International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7417
***Article Received**: 01 May 2023 **Revised:** 30 June 2023 **Accepted:** 28 July 2023*

Improving Data Transmission Rate with Self Healing Activation Model for Intrusion Detection with Enhanced Quality of Service

Simhadri Madhuri[1], S. Venkata Lakshmi[2]
[1] Research Scholar, Department of Computer Science
GITAM (Deemed to be University)
Visakhapatnam, India
madhurisimhadri09@gmail.com
[2]Assistant Professor, Department of Computer Science
GITAM (Deemed to be University)
Visakhapatnam, India
svlakshmi2014@gmail.com

Abstract— Several types of attacks can easily compromise a Wireless Sensor Network (WSN). Although not all intrusions can be predicted, they may cause significant damage to the network and its nodes before being discovered. Due to its explosive growth and the infinite scope in terms of applications and processing brought about by 5G, WSN is becoming more and more deeply embedded in daily life. Security breaches, downed services, faulty hardware, and buggy software can all cripple these enormous systems. As a result, the platform becomes unmaintainable when there are a million or more interconnected devices. When it comes to network security, intrusion detection technology plays a crucial role, with its primary function being to constantly monitor the health of a network and, if any aberrant behavior is detected, to issue a timely warning to network administrators. The current network's availability and dependability are directly tied to the efficacy and timeliness of the Intrusion Detection System (IDS). An Intrusion-Tolerant system would incorporate self-healing mechanisms to restore compromised data. System attributes such as readiness for accurate service, supply identical and correct data, confidentiality, and availability are necessary for a system to merit trust. In this research, self-healing methods are considered that can detect intrusions and can remove with intellectual strategies that can make a system fully autonomous and fix any problems it encounters. In this study, a new architecture for an Intrusion Tolerant Self Healing Activation Model for Improved Data Transmission Rate (ITSHAM-IDTR) is proposed for accurate detection of intrusions and self repairing the network for better performance, which boosts the server's performance quality and enables it to mend itself without any intervention from the administrator. When compared to the existing paradigm, the proposed model performs in both self-healing and increased data transmission rates..

Keywords - Wireless Sensor Networks, Intrusion Detection, Intrusion Tolerant, Self Healing Activation Model, Network Security, Attacks, Data Transmission Levels, Quality of Service.

I. INTRODUCTION

There have been many different types of cyber-attacks and basic computer security issues during the past fifteen years [1]. Organizations are increasingly susceptible to possible security threats, such as invasions, at all levels of Information Communication Technology (ICT), as communication develops and information management systems become more sophisticated and widespread. Firewalls, IDS, Intrusion Prevention Systems (IPS) [2], authentication, encryption, and additional software and hardware solutions are urgently needed to offer a safe and secure information security system [3]. Despite the fact that numerous IDS/IPS systems have been developed, each has its own set of limitations. Some of these limitations include inefficient detection, ineffective preventative strategies, and excessive false alarm rates. In order to detect and prevent assaults on ICT resources [4], IDSs and IPSs have become indispensable security tools, making it crucial to improve upon older designs, methodologies, and procedures. For the detection process to be efficient against unknown threats, anomaly detection must be improved through the use of cutting-edge methods [5]. In this study, a novel self healing activation model is proposed for effective detection of intrusions and enhancing the security levels of the network [6].

Traditional methods of intrusion protection involve looking for the virus's signature in certain locations. While it is undeniable that the traditional method should be utilized to protect against known dangers [7], it does not offer security against zero-day vulnerabilities, which are new assaults that have not been discovered and do not yet have a deployed security patch [8]. The attack cannot be positively identified since anti-virus programs do not yet recognize their signature. Because of their inability to learn and change on their own, such systems need constant external updates to their signature databases [9]. Whether or not a system can intelligently detect new, previously undiscovered hazards and respond to them in such a way that minimizes damage and, ideally, eliminates the threat [10] is one of the major unresolved questions in cyber security. As a result, many forms of artificial intelligence are used for this, with intrusion detection being particularly popular. However, it is crucial that the detection algorithms minimize both false negatives and false positives [11]. The system is vulnerable to further harm at the hands of the attacker if an existing attack is not recognized. However, if a legal behavior is mistakenly identified as an attack, the network will attempt to halt the legitimate behavior, which can result in as much financial and operational harm as a genuine attack that goes undetected [12].

As a relatively new form of network security, intrusion tolerance combines cryptography with fault-tolerant technology to allow it to function normally even if some of its components have been compromised [13]. The present information security defense in depth is the last line of defense in protecting the privacy, authenticity, and accessibility of sensitive system data while keeping service delivery going strong across multiple nations [14]. However, the requirements for intrusion tolerance measures can be destroyed if the breach is persistent and successful. Furthermore, if the attack or intrusion is not identified and prevented, then a concealed intrusion has taken place [15]. Unpredictable risks emerge as the system degenerates [16]. Long-running processes also suffer from software ageing in the application server, which leads to decreased performance and an increase in errors. All three scenarios result in a rapid degeneration of the application server's capacity to provide normal services, if not an outright crash [17]. An intrusion is any malfunction in normal operations that was intentionally caused by an outside source. As part of creating an intrusion-tolerant, single-purpose server [18], it is recommended to set up a self-healing functional framework, including detection and implementation components. IDS (Intrusion Detection System) Model is depicted in Figure 1.

