REPEATED NODE BEHAVIOUR ANALYSIS WITH NODE TRANSMISSION PATTERN ANALYSIS BASED BEHAVIORAL INDEX FOR FALSE ALARM DETECTION IN WIRELESS SENSOR NETWORKS

D. MURLI KRISHNA REDDY[1], DR. R. SATHYA[2], DR.V.V.A.S. LAKSHMI [3]

[1] Research Scholar in CSE Department, Annamalai University, Chidambaram,Tamil Nadu, India
[2]Assistant professor in CSE Department, Annamalai University, Chidambaram,Tamil Nadu, India
[3]Professor &HOD in CSE(AI&ML), Narasaraopet Engineering College, Narasaraopet, India
E-mail: [1]murali.aucse@gmail.com , [2]sathya.aucse@gmail.com , [3]vvaslakshmi@gmail.com

ABSTRACT

Multiple types of sensor failures and inaccurate readings can compromise the integrity of a Wireless Sensor Network (WSN). The inability to quickly and accurately respond to emergencies is a major flaw in many WSN applications. In this research, a unique method for identifying sensor abnormality through the examination of physiological data gathered is proposed. Wireless sensor networks have a number of issues, one of the most significant being security. This research focuses mainly on the characteristics of a layered sensor node and its application in an intrusion detection system due to energy and processing constraints. The method's purpose is to accurately discern between false and true intrusion alarms. It does a comparison between the calculated sensor value and the current reading. The sensor reading is compared to a moving threshold value that indicates whether or not the reading is abnormal. This paper examines strategies for dynamically and efficiently decreasing the possibility of false alarms while increasing the likelihood that no target would go unnoticed. The proposed method adjusts the false positive rate threshold up or down when the false positive rate changes. The likelihood of identifying false alarms improves as a result. The findings recommend pooling data from multiple sensors to produce a comprehensive analysis of the target while keeping intrusions to a minimum. The nodes in the WSN are vulnerable to several sorts of intrusions. The node behaviour analysis is performed to identify the node actions frequently in the WSN. The nodes that are causing false alarms need to be identified for improving the network performance levels. This research presents a Repeated Node Behaviour Analysis with Node Transmission Pattern Analysis based Behavioral Index (RNBA-NTPA-BI)model is proposed for reduction of false alarms in the network. The proposed model is compared with the traditional model by considering the evaluation metrics like node behaviour analysis accuracy levels, false alarms detection accuracy levels. The proposed model exhibits better performance when compared to the traditional models.

Keywords: *Wireless Sensor Networks, Intrusion Detection, False Alarms, Node Behaviour Analysis, Behavioral Index, Network Performance.*

1. INTRODUCTION

A WSN is made up of a collection of battery-operated sensor nodes that are capable of basic physical sensing but have limited data storage, computing capacity, and range. These sensor networks have many different fields of usage [1]. Each sensing node is equipped with a sensing device to collect environmental data. It also has a wireless communication component and a processing unit for handling data locally. Limitations on processing power and energy consumption both apply to this type of wireless sensor network. Today's high-data-intensity uses for WSNs reflect their widespread adoption in both low-power hardware architecture and communication protocols [2]. These kinds of advancement for different applications in wireless sensing and technology for networking are definitely the main facilitators for the successful integration of the physical and cyber worlds [3].

Sensor data reliability issues are also being caused by transmission errors. All of which could lead to a high proportion of false positives [4]. These false positives cause unnecessary delays and disruptions in intrusion detection. Since the gathering of inaccurately produced data can inject the system and can constitute the system, leading to a high number of false alarms, accurate detection of data imperfections at the sensor node is crucial [5]. With continuous monitoring, more and more information is collected as time goes on. This situation necessitates a system with both rapid processing and alarm production [6]. Many different methods for identifying and dismissing false alarms have been developed and implemented. The resource required is usually insufficient for battery driven wireless sensors [7]. The sensors' power can be quickly depleted when using the centralized approach, which is not an energy-efficient method of routing in WSN [8]. In this case, information must be sent to a sink for processing. In this study, a false-alarm detection system is introduced that is both new and effective, with its adaptive and intelligent design [9]. The analysis of intrusions relies heavily on establishing whether or not the abnormal data are actually incorrect [10].

Due to sensor malfunction and resource constraint of the sensor node, such as limitation of power and transmission capability, collected sensor data may be inaccurate [11]. Sensor movement, transmission interference, and malicious data insertion are also potential causes of inaccurate data. Because of possible transmission errors, the sensor data may potentially be incorrect, increasing the likelihood of false alarms [12]. To prevent the system from being compromised and false alarms from being generated, it is crucial to detect data inconsistencies at sensor nodes. When data is collected in real time, the volume of information grows [13].

An Intrusion Detection System (IDS), often known as an additional layer of defense, is used solely for spotting intrusions; it cannot stop or respond to them. The controller is alerted to the attack via an alarm generated by the IDSs [14]. An intrusion detection system that relies on predefined rules is called a signature-based IDS. While rule-based IDS is quite effective at spotting common assaults, it is helpless against zero-day exploits whose signatures aren't already in the intrusion database [15]. IDSs that identify intrusion based on anomalies in traffic or resource use do so by comparing the two. However, there are more false positive and false negative alarms with anomaly based IDSs despite their capacity to identify both known and new assaults [16]. Some IDSs only function in certain environments or with certain routing protocols. Proactive routing protocol is used to identify any abnormalities in the network's routing [17]. Due to its distributed nature, it requires coordination amongst nodes to identify malicious routing activity and to detect the false alarms in the network. The Intrusion Detection System is shown in Figure 1.

