Analyze and evaluate the state of art scheme for fault tolerant WSN

(Corresponding author Email: taranmgc22@gmail.com)

Taranpreet Kaur	Taranpreet Kaur, Assistant professor, Department Computer Science, Mata Gujri College Fatehgarh sahib, Punjab, India
https://www.ijrisat.com/ - **(Old link-upto Vol.5)** **Received: 25th Sep.2022;** **Revised: 15th Oct.2022** **Accepted: 3rd Nov.2022;**	**Vol.No.6,** **grpublication.com/index.php/ijrisat –** **(New link)** **Issue No.11, November, 2022** **Published: 10th Nov.2022**

ABSTRACT

Wireless Sensor Network (WSN) offers a medium that can transmitted signals, microwave, satellite or radio signals for communication process. Wireless Sensors acts as a transceiver that is it receive the signal as well as transmit the signal to the destination. WSN includes a group of nodes that are typically low in functionality. Wi-Fi tools, in addition to optical computing, expanded the major event correlated with detector nodes, the new developments in micro-electro - mechanical systems development. It results in realistic viability for the specific prospect of flowering associated with WSNs. The WSN network faces two types of failures in the networks namely the physical fault and the network fault. When it comes to the physical fault, the process is termed as fault detection and when it is associated on the base of data level. Some schemes are comparable to a common social network, but typically depend on different personality stereotypes that each single PC relates to one individual character. Such problems usually occur when a reputational context is fooled through a disproportionately high effect on a confidence attacking PC.

KEYWORDS: Wireless Sensors, Wi-Fi tools, detector nodes, WSN, physical fault, Network fault, Sensors.

1. INTRODUCTION

Wireless Sensor Network (WSN) offers a medium that can transmit signals, microwave, satellite or radio signals for communication process [1-5]. Wireless

Sensors acts as a transceiver that is it receive the signal as well as transmit the signal to the destination. WSN includes a group of nodes that are typically low in functionality. Wi-Fi tools, in addition to optical computing, expanded the major event correlated with detector nodes, the new developments in micro-electro - mechanical systems development. It lts in realistic viability for the specific prospect of flowering associated with WSNs.

1.1 Fault or intrusion in network

The WSN network faces two types of failures in the networks namely the physical fault and the network fault [6-8]. When it comes to the physical fault, the process is termed as fault detection and when it is associated on the base of data level, it is termed as intrusion in the network. In both the cases, the data packets are going to be affected. If there is physical fault, the CH will not be able to aggregate the data packets and by the end of the process, the overall throughput will be low as injected packets were not transmitted to desired terminals. The intrusion comes into the act when false data packets are sent or received in any Node to Node((N2N) communication[9-12]. Thus, security and antivirus method are highly critical for any system or communication. Intrusions can quickly become dangerous because hubs in specific systems can guarantee many roles.

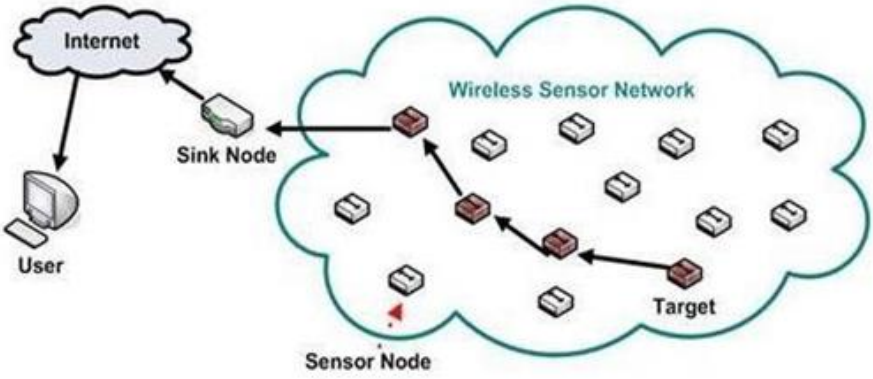

Figure 1: WSN architecture representation [10-12]

Some schemes are comparable to a common social network, but typically depend on different personality stereotypes that each single PC relates to one individual character. Such problems usually occur when a reputational context [13-15](such as a specific reputation for record exchange on a particular system) is fooled through a disproportionately high effect on a confidence attacking PC[16-18].