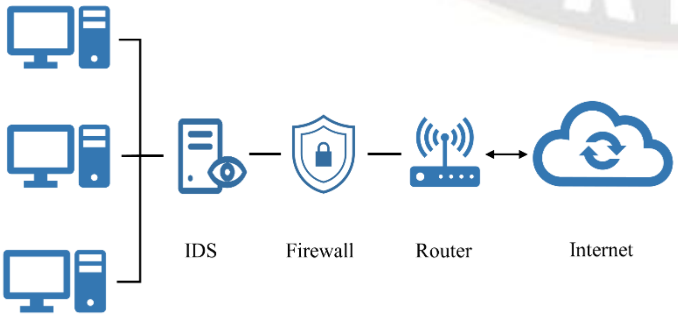

Figure 1. Model of IDS

Because they react to any new, unexpected data or activity, whether malicious or not, non-self based intrusion detection techniques have a high false positive rate [19]. Such an approach yields excellent results in some contexts, such as banking system fraud detection, where it is reasonable to assume that self detectors cover all forms of normal behavior and any anomaly is a fraud [20]. In network systems, as in many others, however, legitimate behavior is likely to shift over time or to experience occasional abnormal events that do not indicate an attack. Whenever valid behavior modifies [21], a large number of false positives are generated by non-self negative selection for such detection of intrusions [22]. Therefore, only those systems should employ negative selection on its own.

Type, intrusion, and danger values are only few of the metrics that can be calculated from an event's analysis. Remember that IDSs vary in how they define anomalous behavior [23]. The inferences drawn when scanning for dangerous occurrences are sensitive to the estimated deviation score, which might vary substantially depending on the technique employed. The supplemented information is recorded alongside the event itself and stored in a database for later use. A continuously updated timeline is kept, with new events added as soon as they have been evaluated. The actual unique events themselves are not necessary for event sequence matching, but rather a kind or properties of events [24]. Timeline analysis and the extraction and classification of event sequences are similar to event classification. The classification system is dynamic; as additional events are added, their profiles may shift and need a reclassification. This can be done in a batch operation that runs at set intervals or in real time.

The self healing model is similar to the security model that put in place to protect a computer network. Network security systems need to be protected in the same way that the human immune system protects the body from outside, previously unseen pathogens. Independent [25], widely distributed, robust, dynamic, self-monitoring, adaptive, and self-healing [26] information processing systems are what we mean when we talk about self-healing models. Automatic and ongoing software monitoring, assessment, repair, and restoration are the most common features of a self-healing system [27]. Self-healing qualities applied to network systems may offer a means to modify fault-finding in networks that have been subjected to multiple attacks [28]. Methods that promote self-healing are complementary to those that prevent attacks from being successful. In this study, a new architecture for an Intrusion Tolerant Self Healing Activation Model for Improved Data Transmission Rate is proposed for accurate detection of intrusions and self repairing the network for better performance, which boosts the server's performance quality and enables it to mend itself without any intervention from the administrator.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7417
***Article Received**: 01 May 2023 **Revised:** 30 June 2023 **Accepted:** 28 July 2023*

II. LITERATURE SURVEY

The intensification of wirelessly connected gadgets has both positive and negative results. It makes people's lives easier, but on the other, the openness of the wireless medium makes the system susceptible to attack. Using cutting-edge anomaly detection methods, an IDS may monitor network traffic for signs of intrusion. In order to tell good traffic from bad, researchers have turned to deep learning algorithms. Utilizing deep learning for IDS purposes, however, has been hampered by the difficulty of mapping tabular data onto images prior to the image classification. Aminanto et al. [2] presented a new method for IDS that involves translating tabular data into a 2-coded color scheme. In order to achieve preferable dimensionality, the suggested approach uses a feature selection technique. To determine how the traits are related, the author analyzed groups of attributes of varying sizes. It also employs the Convolutional Neural Network (CNN) model for Wi-Fi attack classification.

An attack on a WSN aims to cripple or completely eliminate the network's capacity to carry out the tasks for which it was designed. Wireless sensor networks employ intrusion detection as a defense against unanticipated attacks. Host and network security are crucial in this age of rapid technological advancement and ubiquitous Internet use. The goal of developing hacking technology is to break into computer systems. Machine learning (ML) algorithms [30] were used as part of IDS to identify malicious activities on the network. Traditional ML methods, such as support vector machine (SVM), K-nearest neighbor (KNN), and filter-based feature selection, were notoriously inaccurate and prone to misclassifying intrusions. The Boruta choice of features with grid search random forest (BFS-GSRF) algorithm is used in the new IDS framework provided by Subbiah et al. [3]. A number of ML techniques, including linear discriminant analysis (LDA) [32], classification and regression tree (CART), and others, are utilized to assess BFS-GSRF's efficacy.

The popularity of wireless media and gadgets continues to rise alongside the development of new technologies. In example, WLAN deployment has skyrocketed in recent years and is only anticipated to grow in the future. The network is susceptible to attacks that vary from passive listening to active involvement due to the present state of wireless local area network technologies. To counteract these threats, researchers are working on IDSs. When it comes to protecting a wireless local area network (WLAN), IDSs are crucial. Most IDS techniques, however, are incapable of handling sophisticated and ever-changing threats. The purpose of this study is to enhance current WLAN IDSs by developing a system that is better able to dynamically detect attacks of varying complexity. A strategy has been presented by Ozkan-Okay et al. [4] for this situation. There are two main contributions to the suggested technique. The Feature Selection Approach (FSAP) is the first major improvement, since it allows for faster attack detection by cutting down on the number of characteristics. The second contribution is an efficient and effective method for detecting hybrid attacks [23]; we call it SABADT (Signature and Anomaly Based Attack Detection Technique). The proposed methodology is evaluated using the KDD'99 and UNSW-NB15 datasets. The outcomes are evaluated against the outcomes of conventional machine learning techniques. The detection model is first trained with data from KDD'99 and UNSW-NB15, and then tested with the same two datasets.

