protocol, which groups inconsistencies functions. Coordination and synchronizing overflow techniques are common dos attacks. The last element is an application server that communicates with all specific requirements.

3.1 Aspects of the Routing layer

Private navigation and highly secure transferring are two features of the network boundary. In routing the data, networks are deeply linked in order to efficiently communicate correct routing information. In the second, secure data transfer, disruption is used to safeguard data packets from unwanted access. The networks division is in charge of maintaining secrecy.

3.2 Improved Time based Dimensional Malicious Alleviation

The measuring and control geospatial real - time traffic method is utilised to accurately determine the hostile assault. This method presents the position and non-stationary logs of a network through a well way. Figure 3 depicts the system design of a time-oriented geographical distribution.

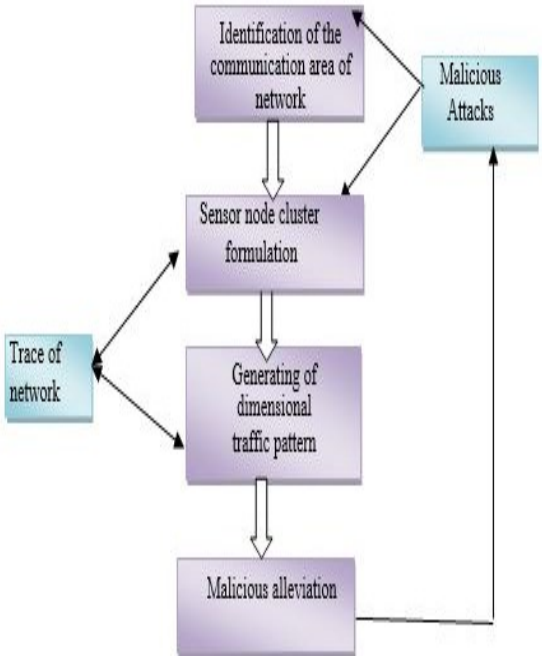

Figure 3: Architecture of ITDMA

3.3 Cluster formulation and network tracing

All stations in an underground sensor network locate their neighbours using the findings, and the information is saved in the networking tracing. The simple introduction of cluster formulation is represented in Algorithm 1

Algorithm 1: Formulation of cluster

Let us Consider,

F1=First cluster; L=Node record; CNi,j=For each nodule the group head np=Node position; nt=Network trace.

Step 1: If node==Base station then

Connect the terminals in the network's scope. Then, using Il as the initial cluster and Node List(L) as L=nodes @coverage, create a clustering organization (base station)

Else

L= nodes@coverage Node List (nodes)

The routers in the member nodes, as well as the connection tracing.

End

Step 2: For each nodule the group leader is denoted as CNi,j Identify the arrangement of CNi,j

np=Ni(p)

insert to the complex trace=∑trace(nt)+{Ni,np}

End the process

The channel's vertices and ground stations connect to the networking trace to construct a clustered networks. Furthermore, the suggested method exclusively uses data from the connection trace. Algorithm 1 depicts the excellent start of nodes

.

3.4 Improved Time Variant Dimensional Traffic Pattern Creation

The networks tracer in the suggested technique contains information on each node's content, as well as the geolocation of nearby nodes with each timescale and congestion behavior. The routing process in the coverage range contains the information of all the neighboring routers, and the framework of the flow patterns will be created based on the basis nodes and nodal location.

However, detecting a denial of service attack at the protocol stack is extremely challenging. Furthermore, the calculated pattern method, which is described in Algorithm 2, aids in the detection of denial of service to a substantial measure and with ease.

Algorithm 2: Time variant dimensional traffic pattern factor

Step1: Determine the set of points that are neighbours at iteration t Construct the clustering according with node structure. C Generate each protoplanetary neighbour connection list (Tn). List of Clustered Neighbors

Cnl=∑ Neighbours@Pα

For each neighbor from Ni from Node record consider, during announcement that the numeral of

Step2: container reputable is denoted as Pμ

Pμ=∑packets∑(Nt@Pα)

Step 3: Whereas the payload(Pl) is planned as below: Pl=(∑payload(packets∈(Nt@Pα)))/Pμ

The node position is identified as NP=Loc(Ni)

The pattern(pi) is create by using the below design Pi={Ni,NP,Pμ,Pl }

The engender blueprint is added in the Pattern set(Rs) as likebelow Rs=∑patterns (Rs)+pi

Step4: End the procedure.