1.2 Specific areas of intrusion

There are various uses of Intrusions in distinctive situations; mentioned below.

a) **Routing:** Intrusions can disturb routing protocols in ad-hoc systems, particularly the multi-cast routing mechanisms. Another idea is

Geographical routing, where vindictive hubs may show up at more than one spot at once [19].

b) **Tampering with Voting and Reputation Systems:** In the event of any environment where there is a voting plan set up for purposes, for example, reporting and recognizing hub in the framework, intrusion may be especially unsafe. As a sample, an attacker may make enough malicious identities over and over-report. Then again, these malicious hubs can shield themselves from constantly being evacuated as they are in a collision [20-22].

c) **Fair Resource Allocation:** Intrusions might likewise be utilized to empower the attacker to get an excessively substantial offer of resources that were planned to be circulated amongst the interconnected nodes [23].

d) **Distributed Storage:** File storage systems in shared networks and WSN networks can be traded off by the Intrusions. This is accomplished by creating the fragmentation and replication forms in the document [24].

e) **Data Aggregation:** Sensor network readings are processed by query protocols in a system. This is done for energy conservation. Sybil identities may have the capacity to report inaccurate sensor readings. A malicious client may have the capacity to change the destination address of data packets by its own packet address [25].

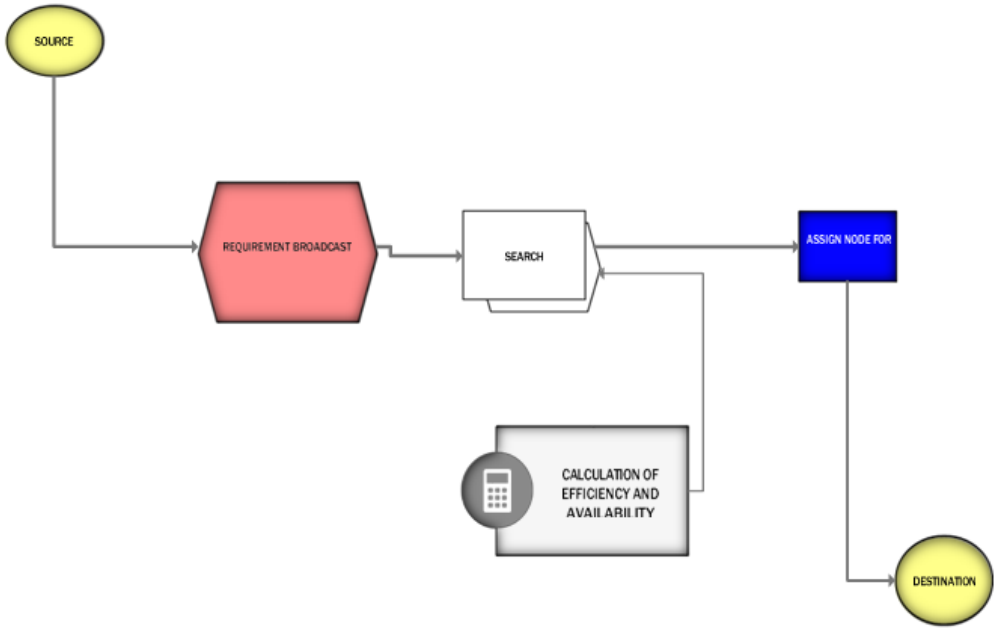

Figure 2: Intrusions detection system [25]

2. LITERATURE REVIEW

In wireless communication, data is transmitted from one node to another node. In such scenario, the nodes are communicated with different coordinate positions. Therefore, the node deployment, routing of data packet to the desired node is

necessary. In this section, the work performed by various researchers focusing to save energy, develop techniques to protect network from intruder and management through interpolation is presented [27-29]. In this paper, a predictive model has been presented to estimate the mobility as well as the remaining energy of the nodes positioned in the WSN. Here, the network is designed in MATLAB tool that consists of a BS with 21 number if SN that were clustered in an area of $150 \times 60m^2$. The designed model has analyzed the effect on remaining energy of SN with Respect to the transmission distance [30-32]. Also, the effect of inter and intra-cluster movement has been analyzed against the mobility factor of SN. Khan and Pushparaj (2021) propose a hybrid Maximum Power Point Tracking (MPPT) controller for solar photovoltaic (PV) systems. The controller utilizes soft computing techniques to optimize the extraction of maximum power from PV arrays under varying environmental conditions. Simulation results show that the proposed hybrid MPPT controller outperforms other techniques, providing more accurate performance and reducing fluctuations around the maximum power point.