Because of the proliferation of Wi-Fi-enabled devices, human intrusion detection based on Wi-Fi has attracted a lot of research and development over the past few years. Currently, available systems passively identify human infiltration by monitoring for temporal signal changes generated by human motion. It is challenging, however, to pinpoint the precise entry point of an attack. Taking into account the effect of intrusion direction on the energy and geographical distributions of statistics of multiple reflections, Wang et al. [5] introduced WIDD, a Wi-Fi-based passive human activity direction detection system. Isolating the amplitude and AoA distributions of the multipath signal is the first step in WIDD, followed by a normality test with the Jarque-Bera (JB) statistic. A novel joint hypothesis testing algorithm [31] was designed to monitor changes in reflections' amplitude and angle-of-arrival (AoA) distributions to detect human intrusion. Finally, the divergence evaluation is used to determine which reflection is more impacted by human intrusion, and the related AoA is extracted to identify the intrusion's direction.

With the proliferation of WSNs and their uses, the number of malicious intrusions [33]and security risks that threaten their normal operations has also expanded considerably. Deep learning (DL) based methods for network intrusion detection (NID) have been the subject of substantial research and development. However, the high computational complexity of DL presents a major hurdle to the actual implementation of the DL-based model, particularly on the devices of WSNs, which have limited processing performance due to their dependence on battery power. In this paper, Zhao et al. [6] suggested using an LDAN for NID since its lightweight construction allows for effective feature extraction.

When it comes to collecting and sending data, WSNs face a unique set of security concerns and threats. DoS attacks are widespread in WSNs and can affect any part of the protocol stack. Dener et al. [7] presented a new Denial-of-Service Intrusion Detection System (DDS) to detect these kinds of attacks on WSNs. The proposed system, dubbed STLGBM-DDS, is an ensemble IDS that uses the LightGBM machine learning algorithm, data balancing, and feature selection techniques to detect intrusions on the Apache Spark big data platform in a Google Colab environment. To reduce the detrimental effects of data inconsistency on system performance, we employed data imbalance processing in the form of the Synthetic Minority Oversampling Technique (SMOTE) and the Tomek-Links sampling methods, jointly referred to as STL. Information Gain Ratio was also employed to pick features during the preprocessing of the data. We looked at how the data-balancing and feature-selection processes affected the system's detection performance.

The rapid development of IoT makes it challenging for cloud-based computing to keep up with the need for low latency and user-friendliness. Edge computing is a decentralized system that combines various aspects of IT, including hardware, software, networking, and storage. On the periphery of an IoT, it offers smart services. Since the edge network is a combination of wireless and wired connections, nodes at the edge have limited access to computing and storage resources. Because of these factors, cyber criminals can easily target the edge network. Detection and data collection on a massive scale within an IoT network is also challenging for an edge node. However, deploying big data-enabled intrusion detection algorithms on resource-constrained edge nodes in IoT is crucial for assuring the high accuracy of IDS [34]. Fuzzy rough sets, Generative Adversarial Networks (GANs), and Convolutional Neural Networks (CNNs) are proposed by Wu et al. [8] as a massive data mining solution to the aforementioned problems in intrusion detection. First, the author presented an approach based on fuzzy rough sets to carry out feature selection for big data using the Internet of Things. The author then utilized CNN's powerful feature extraction tools to build a system that can detect intrusions based on carefully chosen features. The author also presented an innovative approach that combines CNN and GAN to perform intrusion detection in a variety of settings.

The Controller Area Network (CAN) is still widely used despite the fact that it has no built-in security or authentication and has been around for quite some time. Because they are always connected to the internet via Bluetooth, Wi-Fi, and cellular radio, modern automobiles are open targets for cyber attacks. As a result, improving vehicle security through the detection and prevention of cyber attacks is an important necessity. A novel unsupervised intrusion detection and prevention system for automotive CANs was presented in this study by Freitas et al. [9]. This system has the potential to detect and prevent attacks without the need to access information typically only available to car manufacturers or modify the architecture of the ECUs themselves. The author examined how well two machine learning methods performed with minimal data to detect fuzzy and spoofing attacks. Detection can begin, and assaulting frames can be identified sooner if fewer data bytes are needed.

III. PROPOSED MODEL

As the internet and other forms of electronic communication have developed rapidly, so too has the volume of associated data. Traditional network defenses are struggling to keep up with the ever-evolving threat landscape and detect malicious behavior in real time as novel methods of attack emerge. The prospect of malicious actors breaching the system is likewise impossible to rule out. To safeguard the confidentiality, integrity, and availability of the network, intrusion detection systems (IDS) are one such instrument. Although significant progress has been made, IDS still has potential for improvement in its ability to identify novel intrusions while simultaneously increasing detection accuracy.

The predicted intrusion score when looking for damaging occurrences varies substantially based on the conventional methodologies utilized. After the event is enhanced with the data, it is recorded in a database for future use as a historical resource. In real time, events are tracked and added to a timeline as they are assessed. The timeline's primary purpose is to offer context for events, so it's best if it doesn't include specific details about individual occurrences but rather general categories or characteristics. Timeline analysis, like event categorization, is a method for identifying and classifying clusters of related events. When new events are introduced to the system, the event profiles may change, necessitating a reclassification. This can also be done in a batch job that runs at set intervals rather than in real time. A warning signal alerts the system that an unsafe event has occurred that may cause or has already resulted in damage. The self healing model then triggers the model to remove the nodes causing intrusions in the network increasing the security levels.

Network packet loss, aberrant packets, use of unusual ports, abnormal memory or CPU utilization, abnormal activity, and suspicious user behaviour are all examples of potential intrusion signs. These signs and symptoms might range in intensity, and it is possible to draw connections between them and events in the past. When such an incident is detected, the network quickly switches into the self healing processing mode. It is possible for a threat threshold to be breached if a series of events, each of which would be considered admissible individually but would pose a bigger hazard when combined. Once an intrusion alert is received, the network assumes an attack is underway and works to pinpoint its source and halt its progress. When a malicious trace is detected, the system's defenses may prevent the machine from making network connections or executing certain system calls that could cause additional damage. Proposed model framework was shown in Figure 2.