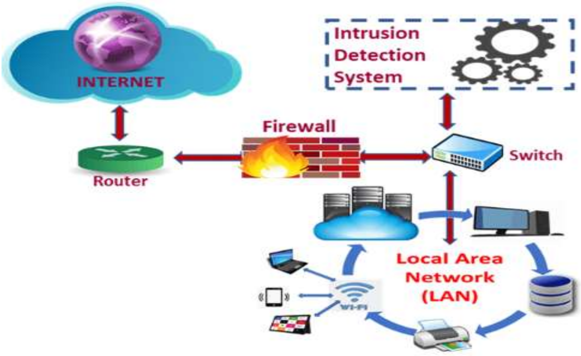

Figure 1: Intrusion Detection System

An IDS keeps monitoring a network for any signs of trouble. It's true to some extent because IDS approaches often need a lot of computation time. A WSN's knowledge on the enemy's whereabouts, however, can be important for creating a plan of action to rout them from a certain territory [18]. As technology advances at a rapid clip and future prospects are taken into account, sensor node capabilities will also rise in the near future. Multimedia data transfer and underwater applications are two potential areas where sensor nodes' greater storage capacity and operating longevity could prove useful [19]. Sensor technology has advanced to the point that these networks will soon be visible and a normal part of our lives [20]. Therefore, a secure WSN is needed to guarantee the safety of data during transmission and the timely delivery of data packets. Denial-of-service attacks, Sybil nodes, and other malicious activity on the part of sensor nodes can often be detected using IDS-based processes [21]. An IDS agent is what keeps an eye out for anything fishy happening on a network. An IDS agent keeps an eye on a network, processes the data it gathers through a detection strategy, and acts on any anomalies it finds [22]. Although many researchers have presented IDS-based security solutions that analyze the operation of sensor node(s) and accurately detect anomalous activity, lowering the false alarm rate is still difficult [23]. Where they differ most is in the detection policies and the process of installing the IDS agent [24]. There are three possible architectures for an IDS agent: centralized, distributed, and hybrid. In the first approach, everything is set up in one place—the sink or base station—while in the second approach, everything is set up independently at each sensor node [25]. The third tactic leverages monitor nodes to continuously keep an eye out for intruders. The Figure 2 shows the Malicious Nodes Generates False Alarms in the WSN.

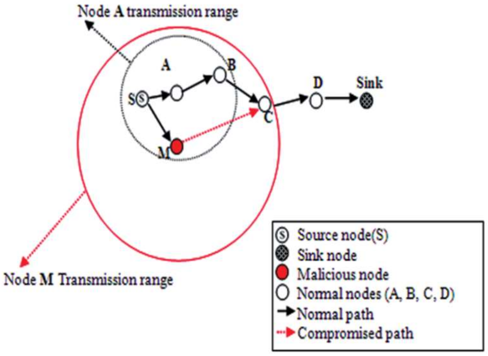

Figure 2: Malicious Nodes Generates False Alarms

In this research, we offer a unique way for detecting sensor anomaly and lowering the number of false alarms generated by these systems by using prediction-based approaches for making comparisons and identifying anomalies. Despite the fact that anomalous values in healthcare are unimportant, classic anomaly detection methods [26] can detect and reject abnormalities from the data. Therefore, it is crucial to do thorough anomaly analysis to establish whether the numbers in question are in fact inaccurate or indicative of genuine medical issues [27]. This evaluation is used to decide whether or not to trigger a real alert. The proposed anomaly detection approach [28] makes use of the correlation between the time and location of physiological variables. Using both past experience and the data sent from various sensor nodes to the base station or to nodes with more powerful processing and memory capacity, a prediction model is constructed. An error computation using a dynamic threshold is performed, and then a majority voting analysis is performed, to identify the sensor outlier and activate alerts. The proposed method has been tested and compared to other methods using real-world network datasets. In addition to a high Detection Rate (DR) and a low False Positive Rate (FPR), experimental findings demonstrate the efficacy of the suggested method.

2. LITERATURE SURVEY

The cyber physical system relies heavily on WSNs, which are self-organizing, multi-hop networks made up of many individual sensors. It works together to sense, collect, process, and transmit data about perceived objects in the network's coverage area, and then delivers that data to the network's owner. Some common attacks in WSN can do serious damage quickly. These include the Blackhole, Grayhole, Flooding, and Scheduling strikes. Since sensor nodes have limited resources and data from the network is redundant and highly correlated, intrusion detection methods for WSN have drawbacks such as a poor detection rate, a substantial calculation overhead, and a high false alarm rate. In light of these issues, Jiang et al. [1] presented SLGBM, a novel intrusion detection technique tailored specifically for WSNs. In order to cut down on processing time, the author first applied the sequence backwards selection (SBS) algorithm on the original traffic data and lowered the dimension of the data in the feature space. Then, various network assaults are identified using a LightGBM algorithm.

IDSs have a tough time keeping up with the ever-changing nature of network threats. With a high false alarm rate (FAR), low recognition accuracy (ACC), and weak generalization capacity, traditional attack recognition systems typically utilize mining data correlations to find abnormalities. Hu et al. [2] proposed a revolutionary intrusion detection approach utilizes an enhanced convolutional neural network (CNN) in conjunction with the adaptable synthetic sampling (ADASYN) algorithm to enhance the existing comprehensive capabilities of IDS and bolster network security. To start, the author applied the ADASYN technique to ensure a more uniform distribution of data points across the sample, which helps the model avoid overreacting to large or small samples. Second, the split convolution module (SPC-CNN) is the foundation of the enhanced CNN, which can expand the feature space and mitigate the effect of redundant interchannel data on model development.

The existence of sea mounts, underwater ridges, and other topographic features makes it difficult to operate high-resolution, broadband, antisubmarine operations sonars in littoral waters, leading to an increase in false alarm rates. The existence of sonar clutter, also known as a non-Rayleigh distributed matching filter envelope, and the signal-processing-induced phenomena known as false alarm rate inflation (FARI) are two major contributors to the increased false alarm rate. Traditional CFAR algorithms can't maintain a constant false alarm rate across all possible ranges and weights when these factors are present. An acoustic model can be used to estimate FARI occurrence if enough data on bathymetry and bottom parameters is available. The true false alarm rate can thus be estimated with more precision. To overcome the challenges posed by FARI and clutter, Hjelmervik et al. [3] presented a new detection methodology that makes use of this method to estimate a range- and bearing-dependent thresholds that can be applied to normalized sonar data to produce a CFAR. Receiver operating characteristic curves are used to evaluate how well the approach performs, and the results reveal that it is superior to more traditional CFAR algorithms such cell averaging, greater of, and ordered statistics CFAR processors.

