Intrusion Detection System based on Energy Efficient Dynamic Clustering in a Heterogeneous Environment of Wireless Sensor Networks (WSNs)

Dr. Rajkumar K. Chougale
Assistant Professor in Electrical Engineering, Bharati Vidyapeeth's college of Engineering, Kolhapur, Maharashtra, India, raj.chougale2015@gmail.com

Ranjeet S. Mithari
Assistant Professor in Mechanical Engineering, Bharati Vidyapeeth college of engineering, Kolkapur, Maharashtra, India, ranjeetmithari8888@gmail.com

Amit A. Desai
Assistant Professor in Mechanical Engineering, Bharati Vidyapeeth's college of Engineering, Kolhapur, Maharashtra, India, meetdesai17@gmail.com

Avadhut R. Jadhav
Assistant Professor in Mechanical Engineering, Bharati Vidyapeeth's college of Engineering, Kolhapur, Maharashtra, India, arjmesa@gmail.com

Sarita S. Shinde
Assistant Professor in Engineering Physics, Bharati Vidyapeeth's college of Engineering, Kolhapur, Maharashtra, India, saritashinde.bv@gmail.com

Gayatri S. Ghorpade
Assistant Professor in Environmental studies, Bharati Vidyapeeth's college of Engineering, Kolhapur, Maharashtra, India, gayatrighorpade20@gmail.com

Abstract

Wireless sensor networks (WSNs) has widely used in the practical-world applications, including the identification of the military targets, the monitoring of forest fires, the detection of medical and/or scientific targets, and, most importantly, in our everyday lives at home. However, because WSNs use broadcast transmission as their communication method and therefore lacks tamper resistance, adversaries can easily compromise WSNs. As a result, a hacker has the ability to listen in on all communication, replay past texts, insert suspensive data groups, and the compromised nodes. The two main security vulnerabilities that affect sensor nodes most frequently are the node and authentication of node compromise. This study proposes a heterogeneous structure for WSN intrusion detection and node capture. Using a cutting-edge method that combines a signature- based and anomaly-oriented methods through the neural network of multi-layer perceptron (MLP) classification through the clustering context, this framework effectively finds the recorded nodes. Additionally, the suggested architecture is effective at a very reasonable level of computation and cost of communication, it could provide a security barrier for actual application of WSN.

Keywords: WSN, intrusion detection, multi-layer perceptron, wireless sensor networks, heterogeneous

DOI Number: 10.14704/nq.2022.20.9.NQ44553 **Neuro Quantology 2022; 20(9):4756-4766**

Introduction

The wireless sensor network (WSN) is a system made up of several low in cost, constrained in resource- sensor nodes that collect crucial environmental data and transfer to a node of sink which acts as a main passage to another network or as a point of access for the human interaction. WSN is the field that is expanding quickly as new technologies become available

and new applications, includes those for home automation, traffic, environmental monitoring, healthcare, and military applications.. A huge number of invasions, including jamming, draining of battery, cycle of routing, Sybil, and the process of cloning, can affect WSN. The mechanism of Complex security can never be executed in WSN due to the sensor nodes' limited computing, memory, and power resources. As a result, implementing security in an energy-efficient manner is crucial for WSN.

Due of the potential impossibility of charging or replacing node batteries in WSN, a attack of sleep deprivation (also known as drainage battery) is the specifically severe attack. In this kind of attack, the intruder keeps the sensor nodes awake, wasting their energy. The limited power sensor nodes are subjected to such high energy consumption during this attack that they are rendered inoperable and cause denial of service via sleep deprivation.

This report presents an overview of ongoing research effort. The comparison of the most recent ID schemes comes next. The proposed model for identifying sleep deprivation attacks is briefly discussed in this paper's conclusion.

The WSNs' topology designs range from a simple wireless multi-hop mesh network to an easy star network. Between the various network hops, data propagation methods like flooding or routing may be used. Traditional WSNs are vulnerable to the series of attacks. These attacks can often be divided into three categories: i) Invasion on network availability, (ii) Invasions on availability of network, and (iii) conversion of invasions on the integrity of service. Initial and third categories of assaults on sensor networks are the main topics of this paper. Security measures for sensor networks now only guard against external threats, failing to prevent internal threats that compromise a number of sensor nodes. An attacker attempts to infiltrate a sensor node during a covert attack in order to inject false data. In this type of assault, a hacker gains access to the network's codes and encryption keys. The enemy can continuously disrupt or disturb the sensor network's regular operations, such as creating routing loops. By transmission the authenticated data towards base station, a compromised node could have an effect on the sensor network. An intrusive party can completely influence the functioning of a select few sensor nodes by physically contacting the nodes.