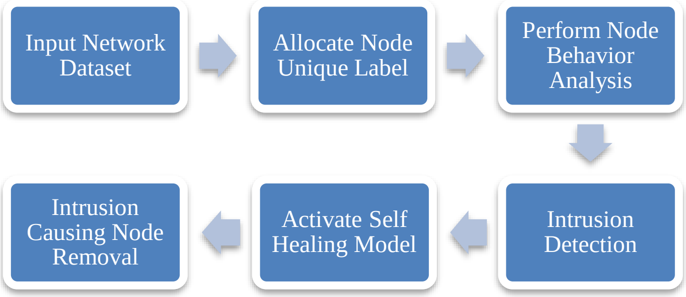
Input Network Dataset
Allocate Node Unique Label
Perform Node Behavior Analysis
Intrusion Detection
Activate Self Healing Model
Intrusion Causing Node Removal

Figure 2: Proposed Model Framework

To avoid overreacting to partial sequence matches on other machines, the safest course of action is to allow the execution of all other commands while raising a warning about the potential harm. When an attack has been identified and the responsible chain of events is determined, the details are shared with all other nodes in the network. Because an attack can be in its early beginnings, they look into their own timelines to see whether they have encountered something similar or if they have experienced a certain prefix of the chain of events. For partial sequence corresponding of sequences arriving from other nodes, the minimal response can be to prevent executing only the actions that will additionally match the dangerous sequence, while allowing execution of all other commands and notifying administrators of a possible threat. When the chronology is updated, it may also find a match with a potentially harmful sequence in a database. A defensive reaction is initiated when a potentially dangerous sequence of events corresponds with the chronology. The self healing model will be triggered if any unusual activity occurs in the network. The self healing model identifies the malicious nodes and removes such nodes to increase the network security levels. In this study, a new architecture for an Intrusion Tolerant Self Healing Activation Model for Improved Data Transmission Rate is proposed for accurate detection of intrusions and self repairing the network for better performance, which boosts the server's performance quality and enables it to mend itself without any intervention from the administrator.

Algorithm ITSHAM-IDTR

{

Input: Network Nodes Dataset {NNset}
Output: Malicious Nodes List {MLset}

Step-1: The nodes that need to involve in data transmission has to update the information to the monitoring authority, as the communication can be performed with the node information. The nodes in the network will be allocated with the unique label that will be used for node communication. The process of unique id generation and allocation is performed as

$$NUID[Max] = \sum_{n=1}^{Max(n)} getaddr(NNset(n)) + nodeparam(NNset(n)) + EntryTime(NNset(n))$$

Here getaddr() is used to know the node address and nodeparam() model is used for maintaining node parameters as routing type, area, channel model and the time instant of each node is also considered.

Step-2: Each node in the network exhibits its unique behavior with other nodes in the network. The nodes behavior is continuously monitored for improving the network performance. The node behavior with other nodes represents the normal or malicious nature of the nodes. The node behavior analysis is performed as

$$NBanal[Max] = \sum_{n=1}^{Max(n)} getNUID(n) + \frac{maxPDR(n)}{\delta} + minener(n) + loss(n)$$

Here δ is the total packets generated in the network and maxPDR() is the model that considers maximum packets delivered to the next intermediate node. The data loss rate is considered using loss() model.

Step-3: The node behavior is continuously monitored and the intrusions in the network are identified based on the nodes behavior. The intrusion is an unusual action in the network that is caused to degrade the network performance. The nodes causing intrusions in the network are detected as

$$INode[Max] = \sum_{n=1}^{Max} \max(NBanal(n)) + \lim_{n \to Max} \left(NUID(n) + \frac{maxNodeLimit(Max)}{\tau}\right)^2 + NUID(maxPDR(n) - minPDR(n)) \begin{cases} 1\ if\ PDR < pTh\ and\ ener < eTh \\ 0 \qquad\qquad otherwise \end{cases}$$

Here τ is the entire network maximum node limit that the nodes causing intrusions in the network can be detected. The nodes are labeled as 1, if the nodes are causing intrusions and 0, if normal in behavior. Here pTh is the threshold value of packets transmitted, eTh is the threshold value of the energy consumption.

Step-4: The proposed model considers self healing model that gets automatically triggered if an intrusion is detected in the network. The nodes that are causing intrusions in the network can be monitored. The self healing model is used to accurately detect the nodes causing intrusions and the self healing triggering is performed as

$$SHModel[Max] = \prod_{n=1}^{Max(n)} \frac{getNUID(INode(n))}{\tau} + \sum_{n=1}^{Max(n)} NUID(Node(minPDR(n)) + NUID(Node(minener(n)) \begin{cases} SHModel\ Trigger\ if\ PDR < pTh\ and\ ener < eTh\ and\ NUID == INode \\ continue \quad otherwise \end{cases}$$

Step-5: The self healing model will detect the intrusions in the network and such intrusion causing nodes will be removed from the network. The node removal from the network is performed to increase the quality of service levels and the process is performed as

$$MLset(SHModel[Max]) = \prod_{n=1}^{Max(n)} getNUID(SHModel(n)) - NUID(Node(n)) + INode(n) \leftarrow update(NUID(n) + PDR(n) + ener(n))$$

}

IV. RESULTS

To detect intrusions, which are either actual violations or immediate risks of violation of computer security regulations and standard security practices, it is necessary to keep monitoring the network and look for telltale indications. Numerous factors can contribute to an incident, including but not limited to: intrusions, attackers gaining access to systems over the Internet, and authorized users of systems misusing their privileges or seeking to gain more privileges for which they are not authorized. Intrusion detection is the process of constantly watching and analyzing a network for any signs of an attack. Prevention of an incursion is feasible with the use of intrusion detection technology and the prompt ending of known attacks or the attempted termination of detected possible occurrences through quarantining or isolation.

