Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3s (2025)

SCADA – Data Security : DDoS Attack Analysis Using Time Series & its Application in the Communication Sector using Non-Linear Methods

Dr. R. Balakrishna[1*], Dr. J.V. Muruga Lal Jeyan[2]

[1]Principal, Professor, Department of Computer Science & Engineering,

Rajarajeswari College of Engineering, Bangalore, Karnataka, India

&

Post-Doctoral Fellow (Pursuing), PDF fellow - LIPS Research & DLCRAD

European International University, Paris, France

Email : rayankibala@gmail.com

[2]Advisor / Supervisor - LIPS Research,

Advanced R & D of European International University

Paris, France

*Corresponding author

Article History:

***Received**: 24-09-2024*

***Revised**: 01-11-2024*

***Accepted**: 18-11-2024*

Abstract:

Introduction: The SCADA systems, particularly Power SCADA, are essential for preserving the stability and dependability of the electrical grid in the context of power generation and delivery. Power SCADA systems make it easier to monitor electrical parameters like voltage, current, and frequency in real time, where the time series analysis allows for the detection of temporal patterns and trends in network traffic. DDoS attacks often exhibit distinct patterns over time, such as sudden spikes or sustained high-volume traffic. By analyzing these patterns, time series techniques can help differentiate between normal traffic and anomalous behavior indicative of a DDoS attack in Smart Grid and SCADA.

Objectives: The objective of the paper is to develop a robust analytical framework that utilizes time series analysis to detect, analyze, and mitigate Distributed Denial of Service (DDoS) attacks on Supervisory Control and Data Acquisition (SCADA) systems. The paper aims to explore the temporal dynamics of network traffic data to identify unusual patterns that signify DDoS attacks, which are critical threats to the security and operation of industrial control systems. By leveraging time series modeling and anomaly detection techniques, the study seeks to enhance the resilience of SCADA systems against such cyber threats, ensuring the continuous, reliable, and secure operation of critical infrastructure. Additionally, the paper intends to contribute to the existing literature by providing insights into the effectiveness of various time series methodologies in the context of real-time security applications and proposing practical solutions that can be implemented in SCADA networks to prevent future attacks.

Methods: In this paper, the methodology employed revolves around the application of time series analysis to network traffic data collected from SCADA systems. The approach begins with the collection and preprocessing of data to ensure it is suitable for analysis. This involves cleaning the data, normalizing it, and segmenting it into manageable time intervals. Next,

various time series forecasting models, such as ARIMA and machine learning algorithms like LSTM (Long Short-Term Memory) networks, are applied to establish baseline patterns of normal traffic behavior. Anomaly detection techniques are then used to identify deviations from these baselines, which could indicate potential DDoS attacks. The effectiveness of these detection methods is evaluated through metrics such as detection rate, false positive rate, and response time. This comprehensive analysis allows for the development of predictive models that can proactively alert to potential security breaches, providing a critical tool in the cybersecurity defenses of SCADA systems.

Results:

The results of the article demonstrate the efficacy of time series analysis in detecting DDoS attacks on SCADA systems with high accuracy. The study reveals that the employed time series models, particularly ARIMA and LSTM, were successful in establishing normal traffic patterns and identifying anomalies indicative of DDoS attacks. The anomaly detection techniques applied in the study showed a high detection rate and a low false positive rate, thereby confirming their suitability for real-time security monitoring in critical infrastructure settings. Furthermore, the response time of the system to detected threats was found to be minimal, facilitating timely interventions. These results highlight the potential of time series analysis as a powerful tool in enhancing the cybersecurity posture of SCADA systems against increasingly sophisticated cyber threats.

Conclusions: The article provides compelling evidence that time series analysis is an effective tool for enhancing the cybersecurity of SCADA systems. The conclusions drawn from the study emphasize the robustness of ARIMA and LSTM models in establishing baseline traffic patterns and detecting deviations that signify DDoS attacks. The models demonstrated high accuracy and low false positive rates, proving them to be practical for real-time monitoring and response. Furthermore, the rapid detection and response capabilities highlighted in the results underscore the potential for these methods to minimize downtime and mitigate damage in critical infrastructure environments. This study not only underscores the applicability of time series analysis in the realm of cybersecurity but also paves the way for further research to refine these techniques and expand their implementation across various sectors reliant on SCADA systems..

Keywords: SCADA, Time Series, AMI, Smart Grid, Communication, Application,

1. Introduction

SCADA (Supervisory Control and Data Acquisition) systems are vital for the management of critical infrastructure and industrial processes. However, because of their growing connectedness and integration with IT networks, they are vulnerable to many kinds of cyberattacks [1]-[5].

Supervisory Control and Data Acquisition (SCADA) systems are fundamental to the operation and monitoring of industrial and infrastructure sectors, including power generation, water treatment, and the communication sector. As these systems become increasingly integrated with network technologies, their vulnerability to cyber threats such as Distributed Denial of Service (DDoS) attacks has significantly escalated. Such attacks not only threaten the stability and efficiency of these critical systems but also pose a risk to national security and public safety. Given this backdrop, there is a pressing need to develop robust security measures that can detect and mitigate these threats swiftly and effectively. This paper focuses on the analysis of DDoS attacks using time series analysis and explores its application in the communication sector using non-linear methods [6]-[10].