False alarms in the intensive care unit (ICU) are a major source of stress for medical staff and a waste of valuable resources. We built convolutional neural network–based classification algorithms that can directly handle time series without the need for human intervention in feature extraction to reduce false alarms in the intensive care unit. Yu et al. [4] experimented with two different network architectures, a deep group convolutional neural network (DGCN) and an embedded deep group convolutional neural network (EDGCN) that both make use of grouping as a core component. Then, to further improve performance, ensemble networks were built using the superior EDGCN. Several data extensions were also attempted in light of the small sample size. The author compared the results to the industry standard, using an indicator called Score, which is calculated as 100 percent (TP+TN) divided by five percent (FP+FN). At last, the author put this model to the test in the virtual lab, where it performed an impressive 80.68 percent correctly.

Intruder detection via wireless sensor networks is a commonplace feature of surveillance applications. The intruder detection has been the subject of numerous research studies that have examined its effectiveness in terms of detection likelihood and false alarm rate. Using an auditory signal model and a sensing probability model, users were able to tackle the problem of passive mobile intruder detection with the model proposed by Sharma et al. [5]. The existence of a mobile intruder can be inferred using a proposed three-tiered hierarchy. K-means clustering is used initially to classify the installed sensor nodes. In both cases, the intruder's distance from the sensor nodes is calculated. The sensing probabilities or received signal strengths given by the sensor nodes are used for binary hypothesis testing at the cluster head. After doing a Likelihood Ratio Test (LRT) on the combined decisions, the cluster heads send them to the fusion hub, where reliable inference about the intrusion detection is made. The optimal threshold value for the detection probability computation is found through numerical evaluation of received signals. The developed fusion rule improves the chances of detection while still maintaining acceptable false alarm rates. The number of actual detections provided by the deployed sensor nodes will determine how reliable the suggested fusion rule is.

The physical-layer maximum a posteriori (MAP) test was developed by Liu et al. [6] to detect false data in MIMO WRNs. The MAP test is designed to lower the average risk of detection mistake by using noisy information about the authentic packet received from the source nodes as a reference. For a fixed degree of certainty in the background data, the author showed that the average risk of detection error decreases exponentially with the number of source nodes. This indicates that a reliable integrity check technique for detecting incorrect data at the destination can be constructed utilizing the plethora of available source nodes. The author also provided a parallel MAP test that improves detection accuracy when the number of source nodes is low and the overhearing channel disparities are high. To further improve throughput, the author included a packet recovery mechanism to retrieve false alerted packets, which are otherwise unchanged packets that were wrongly identified as altered by the MAP test.

Small, light, cheap, and portable photoplethysmogram (PPG) monitoring systems exert a heavy burden on their meager resources, such as their batteries. As a result, there is a significant strain on charging or battery replacement for continuous PPG detecting and transmission. In addition, ambulatory and workout recording conditions usually drastically degrade PPG signals, resulting in frequent false alarms. In order to reduce unnecessary alarms and power consumption in wearable and edge PPG monitoring devices, Reddy et al. [7] suggested a unified quality-aware reduction and pulse-respiration rates estimating approach. To do this, we explore predictive coding strategies for measuring signal quality, compressing data, and predicting heart and breath rates all at once. The proposed unified architecture is evaluated using the five standard PPG databases, and its performance is measured in terms of compression ratio (CR), mean absolute error (MAE), false alarm reduction rate (FARR), processing time (PT), and energy savings (ES).

Smart management systems, which integrate WSNs and intelligent systems, are finding widespread application in the manufacturing, farming, and building industries. False positive attacks (FPAs) and false negative attacks (FNAs) using massively hacked nodes are a challenge to traditional strategies of WSN security, which have concentrated on data integrity and the discovery of anomalies in sensor data. These attacks severely threaten the sensor nodes due to the fact that the communication mechanism does not consider the correlation between node verification operations until the intercepted sensor data are used as input into the system. An FPA and FNA detection method using a knowledge foundation of spatial-temporal history data was presented by Ahn et al. [8]. The main contribution of the present study is the development of a method for identifying incorrect correlations via behavior monitoring in accordance with the discrete event system specification model. The proposed method identifies anomalous correlations and prevents the introduction of false data due to extensive destruction. To further ensure that no hacked nodes contribute to the network's collapse, an innovative strategy is recommended. The proposed spatiotemporal data-based detection method has broad applicability because it is based on a standard security paradigm.

Due to their distributed nature and open connectivity, WSNs are easy targets for a variety of attacks. For these reasons, the selective forwarding attack is among the most challenging inside assaults to detect. In a hostile environment, a node may need to discard data packets, and a cunning malicious node may go undetected. In this research, Ding et al. [9] used a reinforcement learning (RL) approach to simulate a selective forwarding attack launched by hostile smart nodes. The author developed the double-threshold density peaks clustering (DT-DPC) algorithm for detecting the selective forwarding attack under challenging conditions. Because of the persistent anomalies, aberrant nodes are quickly identified as potentially harmful and isolated. Because malicious actions manifest independently and a hostile environment uniformly upsets agglomeration nodes, the neighbor voting approach is used to identify potentially dangerous nodes. DT-DPC increases network throughput even if malevolent smart nodes evade detection by an RL algorithm.

Setting up a WSN relies heavily on accurate node localization. In WSNs, sensors collect data, analyze it, and send it out all at once. It is essential to have the location data for the information source in addition to the sensed data. Using bio-inspired meta-heuristic algorithms is a promising approach to localizing these randomly dispersed sensors. This transforms the difficulty of locating nodes into an optimization challenge. After then, the optimization issue is solved by minimizing the errors to obtain the best possible outcome. Cuckoo Search (CS) and a modified version of CS are just two examples of the bio-inspired algorithms that have been investigated. However, in order to find the best solution, these algorithms require an excessively high number of iterations. This wastefully uses up the sensors' limited resources and slows down the search. To reduce both the time it takes to locate an unknown node and the Average Localization Error (ALE), an Enhanced Cuckoo Search (ECS) technique is proposed by Kotiyal et al. [10]. By breaking out of the search loop as soon as the best possible answer is found, the Early Stopping (ES) technique built into this algorithm greatly speeds up the search time.