The proposed intrusion detection system is an innovative function that goes beyond what can be achieved with simple, conventional approaches. It is the cutting edge of security technology, protecting everything from the kernel to the data flows in a network to the information stored in a network. In this study, a new architecture for an Intrusion Tolerant Self Healing Activation Model for Improved Data Transmission Rate (ITSHAM-IDTR) is proposed for accurate detection of intrusions and self repairing the network for better performance, which boosts the server's performance quality and enables it to mend itself without any intervention from the administrator. Multi-Class Intrusion Detection with Two-Channel Color Mapping (MCID-TCCM) in IEEE 802.11 Wireless Network; Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm (GSRF-BFSA); and the conventional Intrusion Detection Method based on Self-Generated Coding (IDS-SGC) technology for stealthy false data injection attacks in train-ground communication systems are contrasted with the proposed model. The outcomes show that the proposed approach performs better than existing models in self-healing and intrusion detection.

The proposed model allocates a unique label to each node in the network. The node label helps each node to communicate and also it is easy for monitoring the nodes using the allocated label. Accuracy levels of the proposed and existing models for node label allocation are displayed in Table 1 and Figure 3, respectively.

TABLE I. NODE LABEL ALLOCATION ACCURACY LEVELS

Nodes in the Network	**Models Considered**			
	ITSHAM-IDTR Method (%)	*IDS-SGC Method (%)*	*MCID-TCCM Method (%)*	*GSRF-BFSA Method (%)*
20	94.8	89.8	85.3	87.6
40	95.1	90.3	85.5	88.1
60	95.4	90.6	86	88.4
80	95.7	91	86.4	89.1
100	95.8	91.4	86.7	89.3
150	97.1	92.3	87.7	90.1
200	97.4	92.7	88.1	90.8
250	97.5	93.1	88.4	91
300	98	93.4	88.7	91.6

Article Received*: 01 May 2023* ***Revised:*** *30 June 2023* ***Accepted:*** *28 July 2023*

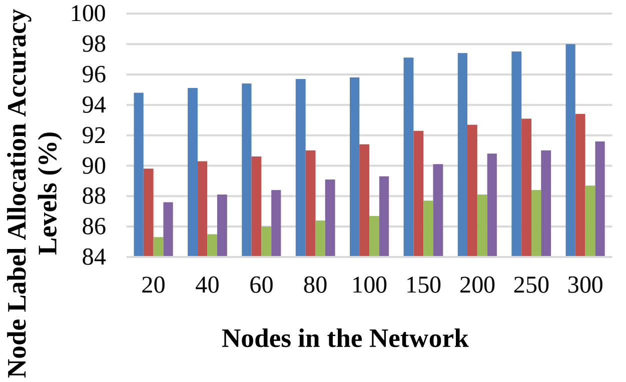

Figure 3: Node Label Allocation Accuracy Levels

The nodes in the network are more vulnerable to attacks. The node behavior is continuously monitored for analyzing the normal or malicious behavior in the network. Analysis of Node Behavior Table 2 and Figure 4 display the various time scales of existing and proposed models, respectively.

TABLE II. NODE BEHAVIOR ANALYSIS TIME LEVELS

Nodes in the Network	Models Considered			
	ITSHAM-IDTR Method (ms)	*IDS-SGC Method (ms)*	*MCID-TCCM Method (ms)*	*GSRF-BFSA Method (ms)*
20	6.1	18.7	25.7	22.7
40	6.7	19	26.1	22.9
60	6.9	19.4	26.7	23.3
80	7	19.5	26.9	23.7
100	7.1	19.7	27	23.8
150	7.2	19.8	27.2	24
200	7.3	20	27.3	24.1
250	7.7	20.4	27.5	24.3
300	8	21	28	24.8

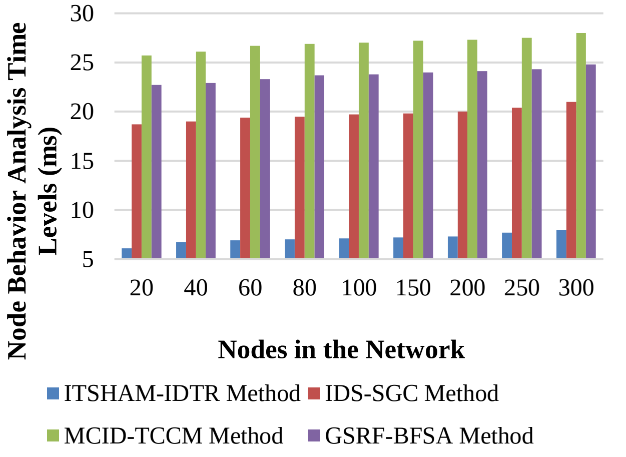

Figure 4: Node Behavior Analysis Time Levels

An intrusion detection system is responsible for keeping tabs on a network or infrastructure to identify any suspicious behavior or policy violations. Typically, SIEM systems will gather reports of intrusion activity and violations and either deliver them to an administrator or store them in a centralized location. Alarm filtering techniques are used by a SIEM system to separate legitimate concerns from fake ones. The intrusion that is caused by malicious nodes are detected accurately in the proposed model. Table 3 and Figure 5 display the existing and proposed models' Intrusion Detection Time Levels.