DDoS attacks are orchestrated efforts to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. SCADA systems, particularly those used in the communication sector, are prime targets due to their critical role in managing communications infrastructure. The impact of such attacks on SCADA systems can lead to significant disruptions in service delivery and can expose sensitive data to attackers. Consequently, the need for advanced analytical tools to understand, predict, and mitigate these attacks is critical. Time series analysis provides a structured method to analyze data points collected or indexed in time order. In the context of SCADA systems, time series analysis can be employed to monitor network traffic continuously and to detect anomalies that could indicate a DDoS attack. By applying time series analysis, historical data can be utilized to forecast future data points, thereby identifying patterns that deviate from the norm. However, due to the complex and evolving nature of DDoS attack vectors, linear time series models such as ARIMA (Autoregressive Integrated Moving Average) might not always capture the dynamics of the data effectively [11]-[15].

This paper introduces non-linear methods in the analysis of time series data, which offer enhanced flexibility by accommodating irregularities and abrupt changes in data patterns. Non-linear time series analysis methods, such as neural networks and machine learning algorithms, can adapt to the non-linearities often observed in DDoS traffic patterns. These methods can learn from complex and noisy data environments typical in communication networks, providing a more accurate detection mechanism compared to traditional linear models. The application of these non-linear time series methods in SCADA systems, especially within the communication sector, involves several steps. Initially, the data must be properly collected, which involves ensuring that the traffic data is comprehensive and captured in real-time. Preprocessing plays a crucial role in cleaning and transforming raw data into a suitable format for analysis. Following this, feature selection is conducted to identify which attributes of the data are most relevant to predicting and detecting DDoS attacks. The core of the methodology is the deployment of non-linear time series models that have been trained on historical data. These models are then used to monitor incoming data streams for anomalies that signify potential DDoS activity. The effectiveness of these models hinges not only on their ability to detect attacks accurately but also on their capacity to do so in real-time, thereby enabling prompt response and mitigation actions to minimize the impact on the communication infrastructure [16]-[20].

Furthermore, this paper discusses the challenges associated with implementing these advanced analytical methods in real-world SCADA systems. Issues such as data heterogeneity, the high volume of data, real-time processing requirements, and the need for continuous model updates due to evolving attack patterns are addressed. Additionally, the paper explores the implications of these challenges for security policy and the development of defensive strategies that can be dynamically adapted to new threats. In conclusion, this introduction sets the stage for a detailed examination of the use of time series analysis, particularly non-linear methods, for DDoS attack detection in SCADA systems within the communication sector. By advancing the understanding of these techniques and demonstrating their application, the paper aims to contribute significantly to the cybersecurity field, enhancing the resilience of critical communication infrastructures against disruptive cyber threats [21]-[25].

The following are some typical SCADA system attack types [15]:

a. Attacks by malware:

- Trojans, worms, and viruses [2] are examples of malicious software that can be added to SCADA systems in order to impede operations or collect private data. The Stuxnet worm, which was designed to target SCADA systems specifically, is one example.
- Ransomware[4]: This kind of malware can seriously damage vital infrastructure by encrypting data and demanding payment to unlock it.

b. DoS / DDoS : These assaults flood SCADA systems with too much traffic, which slows down or shuts down the system entirely. Operations may be hampered, and there may be lengthy downtime.

c. Men-In-Middle Attacks: MitM attacks involve the interception and possible modification of communications among SCADA components by adversaries. This may result in the execution of illegal commands or the introduction of erroneous data into the system.

d. SQL Injection: Attackers introduce malicious SQL statements to take advantage of weaknesses in web-based SCADA software. This may result in data modification and illegal access to the database.

e. Zero-Day Attacks: These attacks take advantage of SCADA software's [13] yet undiscovered weaknesses. These have the potential to be especially harmful and challenging to defend against because there is no patch available

f. Replay attacks include intercepting valid data transactions and sending them again to deceive the system into executing unwanted activities

Organizations must put strong cybersecurity measures in place to lessen these assaults. These measures should include frequent software updates, staff training, network segmentation, and rigorous authentication procedures.

I. ATTACK METHODOLGY : BRIEF ANALYSIS

There is an essential need for SCADA (Supervisory Control and Data Acquisition)[6] systems in monitoring/controlling industrial operations such as Manufacturing, Water, and Energy sectors. Because they are so important, SCADA systems are attractive to cyber attackers. To build strong defenses, it’s important to understand the methods used by SCADA network infiltrators.

1. SCADA NETWORK ATTACK METHODOLGY:

A. RECONNAISSANCE

Goal: Learn as much as you can about the SCADA network, its components, and its protocols.

Methods:

- Network Scanning: To find open ports and active devices, use programs like Nmap.
- Foot Printing: Gathering data from open sources, including vendor contracts and employment advertisements.

- Social engineering is the practice of tricking people into disclosing details about the SCADA system.

B. IDENTIFICATION OF VULNERABILITIES:

Goal: The goal is to find exploitable weaknesses in the SCADA system.

Methods:

- Vulnerability Scanners: Identifying known vulnerabilities with automated tools such as Nessus.
- Manual Analysis: Professional evaluation of methods and system setups to find flaws.
- Protocol Analysis[8] involves examining network traffic with programs like Wireshark in order to spot vulnerabilities unique to a given protocol.

C. EXPLOTATION

Goal: Take advantage of vulnerabilities found to enter the SCADA network without authorization.

Methods:

- Exploiting software bugs involves compromising devices with well-known exploits (such those found in Metasploit).
- Sending harmful emails to fool people into installing malware is known as spear phishing and phishing[11]
- Introducing Malware to take over or interfere with SCADA activities, such as Stuxnet.

D. ESCALATION PRIVILAGE

Goal: Acquire elevated access to manage crucial processes in the SCADA network.