In this research article, the authors have focused on to resolve the problem of packet loss in MWSN network using LEACH-MT2FL clustering approach. This approach is the enhancement of Type-2 Fuzzy logic approach [33-35]. In this approach route is formed using a well- known LEACH approach, and the selection of CH has been performed using Fuzzy logic. From the results it has been observed that the proposed approach performed with better performance parameters evaluated. Pushparaj and Saini et al. conducted a comparative study on biomedical physiological-based ECG signal heart monitoring for the human body. They reviewed techniques for estimating heart rate from various physiological signals, emphasizing the challenges of cardiovascular diseases in the 21st century healthcare system, including the COVID-19 pandemic.

In this paper, the researchers have proposed an enhanced mobility-based GA (Genetic Algorithm) approach that helps to resolve the difficulty of PDR in MWSN and hence enhance the network stability time[36-38]. Here, GA has been used to find the best location of CH along with the total CH's present in the network. Time allotment has been performed by the mechanism using Time division Multiple Access (TDMA) scheme for those nodes that were moving out from the network. From results an enhanced performance has been obtained in terms of network parameters[39-40]. In this research, the authors have used game theory in addition to clustering algorithm. An energy efficient clustering approach has been used for the selection of appropriate CH and later on examined the performance. Pal et al. (2020) discuss the challenges of seamless roaming and mobility management in heterogeneous 4G wireless networks. They aim to find a simple and convenient method for vertical handoff that covers all the necessary parameters for handoff in a simplified manner using a layered approach, enabling both automatic and user-specific handovers. The proposed approach, called the GPA strategy, is developed on a three-layered platform to provide a straightforward architecture that supports both types of

handovers and considers a wide range of factors for decision-making. The proposed approach has been able to lessen the hot spots in the network that results in minimization of delay. Overall, the authors have concluded that the performance of the proposed work is improved against the baseline methods .In this paper; the authors have presented an enhanced Artificial Bee Colony as a swarm inspired approach applied for the detection of intruder in WSN system [41].

The author has divided the entire network in different cluster each contained a single CH as a master node. The clusters are also dived into two types normal and abnormal. The cluster, whose CH distance is larger than the other existing clusters, is categorized as abnormal cluster. Based on this, SVM is trained and tested during communication process [42]. In this article, the problem of implementing clustering in WSN has been resolved using mobility aware hierarchical approach. The mechanism is based on three-layer clustering architecture that includes mobility aware centralized and hybrid clustering algorithms [43]. The results show that an improved WSN performance has been determined in terms of determined parameters.

The researchers proposed Restricted Boltzmann computer- based clustered IDS (RBC-IDS) to undertake comparative study of the usage of IDS deep and machine learning applications in wireless sensor networks (WSNs). RBC-IDS output is analyzed as opposed to current adaptive IDS focused on machine learning called as the Adaptively Controlled and Clustered Hybrid IDS (ASCH-IDS). And the findings obtained indicate that RBC-IDS and ASCH-IDS deliver the same accuracy performance by the time RBC-IDS is identified nearly twice that of ASCH-IDS. The scheme proposed developed detection rate (99%) and accuracy (99.9%) for three secret layers. The solution has been presented by the researchers to resolve the issues related to the coverage in WSN by presenting two sensor development mechanisms named as blind- zone centroid-based scheme (BCBS), and disturbed centroid-based scheme (DCBS) respectively [44].

Kaur and Pal (2019) discuss Quality-of-Service (QoS) management in cloud systems and the importance of addressing security issues in cloud computing. They provide a survey of QoS modeling approaches and propose a cloud computing security framework to effectively tackle security problems. The aim of these approaches is to determine the destination location of SN so that the coverage holes can be heals effectively. Here, BCBS have used blind Zone polygon mechanism to find out the position of the source node with its nearby nodes. The center point of the polygon method is considered as target location with respect to other sensor nodes. On the other side, DCBS technique, finds the coverage holes in every round from using the centroid based approach.