3. PROPOSED MODEL

Collectively monitoring environmental or physical parameters, the sensors that make up a wireless sensor network are dispersed across a given area. Battlefield surveillance is one of the original inspirations for the growth of wireless sensor networks in the military. In a wireless sensor network, environmental factors like weather and topography might affect the sensors' ability to detect anomalies. Each sensor must reliably detect events, with no false positives or negatives. Unfortunately, a sensor may miss an event or produce false alarms due to the unpredictable nature of the site. The odds of detection and the false alarm rates of intrusion detection systems are used to quantify this risk. In this study, how to improve the likelihood of intruder detection in noisy, realistic environments by accurately identifying false alarms is analyzed. The FAR is the proportion of false alarms to total event detections in a network.Every time a sensor detects an event, the false alarm rate is adjusted accordingly. Reputation values are calculated using a binomial model, with prior actions of a sensor serving as input. In this situation, the reputation value, Ri, of sensing unit i is comparable to the sensing unit's weight under the current environmental conditions. A heavier sensor would indicate that it is less susceptible to environmental influences, making it a more reliable choice.

In order to ensure that messages are reliably transmitted, it is necessary to detect the behavior of individual nodes. The malicious nodes that are obstructing the communication channel can then be identified. Identifying the bad actors responsible for packet loss is the primary challenge. Congestion refers to the total breakdown in communication that selfish nodes might generate. Disruptions to the network can occur when individual nodes alter their behavior. An unstable and underperforming network is the direct effect of the disconnected node. By identifying the malicious nodes, behavioral prediction will increase network trust. The key benefit of this prediction method is that it can identify and remove from the network any nodes that are a source of transmission failures due to either malicious intent or selfishness. The stability of the network must be taken into account when observing the pattern of activity, since high network traffic tends to disrupt connections.

Routing protocols that are both efficient and robust at the node level are essential to the stability of conventional communication networks. Trust in a WSN is established at its outer nodes through long-distance communications. In order to finish the routing process in this wireless sensor network, it is necessary to manage the forward node. A markov process in a WSN is used to identify the pattern of behavior. One of the key draws of this approach is its flexibility in allowing for localized modifications to node construction. This technique can identify malicious attempts and build confidence amongst geographically separated nodes. If an untrustworthy node is discovered, the trusted ones must change their settings. Overuse of resources happens if the node is not adjusted. A malicious node is a failure node if its abnormal behavior has an effect on the entire network. It is difficult to foresee how a network's nodes will act. Therefore, full routing is necessary for the node. If the malicious node can be identified early on, it can be brought back to normal. However, if the node is considered malicious, it must be isolated.

Multihop distributed activities are a hallmark of a WSN, but they increase the difficulty of detecting and preventing security attacks. Attackers and malicious nodes are notoriously hard to track down in multihop distributed environments. While there are several techniques to identify and mitigate security attacks on WSNs, most of the present solutions can only deal with a subset of these threats. Any illegal action taken by attackers to disrupt network resources or sensor nodes is considered an incursion. A IDS is a way to monitor network traffic for malicious or illegal actions. IDS's major purpose is to keep tabs on user behavior and network activity across multiple tiers.Since there will always be some technical weaknesses, software faults, or design flaws that may be penetrated by intruders, a single flawless defense is neither practical nor achievable in wireless networks. The best way to protect a wireless network is to set up multiple layers of defense, which is why intrusion detection systems are so important. It is considered a passive defense because it is not designed to stop assaults from happening, but rather to notify network administrators of impending attacks in plenty of time to stop them or at least mitigate their effects. This research presents a Repeated Node Behaviour Analysis with Node Transmission Pattern Analysis based Behavioral Index model is proposed for reduction of false alarms in the network. The Figure 3 shows the architecture of the proposed model.

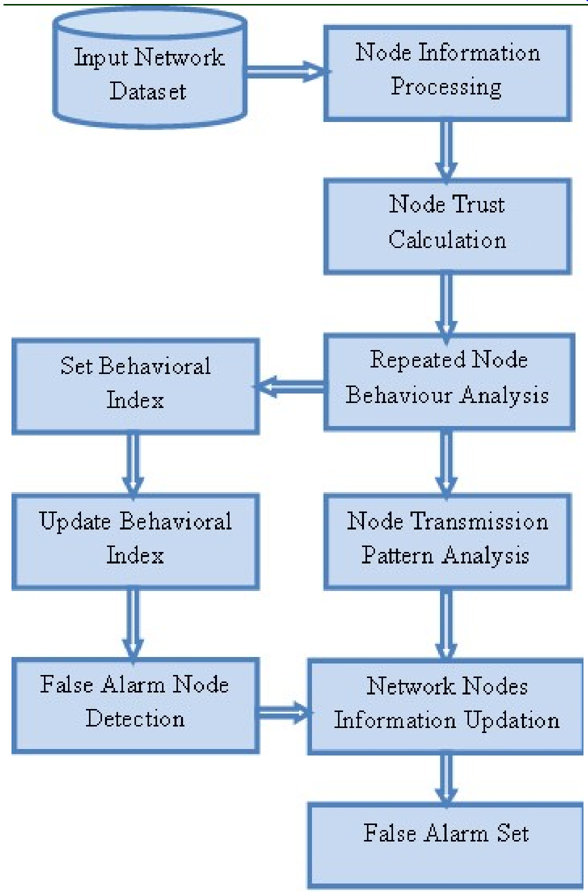
Input Network Dataset
Node Information Processing
Node Trust Calculation
Repeated Node Behaviour Analysis
Set Behavioral Index
Update Behavioral Index
Node Transmission Pattern Analysis
False Alarm Node Detection
Network Nodes Information Updation
False Alarm Set

Figure 3: Proposed Model Framework

Algorithm RNBA-NTPA-BI

{

Input: Network Dataset {NDset}

Output: False Alarm Set {FAset}

Step-1: The nodes from the network dataset are considered and the data of each node and node properties are analyzed. These properties help nodes for further recognition and each node is provided with a immutable key that is used for authentication and accessing. The node information processing and immutable token allocation is performed as

$$NodeInfo[N] = \sum_{i=1}^{N} getNodeattr(i) + TI\big(nodereg(i)\big) + getRand(i) + nodeaddr(i)$$

Here getNodeattr() model is used for considering the node properties and details for further processing. Nodereg() model is used to consider the Time instant TI and getRand() is used to consider a random value for each node and nodeaddr() model considers each node physical address.