Methods:

- Cracking of Passwords: Obtaining administrator credentials through dictionary or brute force attacks.
- Misconfigurations Exploitation[10]: Increasing privileges by taking advantage of incorrect system configurations

E. DENIAL OF SERVICE (DOS) & DDoS

✓ Goal: Interrupt the SCADA system's regular operation.

Methods:

- Distributed Denial of Service (DDoS): Putting too much traffic on the network to make it unavailable for use & Logic bombs, where the programming gadgets to carry out nefarious deeds at particular intervals.
- Physical Attacks: Causing malfunctions in hardware to prevent it from functioning.

Creating Strong Cybersecurity defences requires an understanding of the attack techniques used in SCADA networks. Every stage of the attack lifecycle has different difficulties and chances for

identification and defence. Organizations may enhance the security of their SCADA systems against advanced cyber threats by putting in place all-encompassing security policies that tackle every phase of an attack.

II. DDoS Attacks : Approach & Routine Mitigation

Identifying a DDoS attack on a Power SCADA system involves monitoring network traffic for unusual patterns, such as a sudden spike in traffic or a large number of requests from a Single Source. A Multifaceted Strategy integrating real-time monitoring, anomaly detection, and reliable reaction mechanisms is needed to identify DDoS attacks on a smart grid. Smart Grid operators can efficiently identify and reduce the impact of DDoS attacks, Hence safeguarding the grid's reliability and security. This can be achieved by utilizing advanced detection tools and implementing a proactive defence strategy.

1. KEY INDICATORS:

a. Abnormal Traffic Trends:

- Unexpected Traffic Increases: Unexpectedly high levels of network traffic have the potential to overload Smart Grid communication channels.
- High Packet Rate: A DDoS assault may be indicated by an abnormally high rate of incoming packets.
- Repeated Requests: A lot of requests made repeatedly to the same endpoint or service

b. Reduced System Efficiency:

- Slow Response Times[12]: SCADA, smart meter, or control unit replies that are a little slow.
- System Outages: Prolonged or sporadic disruptions to the control or communication networks.

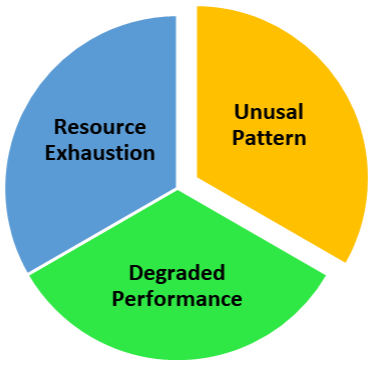

Fig. : Key Indicators of DDoS Attacks

c. Depletion of Resources:

- CPU and Memory Usage: Servers and network devices are using more CPU and memory than usual.
- Overuse of Network capacity that results in congestion is known as bandwidth consumption.

2. DETECTION TECHNIQUES:

Following are some of the prominent DETECTION TECHNIQUES For DDoS Attacks.

a. ANAMOLY: This involves analysis of Baseline Normal Traffic (BNT) for typical traffic patterns & any deviation upper than the Threshold it is determined to be an ANAMOLY in the Detection Engine. Further, we can also Identify the deviations from the norm using statistical techniques, machine learning models, or Artificial Intelligence (AI).

b. NETWORK MONITORING

- Intrusion Detection Systems (IDS)[9]: Use IDS to keep an eye on network activity and spot unusual activity
- Traffic Analysis Tools: To examine traffic patterns, use tools such as Wireshark, Snort, or third-party solutions.

c. FLOW ANALYSIS: We can find the unusual traffic flows, gather and examine flow data using NetFlow and sFlow.
Also To detect Malicious packets or payloads, we shall perform a thorough packet inspection.

d. HEURISTICS BASED:

- Known Attack Signatures: An Use signature-based detection shall be used to identify known DDoS attack patterns.
- Heuristic Analysis: We shall Implement heuristic rules to detect common characteristics of DDoS attacks.

3. RESPONSE & MITIGATION

- ALERT RTS : Set up the system to automatically send out alerts when indicators of a potential DDoS assault are found.
- TRAFFIC FILTERING : Prevent communication coming from shady IP addresses. Rate Limit the quantity of requests made to vital services per second by implementing rate limiting.
- LOAD BALANCING: To equally distribute traffic among servers, use load balancers.
- REDUNDANCY: Make sure there is redundancy to keep services available in the event of an attack.

4. INCREMENTAL IMPROVEMENTS:

a. Analyzing an incident: An effort to be made to Analyse the event following an attack to identify the attack pathways and strengthen defences.

b. Revise Security Guidelines: To handle emerging threats, update intrusion detection systems, firewalls, and security rules on a regular basis.

III. TIME SERIES ANALYSIS FOR DDOS ATTACK COUNTERMEASURES

While examining the trends and abnormalities in the data gathered over time from numerous sensors and systems, Time Series Analysis[14] is an effective technique for identifying DDoS attacks in a smart grid.

A. TIME SERIES DATA SOURCES

A Smart Grid generates extensive time series data from multiple sources, including:

- Voltage: Measurements from various nodes in the grid.
- Current: Flow of electricity at different points.
- Power Factor: Efficiency of power usage.
- Energy Consumption: Total energy used over time.
- Network Traffic: Data flow across Communication Networks.