Compromise of the node is typically regarded as in the most difficult problems out of methods of WSN security.

Specification-Based Detection Technology Research

The technology first specifies a number of specifications before monitoring network activity in accordance with those specifications. Any departure from the norm constitutes abnormal behaviour. These usual behaviours are explicitly determined; machine learning or training data are not used to define them. Consequently, creating and updating requirements will take a lot of time. An intrusion detection system for spotting witch attacks was presented by [7]. The testing procedure employs two procedures. The first is mutual defence. The ID of source of packet is examined when it is received by the sensor node. The second is SRP, which confirms how many packets a node has sent and received. According to simulation results, mutual defence technology is costly and inapplicable in situations where attackers have a limited communication range. A distributed IDS based on predetermined rules was developed by [8]. Data collecting, rule application, and intrusion detection are the system's three steps. The system has some monitoring nodes installed. There are operating in mode of hybrid, gathering of packets also carrying out intrusion detection operations through identifying the traits of recognized attacks. The new approach for wireless sensor network intrusion detection depends on the clusters was given by [9] since the distribution of monitoring nodes and the choice of rules have an impact on the algorithm's performance and monitoring nodes consume a lot of resources.

Detection of Misuse Technology Research

The abuse detection system uses the intrusion mode to identify known assaults. Gatekeeper technology can be applied in wireless sensor networks in accordance with the features of wireless communication propagation and the presumption that nodes are widely scattered. A framework for using IDS with wireless sensor networks was created by Roman et al. There are both local and global agents in this architecture. Each node has a local agent that monitors the

flow of data locally. The network's global agent is present on some nodes and monitors the communication between them. Cluster heads may function as global agents in a hierarchical network topology. To choose the least amount of global agents necessary to cover the entire network in planar topologies, the design employs a method known as spontaneous watchdog. This strategy has two shortcomings. One is that it cannot ensure that all nodes are watched because global proxy selection is random. The second is the absence of consideration for packet collisions.

Heterogeneous Wsn

Multiple types of nodes of sensor make up a heterogeneous wireless sensor network (WSN) (SNs). On these specialized sensor nodes, different applications of supporting various tasks, such as detection of event and localization, also monitoring, may be running. New configurations, problem repairs, and application of new programmes must also be done throughout the lifecycle. This is a tremendously difficult process to complete in the networks along with the thousands of nodes. In comparison to a regular node, a heterogeneous node has a more complicated CPU also memory which allows it to do complex tasks. A heterogeneous node has a transceiver with a longer range and higher bandwidth than a typical node, ensuring trustworthy transmission.

Kinds of Heterogeneous Resources

In a sensor node, resource heterogeneity often takes one of three forms:

- **Heterogeneity in computing**

Due to heterogeneity of computation, and the heterogeneous nodes have more memory and a more potent CPU than the standard node. The heterogeneous nodes could offer processing of complex data and the longer-term storage thanks to their strong computational resources.

- **Heterogeneous Links:**

Link heterogeneity refers to the fact that a heterogeneous node has a longer network transceiver range and higher bandwidth than a typical node. Data transfer may be more dependable as a result.

- **Heterogeneity in energy:**

The heterogeneous node is line got power or has a removable battery because of its energy heterogeneity.

The energy heterogeneity is the most significant of the three types of resource heterogeneity discussed above as these two computational heterogeneities and the link of heterogeneity would take up additional resources of energy. Without energy heterogeneity, computational and link heterogeneity will have an adverse effect on the entire sensor network, shortening its lifetime.

Line power is used in heterogeneous nodes (its battery is replaceable). Various kind of sensors with varying transmission and sensing ranges make up the heterogeneous WSN. We must therefore take into account this disparity in transmission and sensing ranges when choosing the nodes of sensor for intrusion detection. For instance, it is preferable to choose the node with the greater transmission range when two nodes have varied transmission ranges. In this research, N types of sensors are taken into consideration. Here, Type 1 has a greater sensing range and transmission range than Type 2, and so forth.

The sensors are placed in an area A = L x L uniformly and independently.

Methodology

Cluster Oriented Heterogeneous Wireless Sensor Network (HWSN) is vulnerable to different kind of attacks such as jamming, introducing flood, forwarding of selective things, sinkhole, Sybil, alteration of packet, bad mouthing, etc. because it consists of small sensing nodes that are implanted in a hostile or remote area, such as a battlefield. According to my observations, the current intrusion detection systems are unable to withstand all attacks and have several flaws, such as a high false positive rate and a low detection rate. Additionally, since they are not included in the model foundation, unknown attacks cannot be detected.