In this paper, a dynamic scheme has been presented to identify Sybil node in WSN[45]. The algorithm is processes into two parts. The first part includes traffic monitoring whereas, the attack detection has been performed into the second part of the algorithm. A new deep learning technique for the identification of intrusion was presented in this paper. An unsupervised feature learning scheme with a non-

symmetric deep auto encoder (NDAE) has been used. The design has been implemented using the Graphical Processing Unit (GPU) that utilized KDD Cup 99 & NSL KDD dataset. The results have been found improvement compared to the existing work .The scheme utilized three layers of the network model including MAC layer, physical layer and information of node location in the network. The results prove that the proposed scheme perform well with reduced energy consumption and high network performance [46]. Pal and Pali (2018) propose using LTE-A technology and VANET-LTE advanced technology to facilitate congestion-free passage for emergency vehicles, particularly ambulances, in the Tri-City area. The aim is to address traffic congestion and ensure timely access to medical facilities, improving emergency response times.

The researchers have presented an auto organized and dynamic clustering approach to monitor relays in the WSN. The mechanism split the entire network into a set of clusters known as service zone. This helps to minimize the routing overhead, delay by utilizing bandwidth in an optimized way. The clustering mechanism also helps to manage load in the network. The cluster formation in small network reduces the buffer overflow and energy depletion problem[47]. From the experiments, it has been proved that the PDR, delay, energy consumption has been improved by 10 %, 15%, and 53% respectively. The improvement in the life of the network has been increased by 53 % with an energy balance of 51 % .

The researchers have used lightweight algorithm to identify the mobile sybil attacker node in WSN. The researchers have used two kinds of sensor nodes, Watchdog Nodes (WNs), and sensor Nodes (SNs) that are distributed randomly in the network area, in order to detect the Sybil nodes. SNs function is to collect data, and send that data to the base station. In WSN, the information related to the location of nodes is very essential to detect the attacker node or to collect information [48]. Here, two types of Monte Carlo schemes have been used to determine the location of nodes one scheme obtained information through anchor node and other is used both normal as well as anchor scheme. The utilization of both schemes anchors as well as normal enhances the accuracy but also increases the communication cost. The authors have proposed a new fault-tolerant routing procedure in order to lower the data packet lost caused due to route breakage. The proposed mechanism discovers alternate routes to successfully transmit data whenever the ability of any intermediate node gets challenged.

The simulation studies of the designed system were done in NS2. The network was tested against variable traffic levels and a variety of flows in terms of latency time, packet decline, packet transmission ratio, and energy usage calculated against. The suggested concept has been seen to have outperformed the current research in terms of measured output matrices[40,44]. The researchers have demonstrated a Hybrid Intrusion Detection System (IDS) for clustered WSNs on the basis of functional reputation and the rule of misuse. The main principle is that each sensor node determines its neighbors' credibility values by monitoring their behaviors. Base

Station (BS) identifies hostile nodes by combining possible integrity values with harassment laws. The simulation result shows that the proposed solution enhances the network lifetime and strengthens sensed data freshness by centralizing the identification of malicious nodes by increasing energy consumption.

The researchers have addressed confidence-based intrusion detection utilizing multi-attribute assurance measures to improve detection accuracy. The confidence of sensor networks (SNs) is evaluated through cluster heads (CHs) and the confidence of CHs is analyzed through neighboring CHs whereby the difficulty of the evaluation was reduced without any evaluation through the network's various overall CHs. In the similar field, a novel successful group-based scheme for detecting and avoiding massive black hole attacks in WSNs has been introduced. Here, all WSNs are classified into different groups. This mechanism achieved in the term of detection rate of 90% and an improved false-positive rate of 3.75% compared to the previous study [40-42].

The authors described the wireless Ad-hoc routing protocol's interoperability. Interoperability operates in the same manner as it will transmit messages to a neighboring network in case of more than two different networks, Focused exclusively on the constructive Strip Interoperability process, which has proved to cross numerous networks through layer 3 protocols. Use IPv6 and several other related protocols, the tested of this research carried out on Ubuntu Linux. The researchers have proposed a protocol that detect and prevent from selective black hole named as Modified Dynamic Source Routing (MDSR) protocol. A selective black hole attack is a type of black hole attack that has packets dropped in a way that is selectively dropped by malicious nodes. If any kinds of the anomaly are detected, the adjacent IDS node informs all nodes of the network to remove this defected node from the network. A well-known routing protocol Ad-hoc On-demand Distance Vector (AODV) has been presented in this paper that works in addition with Artificial Neural Network (ANN) for MANETs. To measure AODV's reactive routing protocol's Hello message frequency to boost the efficiency of the MANETs [25, 40,45].