TABLE III. TIME INTERVALS FOR INTRUSION DETECTION

Nodes in the Network	Models Considered			
	ITSHAM-IDTR Method (ms)	*IDS-SGC Method (ms)*	*MCID-TCCM Method (ms)*	*GSRF-BFSA Method (ms)*
20	8.4	20.9	24.1	17
40	8.8	21.4	24.4	17.5
60	9.1	21.9	24.7	18
80	9.5	22.4	25	18.5
100	9.6	22.5	25.2	18.6
150	9.8	22.9	25.3	18.8
200	10.1	23	25.6	19.1
250	10.3	23.5	25.8	19.2
300	11	24	26	19.4

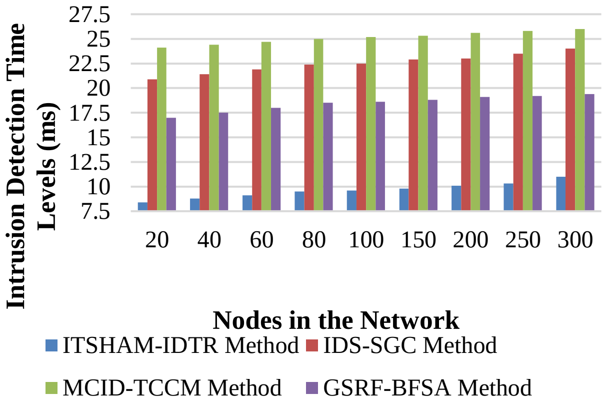

Figure 5: Intrusion Detection Time Levels

When malicious or suspicious actions are discovered, IDS will issue a warning. An analyst in a security operations center (SOC) or an incident responder can analyze a threat based on these signals and take corrective measures as needed. The proposed model considers a self healing model that automatically triggers if there is a intrusion alarm in the network. Intrusion detection systems sift through data in search of intrusions of previously identified attacks. The protocol and application layers are alerted and investigated for these outliers. Table 4 and Figure 6 depict the relative accuracy of the proposed and existing models for intrusion detection.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7417
***Article Received**: 01 May 2023 **Revised:** 30 June 2023 **Accepted:** 28 July 2023*

TABLE IV. ACCURACY OF INTRUSION DETECTION

Nodes in the Network	**Models Considered**			
	ITSHAM-IDTR Method (%)	*IDS-SGC Method (%)*	*MCID-TCCM Method (%)*	*GSRF-BFSA Method (%)*
20	94.5	90.3	91.5	83.5
40	94.8	90.7	92.3	84
60	95.1	91.1	93	84.5
80	95.4	91.4	93.4	84.7
100	95.7	91.7	93.6	84.8
150	96.8	92.8	94.7	86.2
200	97.1	93.1	95.1	86.4
250	97.4	93.4	95.3	86.5
300	97.6	94	96	87

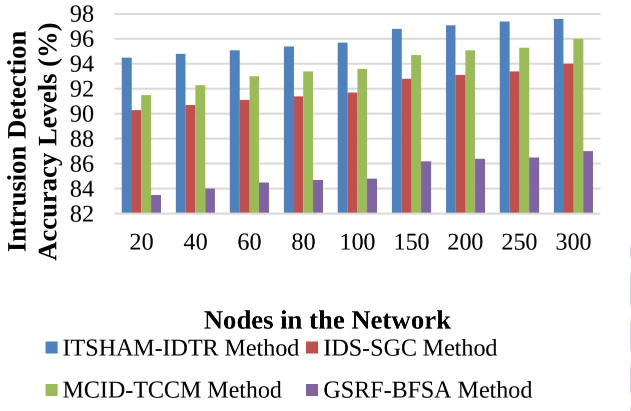

Figure 6: Intrusion Detection Accuracy Levels

The proposed model considers self healing model that automatically activates if a node causing intrusion in the network is detected. The proposed model identifies the nodes behavior frequently and immediately triggers the self healing model that removes the nodes causing the intrusions. The Self Healing Model Accuracy Levels comparison is shown in Table 5 and Figure 7.

TABLE V. SELF HEALING MODEL ACCURACY LEVELS

Nodes in the Network	**Models Considered**			
	ITSHAM-IDTR Method (%)	*IDS-SGC Method (%)*	*MCID-TCCM Method (%)*	*GSRF-BFSA Method (%)*
20	96.1	88.4	90.3	88.7
40	96.4	89	90.7	89.1
60	96.8	90.2	91.1	89.3
80	97.1	90.5	91.4	89.5
100	97.2	90.8	91.6	89.7
150	97.7	91.1	92	90.2
200	98	91.4	92.3	90.4
250	98.1	91.7	92.5	90.6
300	98.3	92	93	91

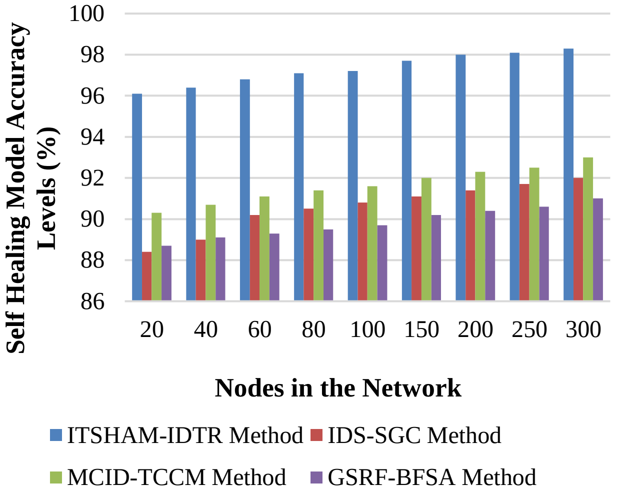

Figure 7: Self Healing Model Accuracy Levels

The proposed model with frequent network nodes monitoring, identifies the malicious actions in the network during data transmission. In order to improve the network's overall quality of service, harmful nodes will be eliminated. Table 6 and Figure 8 illustrate the contrast between the various degrees of network security.