Consequently, the system's performance suffers as a result. In order to enhance the lifespan of the network, the energy-efficient multipath routing mechanisms must be designed as well as Intrusion Detection Systems, which require a

significant amount of the sensor node's energy. The intended research schedule is listed below.

- To research more broad and damaging intrusion detection and the multipath routing oriented tolerance methods to counteract given attacks. Each of these attacks has a different impact on energy use, security, and reliability.
- It's also important to take into account cunning and sneaky attackers who can carry out various targeted attacks, hold specific strategic nodes along with a higher likelihood, switch between good and bad conduct, and work together with other attackers to evade intrusion detection.
- For looking at the usage of "weighted voting," which makes use of neighbor node knowledge of trust and reputation, to improve intrusion detection.

Result Analysis Methods

Due to the diverse character of SNs in Cluster-Based WSN, CH has better capability than generic SN. Subsequently, as CH compiles sensed dataset from SNs, it is frequently attacked. The CH employed to detect intruders effectively decreases the amount of information in the entire network while also reducing energy consumption. These characteristics describe the Cluster-Based WSN.

- Self-management
- Multipath routing and short-range broadcasting communication
- Widespread use of the sensors
- Constant topology changes brought on by node failures and fading
- Restrictions on computing resources, such as memory and battery life

The suggested research, hierarchical system of trust management for a trust-oriented intrusion detection framework is taken into account using "weighted voting," which makes use of neighbor nodes' knowledge of trust and reputation. According to the specifications and limitations of a voting algorithm, voting entails the creation of the data of output object through a set of n objects of input data. Voting is a technique used in data fusion to combine data from many sources (such as sensors) whose outputs may be inaccurate, delayed, or altogether absent. Voting is necessary in highly reliable systems to decide if the redundant units of hardware, separate software, same hardware and modules of software with different data, and different other sets of redundant hardware, software, and/or data, constitute the multiple processing channels.

The other algorithms of voting primary goal are to produce highly reliable outputs from redundant units in order to raise the level of dependability for the entirely critical system. In order to achieve this goal, the best approaches to construct any voting algorithm design technique is to take into account the characteristics/nature of voting algorithms and notion linked with theory of each evaluation parameter. The proposed design strategy, which is based on a thorough comprehension of the idea of dependability, significantly lowers the ratio of false positives (FPs) and false negatives (FNs). A popular fault-masking technique for improving the reliability of real-time critical computer systems is the voting algorithm. The performance of the entire system can be clearly impacted by a voter's dependability. As a result, a critical component of evaluating voting algorithms is quantifying the dependability features for the results. redundant software or data.

Heterogeneous WSN

Various kinds of sensors with varying sensing and the transmission ranges make up the heterogeneous WSN. Therefore, these disparities in detecting and transmission range must be taken into account while choosing the sensor nodes for intrusion detection. For instance, it is preferable to choose the node with the greater transmission range when two nodes have varied transmission ranges. In this research, N types of sensors are taken into consideration. Here, Type 1 has a greater sensing range and transmission range than Type 2, and so forth. The sensors are placed in an area A = LxL uniformly and independently. The 2D Poisson point distribution of the sensors is produced by such a random sensor deployment. A sensor's sensing the coverage area, which is a disc with a radius rs and is located at the sensor, is the only place where the intrusion can be detected.

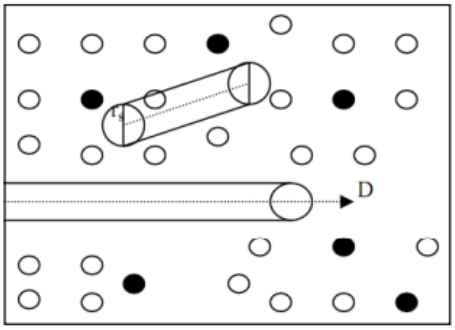

Fig. 1: The Area Shifted by Intruder

Considering Figure 1, where the intruder is seen coming through the boundary and moving D distances. The intruder is only recognized when a sensor is present in the area where they are moving. In this work, only straight paths are taken into account. The scenario where the invader enters from the boundary is depicted in the Figure 1. The area where the invader moved here.

$$S = 2^{*}D^{*}r_s + \Pi r_s^2/2$$

The given section shifted through the intruder is depicted in the Figure 1 and if the intruder enters the WSN region through a random position, ex: the intruder got dropped through the air. This space is provided by

$$S = 2^{*}D^{*}r_s + \Pi r_s^2$$

Algorithm

The node selection algorithm makes an effort to choose nodes with higher capacities than the competition. Large sensing and transmission ranges are indicative of high capacity.

type I sensor set in the WSN region, Si.