Step-2: Each node allocated with a immutable token can utilize the network resources for initiating data transmission. The trust factor of each node is calculated which helps to identify the nodes actions and allowing them for transmission. The trust factors of nodes are calculated based on nodes performance levels. The trust factor calculation is performed as

$$PDR[N] = \sum_{i=1}^{N} \frac{\lambda(i, i+1)}{\omega}$$

$$Loss[N] = \sum_{i=1}^{N} \omega(i) - \lambda(i)$$

$$\tau[M] = \lim_{i \to N} \left(\omega(i) + \frac{\gamma(i)}{N}\right)^2$$

$$NodeTrust[N] = \prod_{i=1}^{N} \frac{getMax(PDR(i, i+1))}{N} + \min\big(Loss(i, i+1)\big) + \max(\tau(i, i+1)) \begin{cases} NodeTrust(i) \leftarrow 1 \; if \max(PDR(i), \tau(i)) \\ 0 \qquad Otherwise \end{cases}$$

λ is the model used to calculate successful transmission of data from one node to next node. ω is the total packets generated. τ is the computational capabilities of the node. γ is the range of transmission in the network.

Step-3: The proposed model considers node Behavioral Index (BI) that is used for the analysis of changes in node behaviour during data transmissions. The initialization of the BI is performed as

$$RVal[N] = \sum_{i=1}^{N} getRand(1000{,}10000)$$

$$BI[N] = \sum_{i=1}^{N} \frac{Rval(i)}{i} + Th$$

BI is the behavior index allocated for each node. The change in node behaviour results in change in BI. Th is the threshold value.

Step-4: The node behaviour analysis is performed repeatedly at regular time intervals. The nodes may turn into malicious because of malwares. The node can cause unusual traffic or change the contents of data. The malicious actions can be identified by analyzing the node properties. The node behaviour analysis is performed repeatedly and the changes in the node behaviour results in updating of BI is performed as

$$NBeh[N] = \sum_{i=1}^{N} \frac{\max(PDR(i))}{\omega} + Loss(i) + BI(i) + \beta\left(TI(NodeTrust(i))\right) \begin{cases} BI \leftarrow BI + RVal(i) & if\,(PDR < PTh\ and\ Loss > LTh) \\ continue & Otherwise \end{cases}$$

PTh is the packer transmission threshold level and LTh is the loss threshold value.β is the model for detecting the change in node trust at regular time intervals.

Step-5: The node transmission pattern analysis is performed that is used to detect the unusual patterns in the traffic. The intrusions in the network is detected based on the pattern changes and the changes in BI that is performed as

$$Intr[N] = \sum_{i=1}^{N} \frac{getattr(NodeTrust(i))}{N} + \delta(NBeh(i,i+1)) + diff(NodeTrust(i)) + diff(attr(i,i+1))$$

δ is the difference in node behaviour.

Step-6: The false alarm causing nodes are identified based on the changes in BI and node behaviour. The false alarms causing nodes are identified and such nodes can be excluded from the data transmissions to avoid malicious actions in the network. The false alarm causing nodes are identified as

$$FAset[N] = \sum_{i=1}^{N} \frac{\max(Intr(NBeh(i))}{\mathrm{N}} + \max(\mathrm{diff}(\mathrm{NodeTrust}(\mathrm{i},\mathrm{i}+1)) + \max(\delta(\mathrm{i},\mathrm{i}+1))$$

}

4. RESULTS

Security concerns have come to the fore as WSN have found widespread use in fields such as military and environmental monitoring. Without any sort of physical protections in place, the data transmitted across wireless sensor networks is extremely susceptible to intrusion. To counteract this type of assault, suitable intrusion detection methods are desperately needed. Wireless sensor networks are a type of decentralized, networked intelligence. A huge number of micro sensor nodes equipped with wireless communication and computation are dispersed across the detecting region. It can do its tasks on its own, adapting to its changing surroundings. Wireless sensor networks have very broad application prospects due to the rapid development of embedded computing technology, wireless communication technology, and distributed information processing technology.

By coordinating the actions of many small sensors, wireless sensor networks may perform continuous, real-time monitoring of any given area or object. After that, the embedded system does its thing with the data. The data is then sent through a series of nodes in a random, self-organizing wireless communication network and on to the user terminal. The procedure is vulnerable because the sensor nodes are dispersed across a vast region without any form of security or because they are operating in a hostile environment. WSNs with limited resources should avoid using elaborate security measures. Due to their low price, sensor nodes are easily seized and can then leak the key, making the entire network vulnerable to attack.

The WSN is made up of hundreds of sensor nodes, each of which is effectively a small sensor designed to keep tabs on the world around it. In places where human monitoring is impractical, such as underwater or in dangerous situations, these sensors become invaluable. WSNs can be used for a wide range of purposes, including but not limited to environmental monitoring, industrial monitoring, healthcare monitoring, and area monitoring. Incoming data packets are compared to the standard behavior to determine if they represent an intrusion. The fundamental issue of the pattern analysis and detection system is that it misses well-known attacks, despite the fact that it may detect new intrusions because it is based on a threshold for normal traffic patterns. A high false positive rate is a drawback of the traditional models, despite the fact that it has a high detection rate and incorrectly classifies only a small fraction of real intrusion attempts as regular packets. Due to its low false positive rate and excellent detection accuracy, the proposed node behaviour analysis model and pattern analysis model performs better and false alarm detection is presented in this research that achieved accurate detection. This research presents a Repeated Node Behaviour Analysis with Node Transmission Pattern Analysis based Behavioral Index (RNBA-NTPA-BI) model is proposed for reduction of false alarms in the network. The proposed model is compared with the traditional Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments (IDM-WSN-SE), Novel Wireless Network Intrusion Detection Method Based on Adaptive Synthetic Sampling and an Improved Convolutional Neural Network (NWSN-IDM-ASS-CNN) and Predicting False Alarm Rates for High-Resolution Antisubmarine Warfare Sonars in a Cluttering Environment Prone to False Alarm Rate Inflation (FAR-HRAWS-CE) models. The results represent that the proposed model performance is high than the traditional models.