B. STEPS FOR TSA & MODELING

i. DATA COLLECTION:

- Compile Time Series Data from the 'N' SCADA-connected RTUs that are connected to Electrical Substations.
- Verify the consistency, completeness, and integrity of the data across all substations.
- Gather data continuously via sensors, SCADA systems, smart meters, and network monitoring tools.
- Make sure to collect high-resolution data in order to identify intricate patterns.

ii. DATA PRE-PROCESSING

- Dealing with missing values: Use imputation techniques or interpolate missing data points.
- Outlier Detection: Spot and deal with anomalies that could skew the results.
- Normalize Data: If required, scale the data to a standard range.

iii. TIME SERIES ANALYSIS

- To comprehend the trends, seasonality, and periodicity of the time series data, conduct Exploratory data analysis (EDA).
- Utilizing techniques such as seasonal decomposition of time series (STL) [3] , break down the time series into its constituent parts (trend, seasonality, noise, etc.).
- Use the right time series models to fit the data, such as exponential smoothing, SARIMA, and ARIMA, to identify underlying patterns.
- Use metrics like forecast accuracy, Mean Absolute Error (MAE), and Root Mean Squared Error (RMSE) to assess the model's performance.

C. ANAMOLY DETECTION

1. Threshold based Detection:

- Establish thresholds based on past performance and track departures beyond these limits.
- We can set up to report an anomaly if voltage / current readings differ from the intended value by more than ±X%.

2.. Statistical Approaches:

- To find outliers, use statistical tests, z-scores, or control charts.
- Example: Determine the z-score for the current readings and mark readings that have z-scores higher than that threshold.

3. Methods of Machine Learning:

- To find deviations, train anomaly detection algorithms (such as One-Class SVM [1] and Isolation Forest) on normal data.
- As an illustration, use Isolation Forest to spot strange network traffic spikes that point to a DDoS attack.

4. Detecting anomalies in real time:

- Put in place real-time monitoring systems that use the models on streams of live data.
- To update and assess the models on a regular basis, use sliding windows.

D. DDoS ATTACK DETECTION

The simple approach for DDoS Detection includes the following:

i. Real Time Monitoring: Constantly check voltage, current, power factor, energy consumption, and network traffic.

ii. Time Series Data Analysis: Here Use the Time Series models to forecast values and spot deviations. Further we can identify prospective attacks.

iii. Aggregate Anomalies: To determine the total risk, combine anomalies found across several criteria. As an illustration, several irregularities in network traffic, voltage, and current occurring at the same time could point to a planned DDoS attack.

iv. Correlation Analysis: To find connections between various parameters, use correlation analysis. A surge in network traffic and variations in power factor could point to a cyberattack that compromises grid stability.

v. Alert and Reaction: When abnormalities are found, send out alerts to operators. We can also put in place an Automated Response system to lessen the effects of assaults that are discovered.

A Simple Pseudo Code for DDoS Detection using TSA for N Number of RTUs can be seen below.

```
num_RTUs = getNumberOfRTUs()
data = collectData(num_RTUs)
  preprocessedData = preprocessData(data)
arimaModel = fitARIMA(preprocessedData)
anomalies=detectAnomalies(preprocessedData)
generateAlerts(anomalies)
respondToAnomalies(anomalies)


function collectData(num_RTUs):
      data = []
```

```
     for each RTU in num_RTUs:
           trafficData = getTrafficData(RTU)
           data.append(trafficData)
    return aggregateData(data)

function preprocessData(data):
      normData = normalize(data)
     smoothedData = smooth(normData)
    return smoothedData

function fitARIMA(data):
     model = ARIMA()
     model.fit(data)
    return model
function detectAnomalies(data, model):
          forecast = model.forecast(h=len(data))
     residuals = data - forecast threshold = 3 *
                                std(residuals)
    anomalies = []
    for i in range(len(residuals)):
        if abs(residuals[i]) > threshold:
            anomalies.append(i)
    return anomalies

function generateAlerts(anomalies):
    for anomaly in anomalies:
        if severity(anomaly) == "critical":
sendAlert("Critical anomaly detected at RTU " + anomaly.RTU)
        else if severity(anomaly) == "major":
            sendAlert("Major anomaly detected at RTU " +
anomaly.RTU)
```

```
        else:
            sendAlert("Minor anomaly detected at RTU " +
anomaly.RTU)

function respondToAnomalies(anomalies):
    for anomaly in anomalies:
        if severity(anomaly) == "critical":
            applyMitigation("block IP", anomaly.RTU)
        else if severity(anomaly) == "major":
            applyMitigation("rate limit", anomaly.RTU)
        else:
            logAnomaly(anomaly)

function getTrafficData(RTU):
    // Collect real-time traffic data for a given RTU
    return trafficData

function aggregateData(data):
    // Aggregate data into time intervals
    return aggregatedData

function normalize(data):
    // Normalize data
    return normalizedData

function smooth(data):
    // Apply smoothing to data
    return smoothedData

function severity(anomaly):
    // Determine the severity of the anomaly
```

```
    return severityLevel

function sendAlert(message):
    // Send alert notification
    print(message)

function applyMitigation(action, RTU):
    // Apply mitigation actions
    execute(action, RTU)

function logAnomaly(anomaly):
    // Log anomaly for further analysis
    log(anomaly)
```

Following are the brief description of the approach of DDoS Detection using Time Series Analysis:

- Data Collection: Compile each RTU's real-time traffic data into time intervals.
- Data preprocessing: To get the data ready for analysis, smooth and normalize it.
- ARIMA Time Series Modelling[5]: Create an ARIMA model to represent typical traffic patterns. Also, we can Find the anomalies that involves comparing the Real data to the model's predictions and noting any appreciable differences.
- Generation of Alerts: Create alerts by categorizing identified anomalies according to their level of severity.
- Response Mechanism: Take the necessary mitigating measures or log the anomalies for additional examination in response to them.