3.5 Detection of Malicious Attacks

Using the patterning cluster rearrangement strategy, the denial of attacks are a type is decreased. The cluster moves from "transmit" to "receive" depends on the prior time element type mechanism. In the configuration mode, the difference of networks traces aids in the formation of a flow patterns and Patterned Set (PS). With each timespan, the data of the neighbourhood connections are displayed in the networking traces. The reputation score for a single cluster members then each location may be determined using the patterning set metadata. The node trust rating output is greater to the predefined threshold to deliver the payload. The package will be forwarded if the trusted calculated values is higher than the maximum node; else, it will be rejected. The networks tracing and template set play a critical role in detecting DOS malicious nodes. For the identity of the nodes with the ground station, where the specifics of all the stations' locations are maintained, one step confirmation is employed. The pattern set (Ps) and the networking trace (Nt) are used as sources for the detecting. Algorithm3 describes an identification process for a DoS session hijacking.

Algorithm 3: DOS Congestion Attack Discovery

Step 1: Identify the packet source ps Sa=Source-Address (p)

The node position(NP) from the network sketch(ns) NP=Nt(Ni(POS))

Step 2: In the next tread the node position is confirmed with the Ground station(GS) If true, then NP=Ps(Ni)@Tα

Else

Start again the process

The acknowledgment of the preceding time blueprint is retrieve from set-up trace.

3.6 Process of Position Update

The movement and foraging motion that was created by other krills will have two techniques, both local and global. Both work in parallel in order to power the ITDMA. Based on these formulations for its first member, in case the amount fits for the above positions, it may be better compared to the fit of the first member. This will have a gravity effect and, if not a repulsive effect. By employing proper motion parameters, the position vector for the krill interval t to $t + \Delta t$ has been defined in Equation (1).

$$X_i(t+\Delta t) = X_i(t) + \Delta t \frac{(dX_i)}{dt} \quad (1)$$

$$\Delta t = C_t \sum_{i=1}^{NV} (UB_j - LB_j) \quad (2)$$

Equations (1) and (2) were obtained from Equation (10) for a better situation.

$$X_i(t+\Delta t) = X_i(t) + Ct \sum_{i=1}^{NV} (UB_j - LB_j) \times (N_i + F_i + D_i) \quad (3)$$

The NV parameter refers to the total variables, UB and LB parameters refer to the upper and lower limits of its j variable. The Ct parameter has been chosen within the range [0, 2]. It is evident that a small value for the parameter will permit an accurate search space exploration. To enhance the search procedure, all reproduction operators of the GA were added to the krill group optimization, and this includes a crossover operator and the mutation operator. This crossover operator has been defined by a probability Cr, control, and m after Xi as per Equation (4). $randi, m$ parameter was a random number within the range [1, 0].

$$X_{i,m} = \begin{cases} x_{r,m} & rand_{i,m} < Cr;\ Cr = 0.2\hat{K}_{i,best} \\ x_{i,m} & else \end{cases} \quad (4)$$

By using Equation (4), the crossover probability for global optimization goes up to zero with a decreasing fit. A mutation operator for the KH algorithm has been defined by a Mu probability with the second m after Xi as per Equation (5).

$$X_{i,m}=\begin{cases} x_{gbest,m}+\mu(x_{pm}-x_{qm}) & rand_{i,m}<Mt,\ Mt=0.5\hat{K}_{i,best} \\ x_{i,m} & else \end{cases} \quad (5)$$

4. SIMULATION RESULTS

The protocol stack NS-2 is used to construct the slowly varying geographical routing path. In a variety of settings, the simulations is made using 100 nodes. The details of the networking tracing are used by the access point and nodes in the data transmission to determine the specified threshold and specific trust level in the broadband service. The time frame in the networks traces updates the characteristics of the neighbor nodes. As a result of the specifics, the one-step testing approach is used to locate the jamming attack.

The recommended technique is superior against M-LEACH, the Krill Herd Process, and clocking values. The assessment is based on classification accuracies, change approach, high false ratio, and challenging task.

4.1 Accuracy of Detection

According to the comparing assertion, the proposed technique achieved high precision than that of the other technique. One confirmation approach demonstrates that its suggested method has improved detection results.