The main purpose of this paper is to connect the effect of separation the malicious nodes in those networks. The authors have focused on routing protocols that are rely on tree dependent topology in which the data is sent through the sensor node towards sink node via tree rooted on the sink. The routing tree was believed to be established by hop-distance towards the sink. Protocols, namely, RESIST-1 as well as RESIST-0, are analyzed for increasing network resilience by means of whole sink attacks.

The risk factor is introduced for measuring the selective forwarding impact. Inspired by the tremendous applications of random-walk proximity and to decrease the counts of the process related to the calculation of proximity, genuine efforts have been made [2, 25]. Structural and numerical attributes of the problem are used to lessen process counts. Based on speeding up the convergence of the underlying

iterative process, the authors used an alternative approach of Chebyshev polynomials names as Chopper.

Traditional iterative procedures used the outcome of the previous iteration to calculate the next iterate. When convergence is observed, iterations are stopped, i.e., when the proximity vector does not show any significant change between two operations, convergence halts there. Chopper Outperforms existing methods significantly by computing the coefficients of linear combination, making converging faster than iteration in the original formula. This reflects significant promptness in the calculating scores of random walk-based proximities.

3. PROBLEM STATEMENT

WSN has emerged as a new wave of technical development when it comes to transfer the data from one node to another node. As mobility is one of the integrated aspects of WSN which is used to support the wired nodes in case of any physical failures, threats other than physical damage comes into play. The intermediate nodes from one source to a terminal are termed as hops and the communication between the nodes is termed as Node to Node (N2N) communication. The communication between the nodes can take place either through Cluster Heads (CHs) or by their own. Most of the research articles which are also mentioned in the introduction and the related work section have used cluster oriented concept to transfer the data from one node to another.

The role of the CHs is to aggregate the data from other nodes in the region and the selection of the CHs are mostly dependent upon the associated residual energy of the candidate node. Residual Energy is the total amount of energy which is extracted from the battery of the sensor node. The consumption of energy is always based on some energy consumption model in which there is certain rule set for the data transfer. In case of fault, CHs will use more energy to transfer the data and will soon lose the probability to become the CH next time. Wireless communication network in which the server faces a lot of service requests which often goes out of the boundary limit of the serving capacity and that leads to either deadlock or packet dumps which eventually reduces the Packet Delivery Ratio (PDR). The PDR can be represented as follows:

$$PDR = \frac{ReceivedPacket}{SentPackets}$$

Gray hole attack is another similar intrusion. As for example, in gray hole attack agrees to sends the same packet to keep the server busy to manage identities of Packets. Black hole attack in a similar fashion sends false packets to the receiving node. Modern framework algorithms like Swarm Intelligence are making their mark in the real-world applications. The challenge of this research work is to develop Machine learning based security architecture to prevent security threat in N2N communication.

4. METHODOLOGY

The proposed methodology is centric based on two orientations namely node level fault or intrusion detection and network level fault or intrusion detection and hence the proposed methodology is designed in two segments. The first segment aims to improve the CH selection process as follows. WSN architectures mostly use the concept of high residual energy along with the distance to the base station. The proposed methodology introduces supplied load to the existing CH selection method with is briefed in the introduction section.

5. CONCLUSION

This main work aims to provide an improved solution to the problems triggered by malicious activities in the N2N communication. In recent technological developments, the networking is one of the rapidly growing fields. It can be expanded in terms of number of nodes and network scale. The network composed of different elements, such as network management, network security, network applications, and many more. By observing and monitoring the node's activities, the behavior of nodes (normal and abnormal) can be identified. In order to provide complete security against various attacks, it is necessary to provide authentication in each level of data transmission layer. To design a wireless network with minimum threat to security using swarm intelligence approach with machine learning approach.

REFERENCES

[1] Mohamed, S.M., Hamza, H.S. and Saroit, I.A., 2017. Coverage in mobile wireless sensor networks (M-WSN): A survey. *Computer Communications*, *110*, pp.133-150.

[2] Khan, A.W., Abdullah, A.H., Anisi, M.H. and Bangash, J.I., 2014. A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks. *Sensors*, *14*(2), pp.2510-2548.

[3] Zhao, Z., Huangfu, W., Liu, Y. and Sun, L., 2011, December. Design and Implementation of Network Management System for Large-Scale Wireless SensorNetworks. In *2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks* (pp. 130-137). IEEE.

[4] Khan, M. J., & Pushparaj. (2021). A novel hybrid maximum power point tracking controller based on artificial intelligence for solar photovoltaic system under variable environmental conditions. Journal of Electrical Engineering & Technology, 16(4), 1879-1889.