TABLE VI. NETWORK SECURITY LEVELS

Nodes in the Network	**Models Considered**			
	ITSHAM-IDTR Method (%)	*IDS-SGC Method (%)*	*MCID-TCCM Method (%)*	*GSRF-BFSA Method (%)*
20	95.5	89.8	87.8	89
40	95.8	90	88.2	89.3
60	96.1	90.4	88.8	89.7
80	96.2	90.6	89.1	89.9
100	96.4	90.8	89.2	90.1
150	97.3	91.6	90	90.9
200	97.4	91.8	90.3	91.1
250	97.6	92	90.4	91.3
300	98.4	92.2	90.6	91.6

***DOI:** https://doi.org/10.17762/ijritcc.v11i9s.7417*
***Article Received**: 01 May 2023 **Revised:** 30 June 2023 **Accepted:** 28 July 2023*

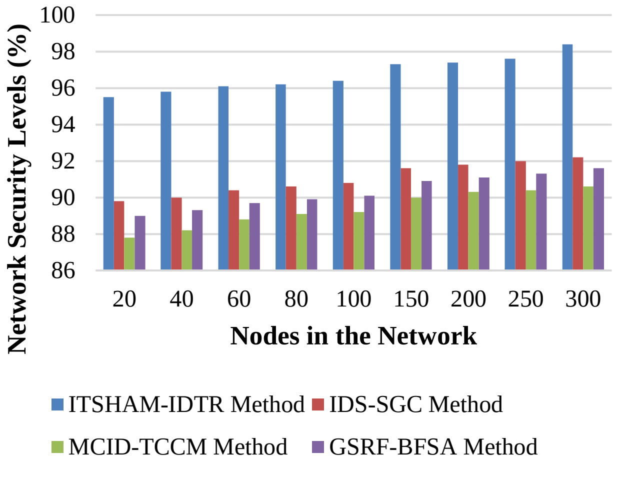

Figure 8: Network Security Levels

V. CONCLUSION

In this research, the idea of a self-healing model is proposed to accurately detect the intrusions and remove the nodes causing intrusions in the network. The proposed method allows for the differentiation of legitimate and harmful behavior, allowing for a more targeted response than is possible with pure intrusion detection approaches, which react to any new behavior in the system. In highly dynamic systems, where novel behaviors occur continuously, this allows for a significant reduction in false positive alarms. When potentially harmful events are broadcasted across the network, defensive measures can spread rapidly to other servers, thwarting an attack before it has a chance to do any real damage. Self-healing servers are becoming increasingly popular, and with that comes increased demands for both survivability and reliability from the services they support. However, it can be difficult to prevent all attacks with security technology, so this research focuses on designing and implementing an intrusion-tolerant, self-healing application server that can handle the unknown state of intrusion and recover from it regularly. In this research, an approach for intrusion tolerance is proposed that makes use of the separation of concerns inherent in modern computer architecture. The framework will be tested in a simulated intrusion-tolerant environment, complete with the necessary security controls and procedures, including a recovery module that can restore corrupted data. Data corruption caused by server invasions can be identified and restored by using this approach. When the server is idle or in a redundant state, both of which keep it busy at all times, it performs this detection and recovery process at regular intervals, even if there is no pending request for it to execute. The framework's performance research reveals that incorporating intrusion detection and self healing module helps in accurate detection of intrusions and increasing the network performance. The proposed model achieves 98.4% accuracy in intrusion detection and self healing. In future, optimization models can be used along with the regular models for calculating best fitness value for intrusion detection in the network and feature dimensionality can be applied to reduce the feature set for enhancing the quality of service.

REFERENCES

[1] X. -Y. Kong and G. -H. Yang, "An Intrusion Detection Method Based on Self-Generated Coding Technology for Stealthy False Data Injection Attacks in Train-Ground Communication Systems," in IEEE Transactions on Industrial Electronics, vol. 70, no. 8, pp. 8468-8476, Aug. 2023, doi: 10.1109/TIE.2022.3213899.

[2] M. E. Aminanto, R. S. H. Wicaksono, A. E. Aminanto, H. C. Tanuwidjaja, L. Yola and K. Kim, "Multi-Class Intrusion Detection Using Two-Channel Color Mapping in IEEE 802.11 Wireless Network," in IEEE Access, vol. 10, pp. 36791-36801, 2022, doi: 10.1109/ACCESS.2022.3164104.

[3] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," in Journal of Communications and Networks, vol. 24, no. 2, pp. 264-273, April 2022, doi: 10.23919/JCN.2022.000002.

[4] M. Ozkan-Okay, Ö. Aslan, R. Eryigit and R. Samet, "SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN," in IEEE Access, vol. 9, pp. 157639-157653, 2021, doi: 10.1109/ACCESS.2021.3129600.

[5] J. Wang, Z. Tian, M. Zhou, J. Wang, X. Yang and X. Liu, "Leveraging Hypothesis Testing for CSI Based Passive Human Intrusion Direction Detection," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7749-7763, Aug. 2021, doi: 10.1109/TVT.2021.3090800.

[6] R. Zhao et al., "An Efficient Intrusion Detection Method Based on Dynamic Autoencoder," in IEEE Wireless Communications Letters, vol. 10, no. 8, pp. 1707-1711, Aug. 2021, doi: 10.1109/LWC.2021.3077946.

[7] Gajare, M. ., & Shedge, D. K. . (2023). CMOS Trans conductance Based Instrumentation Amplifier for Various Biomedical signal Analysis. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 63–71. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2532

[8] M. Dener, S. Al and A. Orman, "STLGBM-DDS: An Efficient Data Balanced DoS Detection System for Wireless Sensor Networks on Big Data Environment," in IEEE Access, vol. 10, pp. 92931-92945, 2022, doi: 10.1109/ACCESS.2022.3202807.

[9] Y. Wu, L. Nie, S. Wang, Z. Ning and S. Li, "Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach," in IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3094-3106, 15 Feb.15, 2023, doi: 10.1109/JIOT.2021.3112159.

[10] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo and F. L. Soares, "An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost

Platform," in IEEE Access, vol. 9, pp. 166855-166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[11] G. A. N. Segura, A. Chorti and C. B. Margi, "Centralized and Distributed Intrusion Detection for Resource-Constrained Wireless SDN Networks," in IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7746-7758, 15 May15, 2022, doi: 10.1109/JIOT.2021.3114270.