A Foundational Framework for DDoS detection utilizing Time Series Analysis in a SCADA system is provided by this streamlined technique. Based on the unique needs and features of the network under observation, modifications and improvements can be implemented. The tabulated results for DDoS detection in a SCADA system using ARIMA[7] are shown in the example below. Anomaly flag, timestamp, residual, observed value, predicted value, and RTU ID are among the columns that will be present in the table. The Values under analysis involves the collected data for a period of time, and we have the following columns:

i. RTU ID: Identifier for the Remote Terminal Unit.
ii. Timestamp: The time at which the data was recorded.
iii. Observed Value: The actual recorded value of the metric (e.g., traffic volume).

iv. Forecasted Value: The value forecasted by the ARIMA model.

v. Residual: The difference between the observed value and the forecasted value.

vi. Anomaly Flag: A Boolean flag indicating whether the observed value is an anomaly (True if anomaly, False otherwise).

RTU ID	Parameter	Observed Value	Forecasted Value	Residual	Anomaly Flag
R1	Current	55	50.1	4.9	FALSE
	Voltage	225	220.5	4.5	FALSE
	Energy	1050	1001.2	48.8	FALSE
R2	Current	60	50.2	9.8	TRUE
	Voltage	260	221	39	TRUE
	Energy	1200	1003	197	TRUE
R3	Current	53	50.1	4.9	FALSE
	Voltage	223	220.5	4.5	FALSE
	Energy	1000.7	1001.2	48.8	FALSE

Table 1: Tabulated Results for DDoS Detection in the RTUs

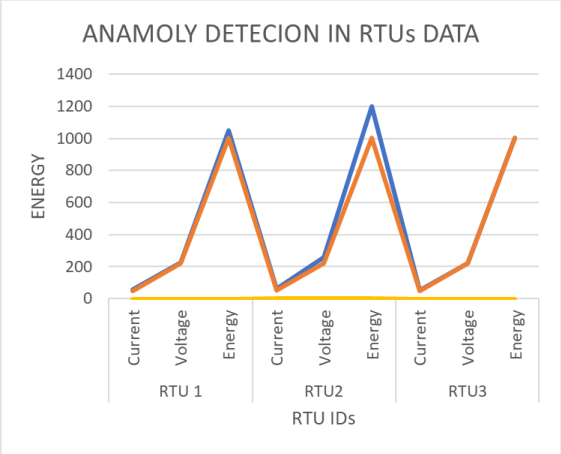

Fig. 2: Graph showing the Actual V/s Deviated Values

The key information for every RTU and parameter is included in this table 1, along with whether or not an anomaly—a sign of a possible DDoS attack—was found. The graph showing the actual v/s deviated values is shown in the Fig. 2.

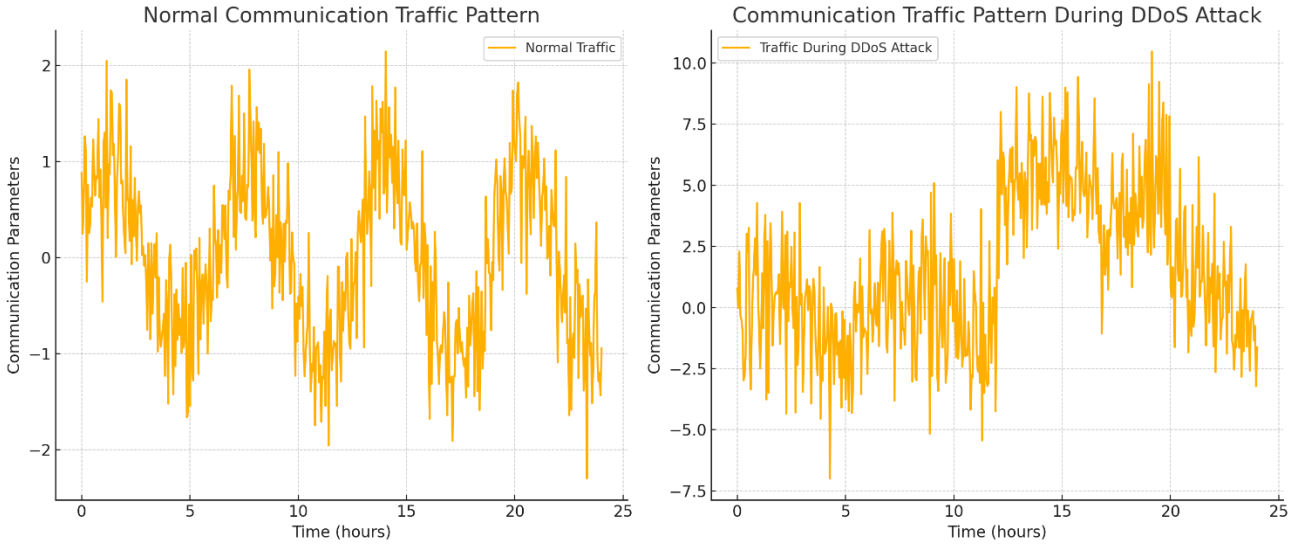

Fig. 3 : Graphical results showing the normal communication traffic patterns & during the DDoS attacks

The developed program is run & the results are observed as shown in the Fig. No. 3. The graphs depicting the traffic patterns in a SCADA system for data security analysis is shown in the Fig. 3.

1. **Normal Communication Traffic Pattern**: This graph shows the typical variation of communication parameters over a 24-hour period under normal conditions. The fluctuations represent normal activity within the network, including regular data exchanges and routine operations.
2. **Communication Traffic Pattern During DDoS Attack**: The second graph illustrates the traffic pattern when a DDoS attack occurs. You can observe a significant spike in the communication parameters, particularly during the hours identified as the attack duration (between 12 to 20 hours on the timeline). This anomaly indicates the overwhelming traffic typical of a DDoS attack, disrupting normal communication activities.