All sensors in the S-set

N(a)- collection of node a's neighbours

Repeat

For i=1 to N

Select node a with min N(a) in set Si

If N(a)≠Ø

Select a

SN= {j/the distance between a and N(a)<(rsi/2)}

If |SN|>1

S=S-(SN U a)

Else S= S-a

until S is set to null.

Based on node type, transmission range, and sensing range, the algorithm chooses a specific group of the nodes to covered the entire area.

Model for Single Sensing Detection

As previously stated, a intruder is only identified at the time it enters into the range of sensing of a certain sensor node. An intruder crosses a border and the barrier is protected by sensors, the intruder is immediately recognized as it gets inserted the WSN region. If not, it must shift a predetermined the distance i.e, D before being picked up through any sensor.

1st Theorem

In time an intruder enters a heterogeneous WSN, the chance P(D) that a intruder will be promptly identified is provided by ni is the number of type I nodes got activated in the areas rsi2/2.

$$p(D = 0) = 1 - \prod_{im1}^{N} e^{-n_i}$$

2nd Theorem

It is possible to determine the probability P(D) that the intruder will be found in the given heterogeneous WSN as where ni is the number of sensors taking part in the intrusion detection region. Assume that is the maximum intrusion distance permissible for a specific application.

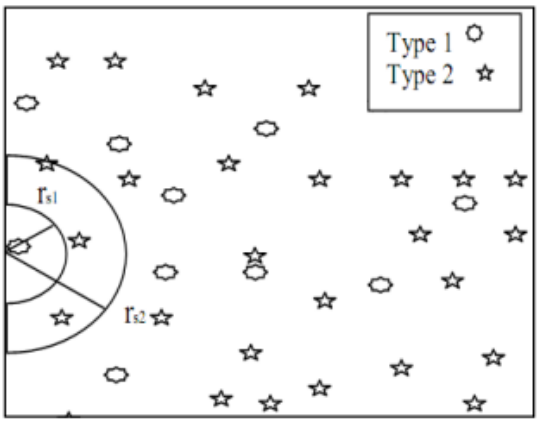

Figure 2: The Section got Covered through the Sensors at the Boundary

$$p(D \le \eta) = 1 - \prod_{i=0}^{N} e^{-n_i}$$

Process of Simulation and the Verification

In the process of simulation, there are 2 different kinds of the nodes. We are changing the settings in this case, such as the range of sensing, range of transmission, count of sensors, etc., to reach the desired outcome. The sensors are evenly spaced out over a two-dimensional area measuring 1000*1000 metres. The maximum permissible incursion distance is 50 metres, while the sensing range varies from 0 to 50 metres. The probability of detection is depicted on the graph. The analytical model is proven to be accurate since the probability of detection stays the same as it did in the case of the analytical data. Single-Sensing of detection could be seen in the illustration. It is obvious that the likelihood of single-sensing of detection is larger than the probability of multiple-sensing detection. It is due to the tougher requirements placed on identifying the intruder by multi-sensing detection (e.g., the requirement of at least 3 sensors).

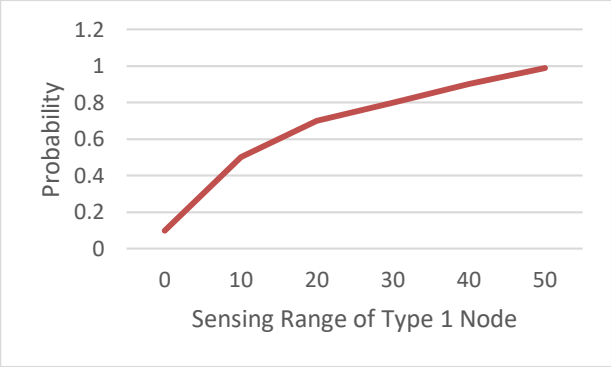

Fig. 3: Probability Analysis

The graph in this case was created by adjusting the sensing which ranges from 0 to 50. Each graph point is the outcome of 100 in the simulations. In order to obtain every point, we must run the simulation 100 times, from which we can calculate the probability. Here, we see that single sensing is also feasible at shorter distances. However, the results of multi sensing will take some time to come in.

Because it requires multiple sensors (here, three sensors in this simulation) for the detection of the intruder. An average amount of nodes chosen by applying the above-mentioned technique is shown in Fig. 4. To determine how many type 1 nodes are activating their IDS module, the density of the type 1 nodes is changed. The number of Type 2 sensors used in this simulation is fixed at 400. The transmission range and sensing ranges are both set at 40. Type 1 has a 45-degree sensing and transmission range. Each execution varies the number of type 1 nodes to see how the selection process will be impacted.