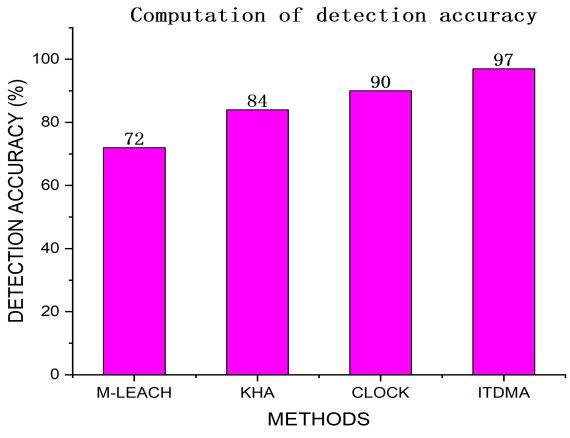

Figure 4: Comparison Of Detection Accuracy

4.2 False Alarm Ratio

For each period windows upgrading process, the neighborhood component details are updated, as well as the completed certification mechanism for each message deal. In comparison to existing comparable methodologies, the suggested system has a relatively low False alarm ratio.

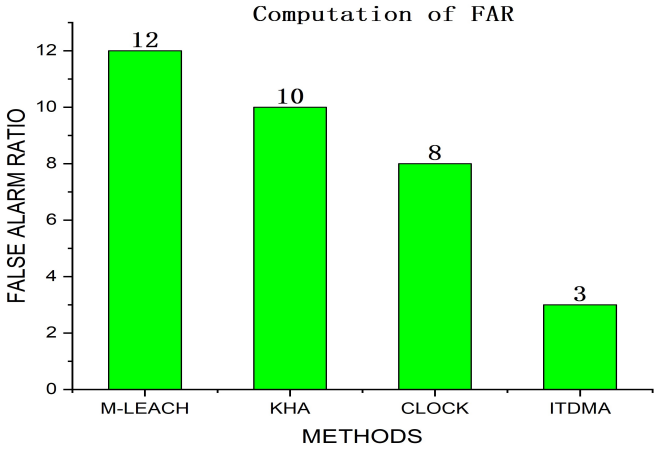

Figure 5: False Alarm Ratio

The edge over the competition is also linked to the network. For enhancing coordination, the system incorporates the notion of neighboring node updates parameters with each timespan system or network traces.

4.3 Performance over Throughput

All of the previous approaches have internet speed than the suggested method. The ITDMA formal specifications the large bandwidth and the least computational burden due to the one-step verification.

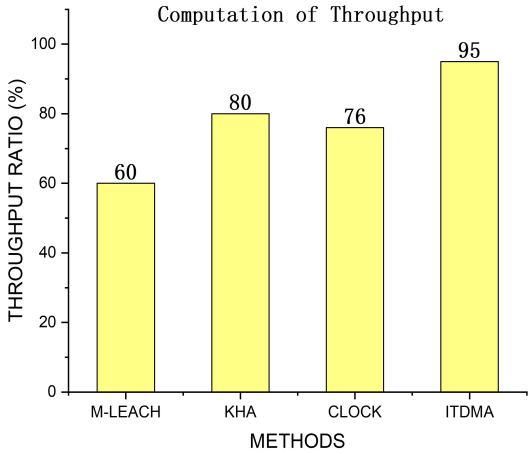

Figure 6: Throughput Ratio

5. CONCLUSION

The primary issues that WSNs confront include a shorter network lifetime, time delays, and a lack of privacy throughout data transfer. WSN nodes interact with one another across a wholly new means, which can be a simple hops or numerous hops. For every time frame exchange, the ITDMA technique has been changed. Through to the networking tracing at the present time frame for each data transfer, it validates the specifics of the community. The trust level of the node is checked to a certain level. The node is transmitted if the trust level is high; alternatively, it is deemed a fake node or jammer and ignored. The ITDMA simulation outcomes were efficient and beat the other options. In the future research direction approach, Artificial Intelligence based Neural Networks can be used for the complex computations for finding the malicious attacks in the Underwater Wireless Sensor Networks which will enhance the performance still further. Localization techniques will be implemented as part of the swarm's continued development.Current algorithms and behaviours will be thoroughly tested for scalability. The swarm's collaborative behaviours will combine high-level evolutionary decision-making, task allocation, and scheduling algorithms, extending the range and efficiency of its autonomous exploration and monitoring capabilities.In the future, using the model given in this research, we want to determine the ideal number of sinks and clusters in the network.

REFERENCES:

[1] Saravanan, T., & Nithya, N. S. (2020, December). Mitigation of attack patterns based on routing reliance approach in MANETs. In *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 387-392). IEEE.

