Zhongguo Kuangye Daxue Xuebao
Journal of China University of Mining and Technology

2024 | Vol 29 | Issue 3 | Page 130-140
Journal Homepage: https://zkdx.ch/
DOI: 10.1654/zkdx.2024.29.3-10

Enhancing DDoS Detection in 5G Systems through Advanced Intrusion Detection Techniques

Umar Danjuma Maiwada*
Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak, Malaysia;
Computer Science Department, Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University Katsina, Nigeria
*Corresponding author

Kamaluddeen Usman Danyaro
Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak, Malaysia

Aliza Bt Sarlan
Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak, Malaysia

Aftab Alam Janisar
Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak, Malaysia

Khairul Shafee B Kalid
Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak, Malaysia

Anas A. Salameh
Department of Management Information Systems, College Of Business Administration, Prince Sattam Bin Abdulaziz University, Saudi Arabia

Abdullah AlAbdulatif
Department of Computer, College of Science and Arts in Al-Rass, Qassim University, Al-Rass Saudi" for Abdullah AlAbdulatif ,Saudi Arabia

Inam Ullah Khan
Department of Electonic Engineering School of Engineering and Applied Science (SEAS,) Isra University, Islamabad Campus, Pakistan

Abstract

As 5G technology continues to advance, it brings unprecedented opportunities for high-speed connectivity and data transfer. However, the proliferation of 5G also opens new avenues for cyber threats, including Distributed Denial of Service (DDoS) attacks. With the advent of 5G technology, the potential for faster and more efficient communication is undeniable. However, this progress also brings about new challenges, particularly in the realm of security. One of the major threats faced by 5G systems is Distributed Denial of Service (DDoS) attacks, which can cripple network performance and compromise user experience. This paper explores the application of advanced intrusion detection techniques for the detection and mitigation of DDoS attacks in 5G systems. The study investigates the unique characteristics of 5G networks, such as increased bandwidth, low latency, and massive device connectivity, and proposes innovative solutions to enhance DDoS detection capabilities. The research aims to contribute to the development of robust security measures, ensuring the resilience of 5G networks against evolving cyber threats. DDoS attacks can overwhelm network resources and disrupt services, making them a significant concern in 5G systems. This paper presents a comprehensive exploration of DDoS detection techniques within the context of 5G systems, with a specific focus on leveraging Intrusion Detection Techniques (IDS). We delve into the unique challenges posed by 5G networks, such as their increased complexity, massive data flows, and low-latency requirements, and how these challenges impact DDoS detection. Our research examines various IDS methods, including signature-based, anomaly-based, and machine learning-based approaches, to assess their suitability for 5G DDoS detection. Furthermore, we propose novel strategies and enhancements tailored to 5G environments to improve the accuracy and efficiency of DDoS detection. These strategies encompass real-time traffic analysis, behavior profiling, and adaptive response mechanisms. Through empirical experiments and simulations, we evaluate the performance of these techniques in detecting and mitigating DDoS attacks in 5G systems. We assess their effectiveness in terms of detection accuracy, false-positive rates, and resource utilization. In conclusion, this research contributes valuable insights into the challenges and solutions related to DDoS detection in 5G systems using Intrusion Detection Techniques. By addressing these challenges, we aim to enhance the security and resilience of 5G networks, ensuring their continued reliability in the face of evolving cyber threats.

Keywords

Intrusion Detection, Botnet, Amplification, DDoS

1. Introduction

The Internet of Things (IoT) is growing and influencing every aspect of our life, including education, home, vehicles, and healthcare [1]. As the number of connected devices grows, various issues for IoT technologies emerge: heterogeneity, scalability, quality of service, security requirements, and many more [2]. In the case of IoT, security is critical in order to maintain consumer trust. Security requirements are perceived as constraints on functional requirements [3, 4]. Finding and correcting a software problem after delivery costs 100 times higher than during requirements and design [5] [6]. Software development teams can address security risks early by implementing security principles throughout the software development lifecycle [7]. One of the primary reasons for the success of the attacks is a lack of attention to the security requirements [7] . Security requirements, cannot be neglected any longer [8]. The increasing amount of software security threats, along with increased security awareness, implies that software security requirements are no longer an option, but rather a requirement [9]. In traditional information systems, security implies unauthorised people cannot reveal, alter, exploit, or harm personal, sensitive, and valuable data [10]. DDoS attacks have targeted industry-leading service providers like Amazon Web Services. Krebs On Security, Cloudflare, Amazon Web Services, and other DDoS attack victims provide security against such attacks [11]. During a Denial of Service (DoS) attack, the attacker attempts to interrupt the target's services by consuming its resources with false requests. Distributed Denial of Service (DDoS) is a DoS attack that is magnified. Multiple sources launch requests during a DDoS attack. As a result, it becomes difficult to mitigate DDoS attacks [2].