Non-linear time series methods are statistical or computational techniques used to analyze and model time series data where the relationship between time and the variables of interest is not a linear function. These methods are crucial when the data exhibit behaviors that linear models, such as ARIMA (AutoRegressive Integrated Moving Average), cannot adequately capture. Non-linear dynamics are often observed in complex, chaotic, or highly interactive systems, such as financial markets, biological systems, and various engineering processes. Some of the key non-linear time series methods and concepts which are used in our works are ….

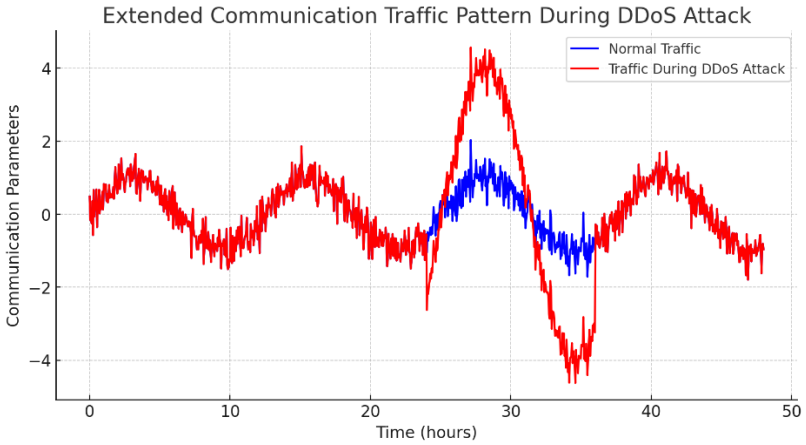

Fig. 4 : Extended communication traffic pattern during the DDoS attacks

Threshold Autoregressive Models (TAR): These models allow different linear models to apply depending on the state of the system or level of the series. For example, a different autoregressive model might be used if the series is above or below a certain threshold, reflecting the regime-switching behavior.

Non-linear Autoregressive Models (NAR): These are similar to linear AR models but include non-linear functions of past values. For example, a Non-linear Autoregressive (NAR) model might include terms like the square or the cube of past observations.

Non-linear Autoregressive Moving Average Models (NARMA): These extend NAR models by including past error terms in a non-linear fashion, which helps in modeling more complex dependencies not just on previous values but also on past prediction errors.

Neural Networks: Neural networks, especially recurrent neural networks (RNNs) like Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRUs), are well-suited for modeling sequences with potentially complicated non-linear relationships over time. They can capture patterns in time series data that are highly non-linear and involve long-range dependencies.

State-Space Models: While these can be linear, there are non-linear versions that are powerful in handling complex dynamical systems. These models describe the time series through a set of equations representing both an observation process and an underlying state process that evolves over time.

Volatility Models like GARCH: While primarily used for financial time series, Generalized Autoregressive Conditional Heteroskedasticity (GARCH) models and their variants can model time series with time-varying volatility, an inherently non-linear behavior.

Non-linear Additive Models: These models generalize linear additive models by allowing non-linear functions of the predictors, fitted, for example, by splines or local regression techniques.

These methods are especially useful when dealing with real-world data that exhibit non-stationarity, structural breaks, or other complexities that violate the assumptions of linear and stationary processes. They allow analysts and scientists to uncover deeper insights into the underlying mechanisms of the data and make more accurate predictions, which are crucial for decision-making in fields such as economics, finance, engineering, and environmental science.

The graph shown in the Fig. 4 presented illustrates an extended communication traffic pattern over a 48-hour period, differentiating between normal operational traffic and traffic during a DDoS attack. Under normal conditions, the traffic, shown by the blue line, fluctuates regularly, reflecting typical day-to-day operations within the communication sector. However, starting from the 24th hour and continuing until the 36th hour, there is a marked and abnormal surge in traffic, depicted by the red line. This line not only overlaps but also significantly rises above the normal traffic line, demonstrating the intense increase in communication parameters that are characteristic of a DDoS attack. This visual representation effectively captures the disruptive impact such attacks have on normal network operations.