The nodes that are connected will be processed for analyzing the node attributes. The node information holds the properties of the nodes that can be used for considering the nodes behaviour. The Node Information Processing Accuracy Levels of the proposed and existing models are shown in the Table 1 and Figure 4.

Table 1: Node Information Processing Accuracy Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	97.8	93	91	92.5
40000	97.9	93.3	91.3	93
60000	98	93.6	91.5	93.5
80000	98.2	93.8	91.7	94
100000	98.3	94.2	91.8	94.5
120000	98.5	94.5	92	95

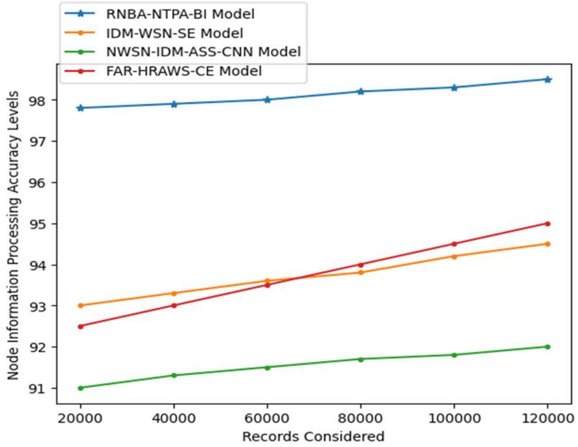

Figure 4: Node Information Processing Accuracy Levels

The node trust calculation is performed for all the information processed nodes. The trust factor if a node reflects the node properties. The trust factor of nodes is used to identify the normal and malicious properties of the nodes. The proposed model calculates the trust factor based on the node capabilities. The Node Trust Calculation Accuracy Levels of the proposed and existing models are depicted in Table 2 and Figure 5.

Table 2: Node Trust Calculation Accuracy Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	97.6	91.8	92.7	92.5
40000	97.8	92	93	92.8
60000	97.9	92.3	93.5	93.1
80000	98	92.5	94	93.4
100000	98.1	92.7	94.6	93.6
120000	98.2	93	95	94

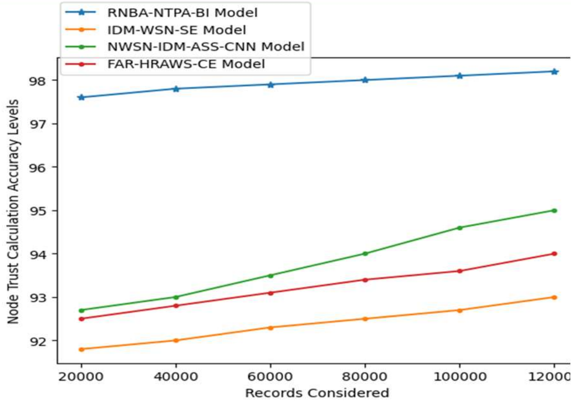

Figure 5: Node Trust Calculation Accuracy Levels

The node behaviour reflects the node nature and transmission capabilities. The node having malicious behaviour will degrade the network performance. The behaviour of each node is analyzed that is used to detect the false alarms in the network by identifying the normal and malicious nodes in the network. The Node Behaviour Analysis Time Levels of the existing and proposed models are shown in Table 3 and Figure 6.

Table 3: Node Behaviour Analysis Time Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	15.4	16	21.5	24.7
40000	16	17	21.7	25
60000	16.4	18	22	25.6
80000	17	19	22.2	26.4
100000	17.6	20	22.4	27.2
120000	18	21	22.6	28

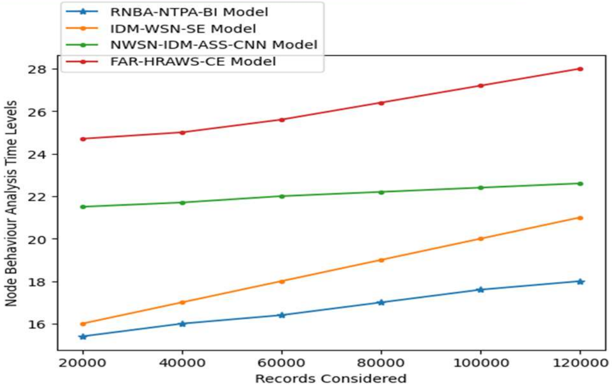

Figure 6: Node Behaviour Analysis Time Levels

The proposed model considers a behavioral index (BI) that is used to identify the node behavioral changes. The BI is unique value that is used to check the status of change in the BI value that indicates the change in the nodes behaviour. The Behavioral Index Updation Accuracy Levels of the proposed and existing models are shown in Table 4 and Figure 7.