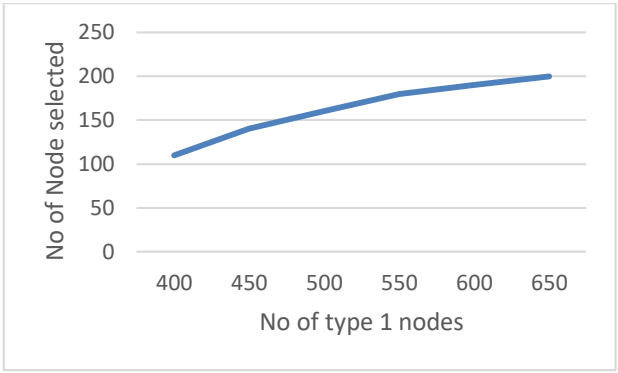

Fig. 4: The Numbers of the Node Selected

Analysis of this algorithm is energy usage is shown in Fig. 5, which is provided below. Here, we contrasted our work with the reference material. We presumed that one unit of energy is consumed by the 1 node for one unit of time. Given graph makes the efficiency of energy very evident.

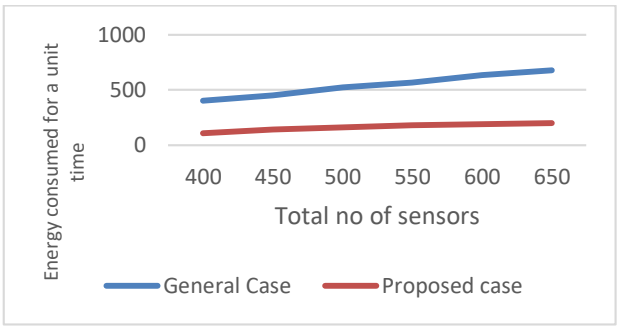

Fig 5: Energy Used

Analysis

WSNs can be utilized in a variety of applications, each with unique characteristics and specifications. So, new techniques, algorithms, and designs are required for this variety of applications. In WSNs, an enemy can threaten a sensor node, alter the data, inject false messages, misbehave on the route, and squander sensor resources. Although there are some restrictions on how security can be implemented in WSNs, including those related to energy, storage, communication, compute, and processing capacities, the issue of security must be taken

into account. As a result, to meet requirements of application, building security protocols necessitates an awareness of these constraints and attaining respectable performance with security measures.

In order to conserve as much of the restricted sensor energy in WSNs as feasible, protocols must adhere to the security level requirement. IDS in WSNs must therefore identify intrusion without endangering sensor energy dissipation. The secured routing protocol for the a WSN aims to guarantee the availability, integrity, and authentication of communications. The majority of WSN routing protocols are susceptible to numerous forms of the attacks, such as adversary nodes advertising routes to fake nodes.

Different strategies can be used to address these issues, such as adequate authentication or building trust tables within each node to make sure that only valid group nodes are receiving broadcast and multicast communication. The CHs are the major targets of attackers in hierarchical routing, which is based on clustering, because they gather data from their neighbors in their clusters and then transfer or deliver it to the BS. This is relevant to the various routing protocols in WSNs. Therefore, securing the CHs in hierarchical routing can help to extend the lifespan of the networks and save energy usage in addition to helping to detect attacks. Finding a good route to the BS and preventing route misbehavior, though, must be taken into account in this routing protocol.

Conclusion

This study covers the likelihood of the intrusion detection in the heterogeneous wireless sensor network (wsn) got deployed in the two-dimensional region as well as the energy-efficient minimization of external intrusion detection. In order to successfully identified as an intruder in the specific wireless sensor network, this probability gives information on the number of sensors that must be deployed as well as their detecting and transmission ranges (wsn). We created an analytical based model for the intrusion detection for heterogeneous WSNs and applied it in both single-sensing detection and multiple-sensing of detection scenes. Here accuracy of the analytical model is shown by the simulation. It considered both single-sensing detection and multiple-sensing detection models. We can mathematically express the probability of intrusion detection within a specific intrusion distance under different application circumstances thanks to the analytical model for intrusion detection. In a heterogeneous WSN, we additionally take network connectivity and broadcast reachability into account.

The simulation findings demonstrate that the suggested analytical model is accurate. Insights into constructing homogeneous and heterogeneous WSNs are provided by this work, which also aids in choosing crucial network characteristics to satisfy application needs.

Future Scope

By using a diverse approach to intrusion detection, assaults on the integrity of service, the authentication, and the secrecy are detected. a heterogeneous IDS framework that combines numerous cutting-edge techniques to increase the likelihood of intrusion detection in WSNs. On the KDD 1999 Cup dataset, various studies that compared the performance of the proposed IDS technique with the K-M algorithm revealed that the MLP does detection above 85% of the record of attacks for the probing, above 94% for DoS, and above 96% for R2L categories. It demonstrated good outcomes in identifying false alarms as well. In the future, some more cutting-edge methods for intrusion detection in WSNs will be taken into consideration.