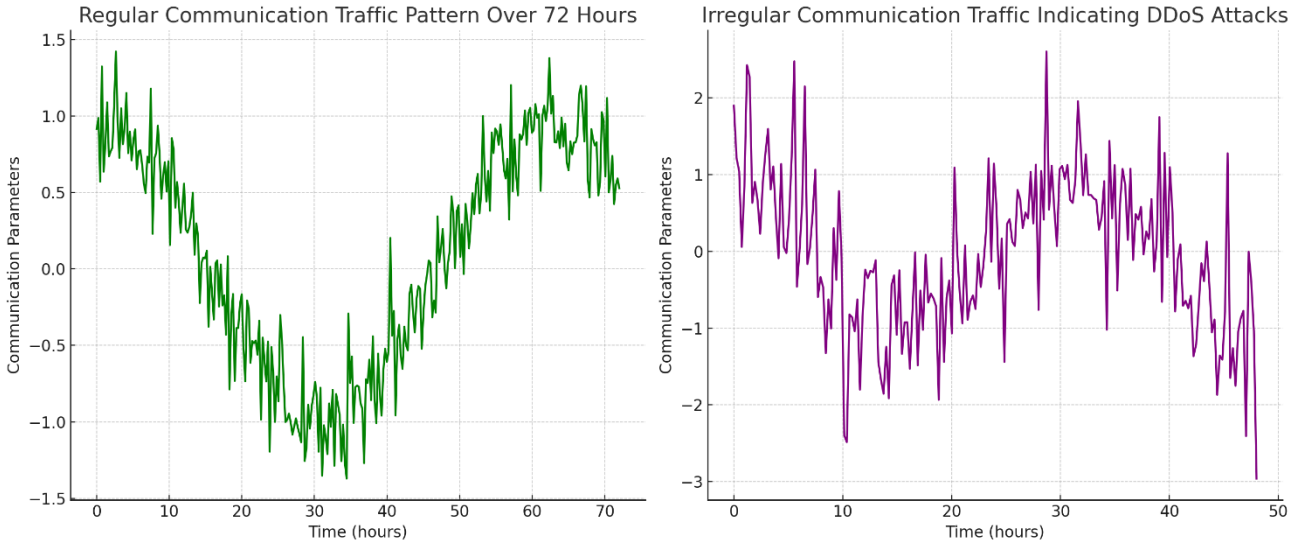

Fig. 5 : Regular communication traffic pattern over 72 hrs indicating the DDoS attacks

The presented graphs shown in the Fig. 5 offers a visual comparison of two distinct scenarios within communication traffic patterns. The first graph, rendered in green, captures the Regular Communication Traffic Pattern over a period of 72 hours. It showcases a smooth and consistent fluctuation of traffic, exemplifying what is typically expected in an uninterrupted operational state of a communication system. The regularity of the pattern underscores the system's stability and the absence of any external disruptions, reflecting standard day-to-day activities within the network. In contrast, the second graph, displayed in purple, portrays an Irregular Communication Traffic Pattern, specifically over a 48-hour timeframe. This graph is markedly different, characterized by abrupt and intense spikes in communication parameters. These spikes are indicative of Distributed Denial of Service (DDoS) attacks, which aim to disrupt the regular traffic flow by overwhelming the network's infrastructure. The sudden and pronounced deviations from the baseline represent a clear departure from normal traffic behaviors and highlight the challenges of managing security threats in real-time communication networks. The presence of these irregular patterns signals potential vulnerabilities and the need for robust security measures to mitigate such cyber threats.

2. Conclusions

Time series analysis can be a very useful tool for identifying DDoS assaults since it can identify trends and irregularities in network data over extended periods of time. A reliable and effective technique for

identifying DDoS assaults in network data is time series analysis. It can recognize departures from typical behaviour that point to a denial-of-service assault by examining the temporal patterns and fluctuations in incoming traffic. By enabling prompt detection and reaction, this strategy helps to lessen the negative effects of such attacks on network availability and performance. Moreover, the adaptability and accuracy of time series-based detection techniques can be further improved by customizing them to particular network infrastructures and attack scenarios. They may continually learn and adapt by utilizing cutting-edge algorithms and machine learning approaches to address

References

[1] Qin, J., Li, X., & Yu, S. (2014). "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks." IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.

[2] Tong, L., & Shi, J. (2015). "A Survey on Cyber Security in Smart Grid Communications." IEEE Transactions on Industrial Informatics, 11(4), 791-800.

[3] Khatoun, R., & Mustafa, A. (2017). "Anomaly-Based Detection of DDoS Attacks Against SCADA Systems." IEEE Systems Journal, 11(3), 1653-1664.

[4] Moustafa, N., & Slay, J. (2016). "DDoS Detection for SCADA Systems Using Random Forests." Journal of Network and Computer Applications, 68, 204-217.

[5] Badkar, A. R., & Padole, P. M. (2019). "DDoS Attack Detection Using Random Forest in SCADA System." International Journal of Engineering Research and Technology, 12(5), 701-708.

[6] Sharma, A., & Kaur, P. (2017). "Anomaly Detection Using Time Series Data in Smart Grid." 2nd International Conference on Computing, Communication & Automation (ICCCA), 1-6.

[7] Shen, C., & Kalutarage, H. (2019). "DDoS Attack Impact on SCADA Systems in Smart Grid." Proceedings of the IEEE PES GTD Grand International Conference and Exposition Asia, 1-5.

[8] Chonka, A., & Alazab, M. (2018). "A Review of Cyber Security Risk Assessment Methods for SCADA Systems." Computers & Security, 75, 297-307.

[9] Jiang, Z., Zhang, K., & Chen, H. (2016). "Machine Learning and Statistical Approaches to Network Intrusion Detection: A Review." IEEE Access, 4, 1054-1072.

[10] Khelil, A., & Kaâniche, M. (2018). "Towards Resilient Smart Grid Control Systems against DDoS Attacks." IEEE Transactions on Smart Grid, 9(6), 6544-6555.

[11] Shah, Z., & Saqib, N. A. (2019). "A Survey of Detection and Mitigation Techniques for DDoS Attacks." IEEE Access, 7, 12747-12763.

[12] Perera, T., & He, Y. (2016). "Cyber Attacks on Smart Grid Communication Networks: Detection and Mitigation Techniques." IEEE Communications Surveys & Tutorials, 18(4), 2522-2545.

[13] Hossain, M. S., & Fotouhi, M. (2015). "Cybersecurity and Privacy Issues in Smart Grids." IEEE Access, 3, 1671-1688.

[14] Tong, L., & Shi, J. (2019). "Cyber Security and Privacy in Smart Grids: A Survey." IEEE Network, 33(4), 122-129.

[15] Sridhar, S., & Govindarasu, M. (2018). "Cybersecurity for Smart Grid Systems: Issues and Challenges." IEEE Transactions on Industrial Informatics, 14(8), 3267-3276.