Table 4: Behavioral Index Updation Accuracy Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	97.8	92.5	94.5	92
40000	98	92.8	94.7	92.3
60000	98.2	93	95	92.5
80000	98.4	93.4	95.2	92.6
100000	98.6	93.7	95.4	92.7
120000	98.7	94	95.5	93

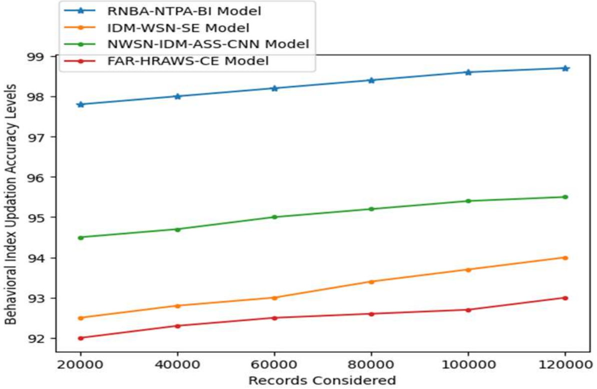

Figure 7: Behavioral Index Updation Accuracy Levels

For pattern analysis to be effective, the data must be classified into a set of known intrusion categories. Due to the fact that big data is the norm for data-heavy applications. Features like as center, spread, form, range, and class are frequently used to characterize patterns in data. The Transmission Pattern Analysis Time Levels of the proposed and existing models are shown in Table 5 and Figure 8.

Table 5: Transmission Pattern Analysis Time Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	14.4	19.7	21.5	22.5
40000	14.7	20	22	22.8
60000	15	20.2	22.5	23.3
80000	15.3	20.4	23	23.8
100000	15.6	20.7	23.5	24.4
120000	16	21	24	25

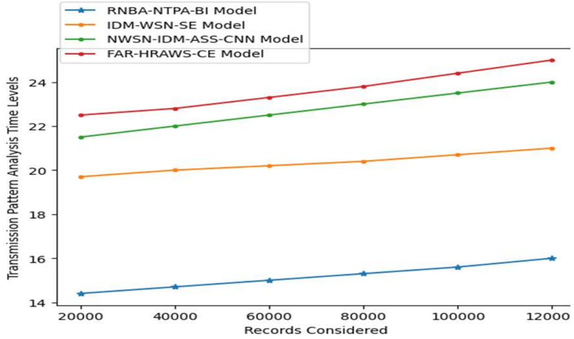

Figure 8: Transmission Pattern Analysis Time Levels

False alarms in the network degrade the network performance. The false alarms are caused by the malicious node sin the network that interrupts the network transmissions. The time complexity levels of the models also will be increase because of the false alarms in the network. The False Alarm Nodes Detection Accuracy Levels of the proposed and traditional models are shown in Table 6 and Figure 9.

Table 6: False Alarm Nodes Detection Accuracy Levels

Records Considered	Models Considered			
	RNBA-NTPA-BI Model	IDM-WSN-SE Model	NWSN-IDM-ASS-CNN Model	FAR-HRAWS-CE Model
20000	97.8	92.7	91	90
40000	98	93	91.4	91
60000	98.1	93.3	91.7	92
80000	98.3	93.4	92	93
100000	98.5	93.6	92.2	94
120000	98.6	94	92.4	95

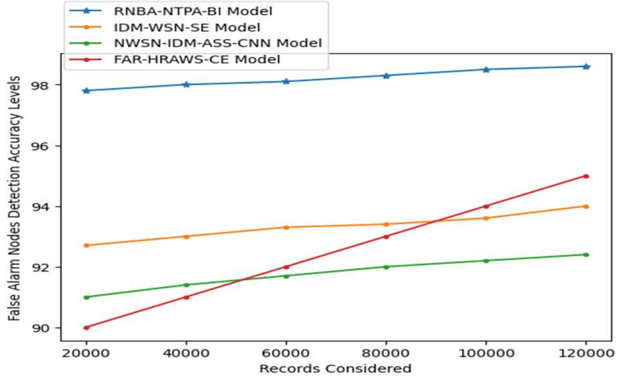

Figure 9: False Alarm Nodes Detection Accuracy Levels

5. CONCLUSION

Due to their specific nature, WSNs demand applications that are capable of efficient learning, adaptation, and inference. To address the challenge of intrusion detection in WSNs, this study proposes a node behavior analysis model for false alarm detection. IDS provide robust protection for the WSN. This study delves into the importance of security and the myriad of potential dangers that can develop in WSN communication settings. It gives a quick rundown of the several ongoing WSN projects that are trying to make use of the Internet of Things. Plans to identify trespassers in currently linked communication situations based on WSN have been formally categorized. Numerous correlations were observed between variables including discovery rate, false positive rate, and compatibility of best-in-class techniques. Although investigating ways to strengthen WSN security is crucial, researchers often struggle to devote enough time and energy to the endeavor. By identifying the optimal attributes via cross-correlation, the recommended model can function with reduced computational overhead. Different types of attacks can be efficiently categorized using the proposed approach. The proposed model's performance is enhanced when the node analysis based pattern analysis model is used instead of the conventional methods. This study proposes a Behavioral Index model based on Repeated Node Behaviour Analysis and Node Transmission Pattern Analysis to reduce network-wide false alarms. The proposed model achieved 98.4% accuracy in malicious pattern analysis and false alarm reduction. In future, the proposed model can be extended with feature dimensionality reduction models and optimization techniques can be applied on the IDS models for accurate false alarm detection and malicious nodes that can be removed from the network to increase the network lifetime.

REFERENCES:

[1] S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020, doi: 10.1109/ACCESS.2020.3024219.

[2] Z. Hu, L. Wang, L. Qi, Y. Li and W. Yang, "A Novel Wireless Network Intrusion Detection Method Based on Adaptive Synthetic Sampling and an Improved Convolutional Neural Network," in IEEE Access, vol. 8, pp. 195741-195751, 2020, doi: 10.1109/ACCESS.2020.3034015.

[3] K. T. Hjelmervik, H. Berg and T. S. Såstad, "Predicting False Alarm Rates for High-Resolution Antisubmarine Warfare Sonars in a Cluttering Environment Prone to False Alarm Rate Inflation," in IEEE Journal of Oceanic Engineering, vol. 45, no. 4, pp. 1527-1537, Oct. 2020, doi: 10.1109/JOE.2019.2936642.

[4] Q. Yu et al., "Intensive Care Unit False Alarm Identification Based on Convolution Neural Network," in IEEE Access, vol. 9, pp. 81841-81854, 2021, doi: 10.1109/ACCESS.2021.3086862.