[5] Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. *Computer networks*, *52*(12), pp.2292-2330.

[6] Sabor, N., Sasaki, S., Abo-Zahhad, M. and Ahmed, S.M., 2017. A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions. *Wireless Communications and*

Mobile Computing, *2017*.

[7] Nadeem, A. and Howarth, M.P., 2013. 'A survey of MANET intrusion detection & prevention approaches for network layer attacks'. *IEEE communications surveys & tutorials*, *15*(4), pp.2027-2045.

[8] Pushparaj, K., & Saini, G. (2021). Comparative Study of Biomedical Physiological based ECG Signal heart monitoring for Human body. In 2021 International Conference on Emerging Technologies: AI, IoT and CPS for Science and Technology Applications, ICET 2021

[9] Ozcelik, M.M., Irmak, E. and Ozdemir, S., 2017, May. 'A hybrid trust based intrusion detection system for wireless sensor networks'. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

[10] Singh, R., Singh, J. and Singh, R., 2017. 'Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks'. *Wireless Communications and Mobile Computing*, *2017*.

[11] Pal, P., Kaur, T., Sethi, D., Kumar, A., Kumar, S., Lamba, A., & Rastogi, U. (2020, February). Vertical handoff in heterogeneous mechanism for wireless lte network-an optimal approach. In 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3) (pp. 1-5). IEEE

[12] Boddu, N., Vatambeti, R. and Bobba, V., 2017. 'Achieving Energy Efficiency and Increasing the Network Life Time in MANET through Fault Tolerant Multi-Path Routing'. *International Journal of Intelligent Engineering and Systems*, *10*(3), pp.166-172.

[13] Kaur, T., & Pal, P. (2019). Cloud computing network security for various parameters, and its application. Int. J. Adv. Sci. Technol, 28(20), 897-904.

[14] Zamani, A.T. and Zubair, S., 2014. 'Key management scheme in mobile Ad Hoc networks'. *International Journal of Emerging Research in Management & Technology*, *3*(4), pp.157-165.

[15] Abdel-Azim, M., Salah, H.E.D. and Eissa, M.E., 2018. 'IDS Against Black-Hole Attack for MANET'. *IJ Network Security*, *20*(3), pp.585-592.

[16] Wazid, M. and Das, A.K., 2017. 'A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks'. *Wireless Personal Communications*, *94*(3), pp.1165-1191.

[17] Schweitzer, N., Stulman, A., Shabtai, A. and Margalit, R.D., 2015. 'Mitigating denial of service attacks in OLSR protocol using fictitious nodes'. *IEEE Transactions on Mobile Computing*, *15*(1), pp.163-172.

[18] Elsaid, S.A. and Albatati, N.S., 2020. An optimized collaborative intrusion detection system for wireless sensor networks. Soft Computing, pp.1-15.

[19] Pal, P., & Pali, L. (2018). Congestion free analysis for emergency vehicles response in tri-city (Panchkula-Chandigarh- Mohali) using LTE-A. Modelling, Measurement and Control A., 91(2),pp. 66-72.IIETA

[20] Zafar, S., Bashir, A. and Chaudhry, S.A., 2019. Mobility-aware hierarchical clustering in mobile wireless sensor networks. *IEEE Access*, *7*, pp.20394-20403.