References

[1] Bleda, F. Fernandez-Luque, A. Rosa, J. Zapata and R. Maestre, “Smart sensory furniture based on WSN for ambient assisted living,” IEEE Sensors Journal, vol. 17, no. 17, pp. 5626–5636, 2017.

[2] J. Wu, K. Ota, M. Dong and C. Li, “A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities,” IEEE Access, vol. 4, pp. 416–424, 2016.

[3] S. Jokhio, I. Jokhio and A. Kemp, “Light-weight framework for security-sensitive wireless sensor networks applications,” IET Wireless Sensor Systems, vol. 3, no. 4, pp. 298–306, 2013.

[4] F. Valeur, G. Vigna, C. Kruegel and R. Kemmerer, "Comprehensive approach to intrusion detection alert correlation," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 146–169, 2004.
[5] Mishra, K. Nadkarni and A. Patcha, "Intrusion detection in wireless adhoc networks," IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, 2004.
[6] N. Ye, Q. Chen and C. Borror, "EWMA forecast of normal system activity for computer intrusion detection," IEEE Transactions on Reliability, vol. 53, no. 4, pp. 557–566, 2004.
[7] R. Erbacher, K. Walker and D. Frincke, "Intrusion and misuse detection in large-scale systems," IEEE Computer Graphics and Applications, vol. 22, no. 1, pp. 38–47, 2002.
[8] Hoyle, M. Rau, K. Paech, C. Bonnett, S. Seitz et al., "Anomaly detection for machine learning redshifts applied to SDSS galaxies," Monthly Notices of the Royal Astronomical Society, vol. 452, no. 4, pp. 4183–4194, 2015.
[9] Sun, L. Osborne, Y. Xiao and S. Guizani, "Intrusion detection techniques in mobile adhoc and wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 56–63, 2007.
[10] Y. Wang, X. Wang, B. Xie, D. Wang and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.
[11] S. Shin, T. Kwon, G. Jo, Y. Park and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," IEEE Transactions on Industrial Informatics, vol. 6, no. 4, pp. 744–757, 2010.
[12] S. Bu, F. Yu, X. Liu and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," IEEE Transactions on Wireless Communications, vol. 10, no. 9, pp. 3064–3073, 2011.
[13] F. Bao, I. Chen, M. Chang and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169–183, 2012.
[14] M. Wei and K. Kim, "Intrusion detection scheme using traffic prediction for wireless industrial networks," Journal of Communications and Networks, vol. 14, no. 3, pp. 310–318, 2012. IASC, 2023, vol.35, no.1 723
[15] J. Chen, J. Li and T. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors: Global and local," IEEE Transactions on Wireless Communications, vol. 12, no. 9, pp. 4742–4755, 2013.
[16] Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman and W. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013.
[17] Sun, X. Shan, K. Wu and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," IEEE Systems Journal, vol. 7, no. 1, pp. 13–25, 2013.
[18] V. Matyas and J. Kur, "Conflicts between intrusion detection and privacy mechanisms for wireless sensor networks," IEEE Security & Privacy, vol. 11, no. 5, pp. 73–76, 2013.
[19] G. Han, J. Rodrigues, J. Jiang, L. Shu and W. Shen, "IDSEP: A novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," IET Information Security, vol. 7, no. 2, pp. 97–105, 2013.
[20] H. Moosavi and F. Bui, "A Game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1367–1379, 2014
[21] Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography. Computers and Electrical Engineering, 102, 108205.
[22] Gupta, S., Iyer, S., Agarwal, G., Manoharan, P., Algarni, A. D., Aldehim, G., & Raahemifar, K. (2022). Efficient Prioritization and Processor Selection Schemes for HEFT Algorithm: A Makespan Optimizer for Task Scheduling in Cloud Environment. Electronics, 11(16), 2557.

[23] Balyan, A. K., Ahuja, S., Lilhore, U. K., Sharma, S. K., Manoharan, P., Algarni, A. D., ... & Raahemifar, K. (2022). A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. Sensors, 22(16), 5986.

[24] Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework. Computer Communications.

[25] Ramesh, T. R., Lilhore, U. K., Poongodi, M., Simaiya, S., Kaur, A., & Hamdi, M. (2022). PREDICTIVE ANALYSIS OF HEART DISEASES WITH MACHINE LEARNING APPROACHES. Malaysian Journal of Computer Science, 132-148.

[26] Poongodi, M., Malviya, M., Hamdi, M., Vijayakumar, V., Mohammed, M. A., Rauf, H. T., & Al-Dhlan, K. A. (2022). 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun., 16(5), 442-448.