[5] A.Sharma and S. Chauhan, "Sensor Fusion for Distributed Detection of Mobile Intruders in Surveillance Wireless Sensor Networks," in IEEE Sensors Journal, vol. 20, no. 24, pp. 15224-15231, 15 Dec.15, 2020, doi: 10.1109/JSEN.2020.3009828.

[6] X. Liu and S. W. Kim, "Harnessing Node Multiplicity for Detecting and Mitigating False Data in Wireless Relay Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3067-3078, 2020, doi: 10.1109/TIFS.2020.2980199.

[7] G. N. K. Reddy, M. S. Manikandan, N. V. L. N. Murty and L. R. Cenkeramaddi, "Unified Quality-Aware Compression and Pulse-Respiration Rates Estimation Framework for Reducing Energy Consumption and False Alarms of Wearable PPG Monitoring Devices," in IEEE Access, vol. 11, pp. 41708-41740, 2023, doi: 10.1109/ACCESS.2023.3269584.

[8] J. S. Ahn and T. H. Cho, "Modeling and Simulation of Abnormal Behavior Detection Through History Trajectory Monitoring in Wireless Sensor Networks," in IEEE Access, vol. 10, pp. 119232-119243, 2022, doi: 10.1109/ACCESS.2022.3202541.

[9] J. Ding, H. Wang and Y. Wu, "The Detection Scheme Against Selective Forwarding of Smart Malicious Nodes With Reinforcement Learning in Wireless Sensor Networks," in IEEE Sensors Journal, vol. 22, no. 13, pp. 13696-13706, 1 July1, 2022, doi: 10.1109/JSEN.2022.3176462.

[10] Kotiyal, V., Singh, A., Sharma, S., Nagar, J., & Lee, C.-C. (2021). Ecs-nl: An enhanced cuckoo search algorithm for node localisation in wireless sensor networks. Sensors, 21(11), 3576.

[11] Singh, A., Amutha, J., Nagar, J., Sharma, S., & Lee, C.-C. (2022). Lt-fs-id: Log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network. Sensors, 22(03), 1070.

[12] Singh, J., Chaturvedi, A., Sharma, S., & Singh, A. (2021). A novel model to eliminate the doubly nearfar problem in wireless powered communication network. IET Communications, 15, 1539–1547.

[13] Sharma, S., Kumar, R., Singh, A., & Singh, J. (2020). Wireless information and power transfer using single and multiple path relays. International Journal of Communication Systems, 33(14), e4464.

[14] Amutha, J., Sharma, S., & Nagar, J. (2020). WSN strategies based on sensors, deployment, sensing models, coverage and energy efciency: Review, approaches and

open issues. Wireless Personal Communications, 111(2), 1089–1115.

[15] Amutha, J., Nagar, J., & Sharma, S. (2021). A distributed border surveillance (DBS) system for rectangular and circular region of interest with wireless sensor networks in shadowed environments. Wireless Personal Communications, 117(3), 2135–2155.

[16] Sharma, S., & Nagar, J. (2020). Intrusion detection in mobile sensor networks: A case study for diferent intrusion paths. Wireless Personal Communications, 115, 2569–2589.

[17] Amutha, J., Sharma, S., & Sharma, S. K. (2021). Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research fndings, challenges and future directions. Computer Science Review, 40, 100376.

[18] Singh, A., Kotiyal, V., Sharma, S., Nagar, J., & Lee, C.-C. (2020). A machine learning approach to predict the average localization error with applications to wireless sensor networks. IEEE Access, 8, 208253–208263.

[19] Khan, T., Singh, K., Hasan, M. H., Ahmad, K., Reddy, G. T., Mohan, S., & Ahmadian, A. (2021). Eters: A comprehensive energy aware trust-based efcient routing scheme for adversarial WSNs. Future Generation Computer Systems, 125, 921–943.

[20] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for efective communication in wireless sensor networks. Wireless Personal Communications, 105(4), 1475–1490.

[21] Singh, A., Nagar, J., Sharma, S., &Kotiyal, V. (2021). A gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks. Expert Systems With Applications, 172, 114603.

[22] Vallathan, G., John, A., Thirumalai, C., Mohan, S., Srivastava, G., & Lin, J.C.-W. (2021). Suspicious activity detection using deep learning in secure assisted living IoT environments. The Journal of Supercomputing, 77(4), 3242–3260.

[23] Yadav, A. K., Singh, K., Ahmadian, A., Mohan, S., Shah, S. B. H., &Alnumay, W. S. (2021). Emmm: Energy-efcient mobility management model for context-aware transactions over mobile communication. Sustainable Computing: Informatics and Systems, 30, 100499.

[24] S. Lalar, S. Bhushan, and N. A. Surender, “Clone detection using fuzzy logic in static wireless sensor network,” International Journal of Vehicle Information and Communication Systems, vol. 5, no. 3, pp. 334–353, 2020.

[25] M. Numan, F. Subhan, W. Z. Khan et al., “A systematic review on clone node detection in static wireless sensor networks,” IEEE Access, vol. 8, pp. 65450–65461, 2020.

[26] M. Jamshidi, S. S. Poor, N. N. Qader, M. Esnaashari, and M. R. Meybodi, “A lightweight algorithm against replica node attack in mobile wireless sensor networks using learning agents,” IEIE Transactions on Smart Processing & Computing, vol. 8, no. 1, pp. 58–70, 2019.

[27] M. Jamshidi, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, “Using time-location tags and watchdog nodes to defend against node replication attack in mobile wireless sensor networks,” International Journal of Wireless Information Networks, vol. 27, no. 1, pp. 102–115, 2020.

[28] S. Anitha, P. Jayanthi, and V. Chandrasekaran, “An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks,” Measurement, vol. 167, p. 108272, 2021.

[29] L. Sujihelen and C. Jayakumar, “Inclusive elliptical curve cryptography (IECC) for wireless sensor network efficient operations,” Wireless Personal Communications, vol. 99, no. 2, pp. 893–914, 2018.

[30] L. Sujihelen and C. Senthilsingh, “Detect the replica node in mobile wireless sensor networks,” in 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021.