[12] Y. Du, J. Xia, J. Ma and W. Zhang, "An Optimal Decision Method for Intrusion Detection System in Wireless Sensor Networks With Enhanced Cooperation Mechanism," in IEEE Access, vol. 9, pp. 69498-69512, 2021, doi: 10.1109/ACCESS.2021.3065571.

[13] A.Ghasempour, "Internet of Things in smart grid: Architecture applications services key technologies and challenges", Inventions, vol. 4, no. 1, pp. 22, Mar. 2019.

[14] M. Nivaashini and P. Thangaraj, "Computational intelligence techniques for automatic detection of Wi-Fi attacks in wireless IoT networks", Wireless Netw., vol. 27, no. 4, pp. 2761-2784, May 2021.

[15] M. Hassaballah, M. A. Hameed, A. I. Awad and K. Muhammad, "A novel image steganography method for industrial Internet of Things security", IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7743-7751, Nov. 2021.

[16] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, pp. e4150, Jan. 2021.

[17] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning", Int. J. Inf. Secur., vol. 20, no. 3, pp. 387-403, Jun. 2021.

[18] A.Thakkar and R. Lohiya, "A survey on intrusion detection system: Feature selection model performance measures application perspective challenges and future research directions", Artif. Intell. Rev., vol. 55, pp. 453-563, Jul. 2021.

[19] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system", Comput. Secur., vol. 92, May 2020.

[20] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection", IEEE Trans. Inf. Forensics Security, vol. 13, no. 3, pp. 621-636, Mar. 2018.

[21] L. Jing and Y. Tian, "Self-supervised visual feature learning with deep neural networks: A survey", IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, no. 11, pp. 4037-4058, Nov. 2021.

[22] R. S. H. Wicaksono, A. A. Septiandri and A. Jamal, "Human embryo classification using self-supervised learning", Proc. 2nd Int. Conf. Artif. Intell. Data Sci. (AiDAS), pp. 1-5, Sep. 2021.

[23] H. Firat and D. Hanbay, "Classification of hyperspectral images using 3D CNN based ResNet50", Proc. 29th Signal Process. Commun. Appl. Conf. (SIU), pp. 1-4, Jun. 2021.

[24] Simhadri Madhuri, S Venkata Lakshmi, “ Detecting Emotion from Natural Language Text Using Hybrid and NLP Pre-trained Models”, “Turkish Journal of Computer and Mathematics Education” Vol.12 No.10 (2021), 4095-4103, doi: 10.17762/turcomat.v12i10.5122

[25] María, K., Järvinen, M., Dijk, A. van, Huber, K., & Weber, S. Machine Learning Approaches for Curriculum Design in Engineering Education. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/111

[26] A.A. Septiandri, A. Jamal, P. A. Iffanolida, O. Riayati and B. Wiweko, " Human blastocyst classification after in vitro fertilization using deep learning ", Proc. 7th Int. Conf. Advance Inform. Concepts Theory Appl. (ICAICTA), pp. 1-4, Sep. 2020.

[27] Q. Duan, X. Wei, J. Fan, L. Yu and Y. Hu, "CNN-based intrusion classification for IEEE 802.11 wireless networks", Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC), pp. 830-833, Dec. 2020.

[28] Al-Turaiki and N. Altwaijry, "A convolutional neural network for improved anomaly-based network intrusion detection", Big Data, vol. 9, no. 3, pp. 233-252, Jun. 2021.

[29] L. Pan and X. Xie, "Network intrusion detection model based on PCA+ADASYN and XGBoost", Proc. 3rd Int. Conf. E-Bus. Inf. Manage. Comput. Sci., pp. 44-48, Dec. 2020.

[30] Chang Lee, Deep Learning for Speech Recognition in Intelligent Assistants , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[31] M. Ozkan-Okay and R. Samet, "Hybrid intrusion detection approach for wireless local area network", Proc. 7th Int. Conf. Control Optim. Ind. Appl., pp. 311-313, 2020.

[32] Ö. Aslan, M. Ozkan-Okay and D. Gupta, "A review of cloud-based malware detection system: Opportunities advances and challenges", Eur. J. Eng. Technol. Res., vol. 6, no. 3, pp. 1-8, Mar. 2021.

[33] S Venkata Lakshmi, Valli Kumari Vatsavayi “Query optimization using clustering and Genetic Algorithm for Distributed Databases”, International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2016, doi: 10.1109/ICCCI.2016.7479934.

[34] S Venkata Lakshmi, Valli Kumari Vatsavayi “Teacher-Learner & Multi-Objective Genetic Algorithm Based Query Optimization Approach For Heterogeneous Distributed Database Systems”, Journal of Theoretical and Applied Information Technology, April 2017.

[35] Dhabliya, D. (2021). An Integrated Optimization Model for Plant Diseases Prediction with Machine Learning Model . Machine Learning Applications in Engineering Education and Management, 1(2), 21–26. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/15

[36] Sunita A Yadwad, Dr V. Valli Kumari and Dr S Venkata Lakshmi. Service Outages Prediction through Logs and Tickets Analysis. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 4, 2021, doi: 10.14569/IJACSA.2021.0120424.

[37] Simhadri Madhuri, S Venkata Lakshmi, “A Trusted Node Feedback Based Clustering Model For Detection Of Malicious Nodes In The Network”, Journal of Theoretical and Applied Information Technology, Vol.101. No 7, 2023

***Article Received**: 01 May 2023 **Revised:** 30 June 2023 **Accepted:** 28 July 2023*

[38] Simhadri Madhuri, S Venkata Lakshmi, “A machine learning-based normalized fuzzy subset linked model in networks for intrusion detection”, Soft Computing, 2023, doi: 10.1007/s00500-023-08160-6