[27] Poongodi, M., Malviya, M., Kumar, C., Hamdi, M., Vijayakumar, V., Nebhen, J., & Alyamani, H. (2022). New York City taxi trip duration prediction using MLP and XGBoost. International Journal of System Assurance Engineering and Management, 13(1), 16-27.

[28] Poongodi, M., Hamdi, M., & Wang, H. (2022). Image and audio caps: automated captioning of background sounds and images using deep learning. Multimedia Systems, 1-9.

[29] Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[30] Ramesh, T. R., Vijayaragavan, M., Poongodi, M., Hamdi, M., Wang, H., & Bourouis, S. (2022). Peer-to-peer trust management in intelligent transportation system: An Aumann's agreement theorem based approach. ICT Express.

[31] Hamdi, M., Bourouis, S., Rastislav, K., & Mohmed, F. (2022). Evaluation of Neuro Image for the Diagnosis of Alzhimer's Disease Using Deep Learning Neural Network. Frontiers in Public Health, 35.

[32] Poongodi, M., Hamdi, M., Malviya, M., Sharma, A., Dhiman, G., & Vimal, S. (2022). Diagnosis and combating COVID-19 using wearable Oura smart ring with deep learning methods. Personal and ubiquitous computing, 26(1), 25-35.

[33] Sahoo, S. K., Mudligiriyappa, N., Algethami, A. A., Manoharan, P., Hamdi, M., & Raahemifar, K. (2022). Intelligent Trust-Based Utility and Reusability Model: Enhanced Security Using Unmanned Aerial Vehicles on Sensor Nodes. Applied Sciences, 12(3), 1317.

[34] Muniyappan, A., Sundarappan, B., Manoharan, P., Hamdi, M., Raahemifar, K., Bourouis, S., & Varadarajan, V. (2022). Stability and numerical solutions of second wave mathematical modeling on covid-19 and omicron outbreak strategy of pandemic: Analytical and error analysis of approximate series solutions by using hpm. Mathematics, 10(3), 343.

[35] Rawal, B. S., Manogaran, G., & Poongodi, M. (2022). Implementing and Leveraging Blockchain Programming.

[36] Bourouis, S., Band, S. S., Mosavi, A., Agrawal, S., & Hamdi, M. (2022). Meta-Heuristic Algorithm-Tuned Neural Network for Breast Cancer Diagnosis Using Ultrasound Images. Frontiers in Oncology, 12, 834028.

[37] Lilhore, U. K., Poongodi, M., Kaur, A., Simaiya, S., Algarni, A. D., Elmannai, H., ... & Hamdi, M. (2022). Hybrid Model for Detection of Cervical Cancer Using Causal Analysis and Machine Learning Techniques. Computational and Mathematical Methods in Medicine, 2022.

[38] Dhiman, P., Kukreja, V., Manoharan, P., Kaur, A., Kamruzzaman, M. M., Dhaou, I. B., & Iwendi, C. (2022). A Novel Deep Learning Model for Detection of Severity Level of the Disease in Citrus Fruits. Electronics, 11(3), 495.

[39] Dhanaraj, R. K., Ramakrishnan, V., Poongodi, M., Krishnasamy, L., Hamdi, M., Kotecha, K., & Vijayakumar, V. (2021). Random Forest Bagging and X-Means Clustered Antipattern Detection from SQL Query Log for Accessing Secure Mobile Data. Wireless Communications and Mobile Computing, 2021.

[40] Maurya, S., Joseph, S., Asokan, A., Algethami, A. A., Hamdi, M., & Rauf, H. T. (2021).

Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT. Sensors, 21(23), 7793.

[41] Poongodi, M., Nguyen, T. N., Hamdi, M., & Cengiz, K. (2021). Global cryptocurrency trend prediction using social media. Information Processing & Management, 58(6), 102708.

[42] Poongodi, M., Sharma, A., Hamdi, M., Maode, M., & Chilamkurti, N. (2021). Smart healthcare in smart cities: wireless patient monitoring system using IoT. The Journal of Supercomputing, 77(11), 12230-12255.

[43] Rawal, B. S., Manogaran, G., & Hamdi, M. (2021). Multi-Tier Stack of Block Chain with Proxy Re-Encryption Method Scheme on the Internet of Things Platform. ACM Transactions on Internet Technology (TOIT), 22(2), 1-20.

[44] Poongodi, M., Malviya, M., Hamdi, M., Rauf, H. T., Kadry, S., & Thinnukool, O. (2021). The recent technologies to curb the second-wave of COVID-19 pandemic. Ieee Access, 9, 97906-97928.