[21] Otoum, S., Kantarci, B. and Mouftah, H.T., 2019. 'On the feasibility of deep learning in sensor network intrusion detection'. *IEEE Networking Letters*, *1*(2), pp.68-71.
[22] Fang, W., Song, X., Wu, X., Sun, J. and Hu, M., 2018. Novel efficient deployment schemes for sensor coverage in mobile wireless sensor networks. *Information Fusion*, *41*, pp.25-36.
[23] Jamshidi, M., Ranjbari, M., Esnaashari, M., Qader, N.N. and Meybodi, M.R., 2018. Sybil node detection in mobile wireless sensor networks using observer nodes. *JOIV: International Journal on Informatics Visualization*, *2*(3), pp.159- 165.
[24] Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q., 2018. 'A deep learning approach to network intrusion detection'. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), pp.41-50.
[25] Yang, X., Wang, L. and Xie, J., 2017. Energy efficient cross-layer transmission modelfor mobile wireless sensor networks. *Mobile Information Systems*, *2017*.
[26] Abuarqoub, A., Hammoudeh, M., Adebisi, B., Jabbar, S., Bounceur, A. and Al-Bashar, H., 2017. Dynamic clustering and management of mobile wireless sensor networks. *Computer Networks*, *117*, pp.62-75.
[27] Mohanapriya, M. and Krishnamurthi, I., 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40(2), pp.530-538.
[28] Shah, S.K. and Vishwakarma, D.D., 2012, July. 'FPGA implementation of ANN for reactive routing protocols in MANET'. In *2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)* (pp. 11-14). IEEE.
[29] Le Fessant, F., Papadimitriou, A., Viana, A.C., Sengul, C. and Palomar, E., 2012. A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Computer communications, 35(2), pp.234-248.
[30] Emperuman, M. and Chandrasekaran, S., 2020. Hybrid continuous density HMM- based ensemble neural networks for sensor fault detection and classification in wireless sensor network. *Sensors*, *20*(3), p.745.
[31] Wang, W., Sallenback, E., Ning, Z., Iradukunda, H.N., Lu, W., Zhang, Q. and Zhu, T., 2020. Mail Leak: Obfuscation-Robust Character Extraction Using Transfer Learning. *arXiv preprint arXiv:2012.11775*.
[32] Gracy Theresa, W., M. Prakash, and J. Betina Antony. "Multicast on-route cluster propagation using to identify the network intrusion detection system in mobile ad hoc network." *International Journal of Communication Systems* (2021): 4850.
[33] Sarkar, S. and Datta, R., 2017. An adaptive protocol for stable and energy-aware routing in MANETs. IETE Technical Review, 34(4), pp.353-365.
[34] Singh, D., Mishra, P. M., Lamba, A., & Swagatika, S. (2020). Security issues in different layers of IoT and their possible mitigation. *International Journal of Scientific & Technology Research*, *9*(04), 2762-2771.
[35] Lamba, Anil and Pal, Pushparaj and Singh, Satinderjeet and Singh, Balvinder and Muni, Sivakumar Sai Rela, Quantum Computing Technology (QCT) - A Data

Security Threat (2018). JETIR, Volume 5, Issue 4, April 2018.
[36] Aggarwal, P., & Pal, P. (2014). Implementation of an efficient low complexity method for wireless CE using a BEM for the wireless channel taps. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2,*594-600.
[37] Pal, P., & Verma, A. (2014). A survey to maximize retransmission of packets in WMSN. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2*, 575-581.
[38] Kaur, A., Pal, P., & Pal, P. K. (2014). An Efficient Way of Broadcasting Response Message to Help Demanding Vehicle in VANET'. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2*, 546-548.
[39] Walia, A., & Pal, P. (2014). An implemented approach of VANET using location information based technique for safe city and vehicle. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2*, 400-405.
[40] Gulati, V., & Pal, P. (2014). Enhancement of ICA Algorithm Using MatLab for Change Detection in Hyperspectral Images. *International Journal of Education and Science Research Review*, *1*(5), 1-9.
[41] Gulati, V., & Pal, P. A. (2014). Survey on various change detection techniques for hyper spectral images. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(8), 2277.
[42] Chauhan, J., & Pal, P.(2014). A Review to Vho for Wimax and Wifi Networks. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2*, 114-117.
[43] Kapoor, S., Pal, P., Gupta, S., & Sharma, M. (2014). Stable AODV protocol in mobile Ad-Hoc network. *Int. J. Adv. Res. Comput. Sci. Softw. Eng*, *4*(6).
[44] Miglani, E., Gupta, S., & Pal, P. (2014). Simulative Investigation on 3, 4 and 5 Level Discrete Wavelet Transform for Digital Video Watermarking. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(6), 2277.
[45] Verma, A., & Pal, P. (2014). A survey to maximize retransmission of packets in WMSN. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *vol*, *2,* 575-581.
[46] Singh, A., Pal, P., Gupta, S., & Singh, H. (2014). Optimal Path Selection in Dynamic Source Routing. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *2*.
[47] Kadian, A. K., Pal, P., & Goyal, V. (2013). Concept of Dynamic Bandwidth Allocation and Scheduling Algorithms in Passive Optical Networks. International EJournal of Mathematics and Engineering, 224, 2195–2200.
[48] Manwall, R., Mathuriya, A., Garg, S., & Pal, P. (2012). Performance evaluation of energy saving in WSN by using simulator ns2. *vol*, *1*, 6-9.