[2] Tian, S., Li, Y., Kang, Y., & Xia, J. (2021). Multi-robot path planning in wireless sensor networks based on jump mechanism PSO and safety gap obstacle avoidance. Future Generation Computer Systems, 118, 37-47.

[3] Jari, A., &Avokh, A. (2021). PSO-based sink placement and load-balanced anycast routing in multi-sink WSNs considering compressive sensing theory. Engineering Applications of Artificial Intelligence, 100, 104164.

[4] Jiang, X.; Shi, C.; Wang, Y.; Smalley, J.; Cheng, J.; Zhang, X. NonresonantMetasurface for Fast Decoding in Acoustic Communications. Phys. Rev. Appl. 2020, 13, 014014.

[5] Saeed, N.; Celik, A.; Al-Naffouri, T.Y.; Alouini, M.S. Underwater optical wireless communications, networking, and localization: A survey. Ad Hoc Netw. 2019, 94, 101935.

[6] Lončar, I., Babić, A., Arbanas, B., Vasiljević, G., Petrović, T., Bogdan, S., &Mišković, N. (2019). A heterogeneous robotic swarm for long-term monitoring of marine environments. Applied Sciences, 9(7), 1388.

[7] Mridula, K.; Ameer, P. Localization under anchor node uncertainty for underwater acoustic sensor networks. Int. J. Commun. Syst. 2018, 31, e3445.

[8] Saravanan, T., & Sasikumar, P. Assessment and Analysis of Action Degeneracy Due to Blackhole Attacks in Wireless Sensor Networks. In *Proceedings of 6th International Conference on Recent Trends in Computing: ICRTC 2020* (p. 345). Springer Nature.

[9] D. Tang, T. Li, J. Ren, J. Wu, Cost-Aware SEcure Routing (CASER) protocol design for wireless sensor networks. IEEE Trans. Parallel. Distributed Syst. 26(4), 960–973 (2015).

[10] Saravanan, T. (2021). Enhancing Node Lifetime In Wireless Sensor Networks Using Itdms With Apteen Protocol. *Design Engineering*, 8239-8250.

[11] Kumaresan T, Saravanakumar S, and Balamurugan R, 2017"Visual and Textual Features Based Email Spam Classification Using S-Cuckoo Search and Hybrid Kernel Support Vector Machine" Cluster Computing, Springer, and DOI: https://doi.org/10.1007/s10586-017-1615-8

[12] Saravanan, T., & Nithya, N. S. (2019). Modeling displacement and direction aware ad hoc on-demand distance vector routing standard for mobile ad hoc networks. *Mobile Networks and Applications*, *24*(6), 1804-1813.

[13] Saravanakumar S,Karthiga R and Sangeetha K 2017"Advanced Analysis of Anatomical Structures using Hull based Neuro-Retinal Optic Cup Ellipse Optimization in Glaucoma Diagnosis", CiiT International Journal of

Digital Image Processing Issue January 2013, DIP012013001

[14] Saravanan, T., & Nithya, N. S. (2018, December). Energy Aware Routing Protocol Using Hybrid ANT-BEE Colony Optimization Algorithm For Cluster Based Routing. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1-6). IEEE.

[15] Saravanan, T. (2014). An Efficient Multi Channel Query Scheduling In Wireless Sensor Networks. *International Journal of Computer Science and Network Security (IJCSNS)*, *14*(2), 71.

[16] Saravanan, T., & Thillaiarasu, N. (2021, March). Optimal Grouping and Belief based CH selection in mobile ad-hoc network using Chunk Reliable Routing Protocol. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 933-940). IEEE.

[17] Saravanan, T., Ambikapathy, A., Faraz, A., & Singh, H. Blockchain and Big Data for Decentralized Management of IoT-Driven Healthcare Devices. In *Convergence of Blockchain, AI, and IoT* (pp. 57-81). CRC Press.

[18] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671-2701.

[19] Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *arXiv preprint arXiv:2005.09140*.

[20] Singh, G., & Khare, N. (2021). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, 1-11.

[21] Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 1-20.

[22] Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *Security and Privacy*, *1*(5), e39.

[23] Xue, Y., Jia, W., Zhao, X., & Pang, W. (2018). An evolutionary computation based feature selection method for intrusion detection. *Security and Communication Networks*, *2018*.

[24] Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., ... & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, *43*(3), 42.

[25] Jamil, H., Yang, N., & Weng, N. (2021, June). Securing Home IoT Network with Machine Learning Based Classifiers. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)* (pp. 289-294). IEEE.