[45] Rawal, B. S., Manogaran, G., Singh, R., Poongodi, M., & Hamdi, M. (2021, June). Network augmentation by dynamically splitting the switching function in SDN. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE. Poongodi, M., Hamdi, M., Varadarajan, V., Rawal, B. S., & Maode, M. (2020, July). Building an authentic and ethical keyword search by applying decentralised (Blockchain) verification. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 746-753). IEEE.

[46] Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. IEEE Access, 7, 158481-158491.

[47] Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS detection mechanism using trust-based evaluation system in VANET. IEEE Access, 7, 183532-183544.

[48] M. M. Kamruzzaman, ""New Opportunities, Challenges, and Applications of Edge-AI for Connected Healthcare in Smart Cities,"" 2021 IEEE Globecom Workshops (GC Wkshps), 2021, pp. 1-6, doi: 10.1109/GCWkshps52748.2021.9682055."

[49] Md Selim Hossain, MM Kamruzzaman, Shuvo Sen, Mir Mohammad Azad, Mohammad Sarwar Hossain Mollah, Hexahedron core with sensor based photonic crystal fiber: An approach of design and performance analysis," Sensing and Bio-Sensing Research, 32, 100426

[50] Mingju Chen, Xiaofeng Han, Hua Zhang, Guojun Lin, M.M. Kamruzzaman, Quality-guided key frames selection from video stream based on object detection, Journal of Visual Communication and Image Representation, Volume 65, 2019, 102678, ISSN 1047-3203

[51] M. M. Kamruzzaman: Performance of Decode and Forward MIMO Relaying using STBC for Wireless Uplink. JNW 9(12): 3200-3206 (2014)

[52] M. M. Kamruzzaman, "Performance of Turbo Coded Vertical Bell Laboratories Layered Space Time Multiple Input Multiple Output system," Computer and Information Technology (ICCIT), 2013 16th International Conference on, Khulna, 2014, pp. 455-459.

[53] Yan Zhang, M. M. Kamruzzaman, and Lu Feng "Complex System of Vertical Baduanjin Lifting Motion Sensing Recognition under the Background of Big Data," Complexity, vol. 2021, Article ID 6690606, 10 pages, 2021. https://doi.org/10.1155/2021/6690606

[54] Md Hossain , MM Kamruzzaman , Shuvo Sen, Mir Mohammad Azad, Mohammad Sarwar Hossain Mollah , Hexahedron Core with Sensor Based Photonic Crystal Fiber, 2021

[55] Md Nazirul Islam Sarker, Md Lamiur Raihan, Yang Peng, Tahmina Chumky, MM Kamruzzaman, Roger C Shouse, Huh Chang Deog, "COVID-19: Access to Information, Health Service, Daily Life Facility and Risk Perception of Foreigners during Coronavirus pandemic in South Korea," Archives of Medical Science, 2021, https://doi.org/10.5114/aoms/141164

[56] Y. Shi, S. Wang, S. Zhou and M. M. Kamruzzaman. (2020). Study on Modeling Method of Forest Tree Image Recognition

Based on CCD and Theodolite. IEEE Access, vol. 8, pp. 159067-159076, 2020, doi: 10.1109/ACCESS.2020.3018180

[57] Guobin Chen, Zhiyong Jiang, M.M. Kamruzzaman. (2020). Radar remote sensing image retrieval algorithm based on improved Sobel operator, Journal of Visual Communication and Image Representation, Volume 71, 2020, 102720, ISSN 1047-3203 https://doi.org/10.1016/j.jvcir.2019.102720.

[58] Yuanjin Xu, Ming Wei, M.M. Kamruzzaman, Inter/intra-category discriminative features for aerial image classification: A quality-aware selection model,Future Generation Computer Systems,Volume 119,2021,Pages 77-83,ISSN 0167-739X,https://doi.org/10.1016/j.future.2020.11.015.

[59] Xing Li, Junpei Zhong, M.M. Kamruzzaman, "Complicated robot activity recognition by quality-aware deep reinforcement learning", Future Generation Computer Systems,Volume 117, 2021, Pages 480-485.

[60] Bin Yuan, M. M. Kamruzzaman, Shaonan Shan, "Application of Motion Sensor Based on Neural Network in Basketball Technology and Physical Fitness Evaluation System", Wireless Communications and Mobile Computing, vol. 2021, Article ID 5562954, 11 pages, 2021. https://doi.org/10.1155/2021/5562954

[61] Chi, Z., Jiang, Z., Kamruzzaman, M.M. et al. Adaptive momentum-based optimization to train deep neural network for simulating the static stability of the composite structure. Engineering with Computers (2021). https://doi.org/10.1007/s00366-021-01335-5