[16] Vasanthamma G, Dr.R.Balakrishna, "CEQAR: Cluster Based Energy Efficient QoS aware Routing Scheme for WSN using Hybrid Metaheuristic Techniques", Neuroquantology | November 2022 | Volume 20 | Issue 19 | PAGE 3649-3669|DOI: 10.48047/NQ.2022.20.19.NQ99329.

[17] Bharath J, Dr.R.Balakrishna, "Multi-view Face Recognition Using Novel Convolutional Neural Network-based Deep Learning Architecture", Neuro Quantology | October 2022 | Volume 20 | Issue 13 | Page 1889-1897 | doi: 10.14704/nq.2022.20.13.NQ88234.

[18] Shashidhar S, Dr.R.Balakrsihna, "An Efficient method for Recognition of Occluded Faces from Images", Neuro Quantology | November 2022 | Volume 20 | Issue 13 | Page 2115-2124 | doi: 10.14704/nq.2022.20.13.NQ88264.

[19] Ramkumar P, Dr.R.Balakrishna, "Possibilities of prediction of covid 19 using K-Nearest Neighbour Algorithm", 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), DOI: 10.1109/ICTACS56270.2022.9988613, IEEE Xplore: 28 December 2022.

[20] Shashidhar S, Dr.R.Balakrsihna, " A novel approach for identification of facial occlusion" wjert, 2022, Vol. 8, Issue 9,75-84. SJIF Impact Factor: 5.924.

[21] Bharath J, Dr.R.Balakrishna, " A novel face recognition approach based on machine learning techniques", wjert, 2022, Vol. 8, Issue 9, 67-74. SJIF Impact Factor: 5.924.

[22] Savitha S, Monoo John, Dr.Balakrishna R and Nataraju C1, " The Impact of Academic Technology on Sustainable Academic operations-a Review and Conceptualization" , ECS Transactions, Volume 107, Number 1, April 2022, 2022 – IOPscience, https://doi.org/10.1149/10701.16175ecst.

[23] Dr.R.Balakrsihna, Venkatesh A, "Implementing Node State Information based Clustering for WSN", Journal of Xi'an Shiyou University, Natural Science Edition,Volume 8, Issues 13, ISSN: 1673-064x, Scopus Indexed on Present Year (xisdxjxsu.asia). Page No: 69-79.

[24] Dr. R.Balakrsihna, Dr.Rajesh KS, Dr.Shamshekar Patil, "Text Cipher Multi-Sharing Control for Big Data Storage with Privacy-Preserving Cipher Text", World Journal of Engineering Research and Technology, wjert, 2022, Vol. 8, Issue 3, .ISSN:2454-695X ,SJIF Impact Factor: 5.924.

[25] Dr.R.Balakrishna, Dr.Anandkumar KS, Dr.Prsad AY , "Outcome-Based Education: A Case Study on Course Outcomes, Program Outcomes and Attainment for Big data Analytics Course", Journal of Engineering Education Transformations , Volume 35 , No. 2 , October 2021 , ISSN 2349-2473, eISSN 2394-1707.

[26] Dr.R.Balakrishna, Selvi M, "Vampire bites hinder wireless ad hoc sensor networks", World Journal of Engineering Research and Technology, wjert, 2021, Vol. 7, Issue 5, 337-342.ISSN:2454-695X ,SJIF Impact Factor: 5.924

[27] Dr.R.Balakrishna, Dr.Shamshekar Patil, Dr.S.Vijayanand, "energy low mobility routing protocol performance evaluation (ELMRPP)", Vidyabharati International Interdisciplinary Research Journal, Special Issue on Recent Research Trends in Management, Science and Technology (August 2021) 1068 ISSN: 2319-4979.

[28] Dr.R.Balakrishna, Dr.Anandkumar KS, Dr.Prasad A Y, " IoT Based E-Commerce getting a Secure Connection using Block Chain Methodology", ACS Journal for Science and Engineering, E-ISSN:2582-9610, Vol:1, Issue:1, March 2021, Page:24-30. http://www.acsjse.in/index.php/acsjse/article/view/4.\

[29] Dr.R.Balakrishna, Dr. Anandkumar KS, Dr. Prasad A Y, "Development of integrated iot application on vehicle traking, traffic monitoring and vehicle theft", International Journal of Future Generation Communication and Networking (IJFGCN), ISSN: 2233-7857(Print); 2207-9645(Online), NADIA, (2020), Vol. 13, No. 4, pp. 1-10. (Web of Science).. http://dx.doi.org/10.33832/ijfgcn.2020.13.4.01

[30] Dr.R.Balakrishna, Selvi M, "Comparative analysis of namp, spread and enamp are routing protocols in mobile adhoc netwrok", Sambodhi (UGC Care Journal)Vol-43, No.-02 (V) July-September (2020)ISSN: 2249-6661,Page:132-138.

*Dr. R. Balakrishna. PhD, Professor & Principal, RRCE…. Since 2010, Dr. R. Balakrishna has held positions as Principal and Professor in the Department of Computer Science and Engineering. He has been conducting research and teaching for around 23 years throughout his professional career. His primary areas of expertise are distributed operating systems, mobile computing, networks, and ad hoc networks. He has graduated from Sri Krishnadevaraya University with a Ph.D. He has lifetime memberships in a number of groups and organizations, including IAENG, IEEE, CSI, and ISTE. In addition to writing five textbooks, he has 32 papers in national and international conferences and 98 papers in peer-reviewed international journals. He has guided 14 M.Tech. Scholars, 8 Masters and 60 B.E students for their academic project. 11 Ph.D. Degrees awarded, currently he is guiding 6 PhD scholars at VTU.