A Distributed Denial of Service (DDoS) attack is a type of cyber-attack where multiple compromised devices are used to flood a target system or website with an excessive amount of traffic, making it unavailable to its intended users. The goal of a DDoS attack is to disrupt the normal functioning of a website or network, and the distributed nature of the attack makes it difficult to defend against. DDoS attacks work by overwhelming a target system with an excessive amount of traffic from multiple sources, resulting in the system being unable to handle the volume of incoming requests and becoming unavailable to its intended users [12]. This is accomplished in several ways: Botnets: A botnet is a network of compromised devices (bots) that can be controlled remotely to launch a coordinated attack. Amplification attacks: This involves exploiting vulnerabilities in network protocols to amplify the size of the traffic being sent to the target system. Flooding: This involves overwhelming the target system with a high volume of traffic from multiple sources, such as sending large amounts of data or requests to the target system [13]. Application layer attacks: This type of attack targets the application layer, for example by sending malformed requests to a web application that consumes large amounts of server resources. The attacker will usually use a combination of these techniques to achieve maximum impact and make the target system unavailable. In a DDoS attack, the attacker uses the combined traffic from multiple sources to overwhelm the target system, making it unavailable to its intended users [14].

DDoS attack works by overwhelming the target system with a huge amount of traffic from multiple sources. The attack is launched using a network of infected computers, also known as "bots", "zombies", or "botnets". The attacker infects these devices with malware, giving them the ability to remotely control the devices and use them to launch the attack. During the attack, the attacker commands the infected devices to send large amounts of traffic simultaneously to the target system, causing it to become overwhelmed and unable to process legitimate requests. The results in the target system is becoming unavailable or slower to its intended users. The use of multiple infected devices makes it difficult for the target system to defend itself, as the attack is coming from multiple directions at once [15]. This makes DDoS attacks a significant threat to organizations and websites, as they can cause widespread disruption and result in significant financial losses. Intrusion Detection is a security technique used to detect unauthorized access, misuse, or malicious behavior within a computer system or network. The goal of Intrusion Detection is to identify and alert administrators of security threats in real-time, allowing them to respond and prevent further damage. Intrusion Detection can be achieved through various techniques, including Signature-based detection: This technique uses a database of known attack patterns or signatures to identify, and alert known threats. Anomaly-based detection: This technique identifies behavior that deviates from normal patterns and raises an alert if it detects an abnormal event. Behavior-based detection: This technique uses machine learning algorithms to model normal system behavior and raise an alert if it detects a deviation from that behavior [16]. Intrusion Detection is an important aspect of a comprehensive security strategy, as it helps organizations detect and respond to security incidents in a timely manner. However, it is not a replacement for other security measures such as firewalls, encryption, and access controls, and should be used in conjunction with other security measures. The paper is organized as Introduction, literature review, methodology and Result of findings.

2. Literature Review

The number of Internet of Things (IoT) devices is expanding, and a lack of security in these devices has turned IoT devices into a breeding ground for malicious actions [17].

A. Security

In the context of computers and software, security has come to mean a way of thinking about protecting the system's critical assets, such as information, the operating system, networking, and programs. Defense, detection, and deterrence are the three methods of security implementation [18]. Donning a black hat and thinking like a bad guy is the most effective way to incorporate security into software development [19]. However, most software companies choose to use existing security standards as a guideline to secure their system. To aid in information security management, various security standards are used. COBIT, ISO 27001 and 27002, National Institute of Standards and Technology (NIST), and common criteria are the most widely discussed security standards in published studies because they were created by well-known organizations and drew the attention of more security practitioners than the others [18] [20].
The formula is: risk (MI) = (threat x vulnerability x probability of occurrence x impact)/controls in place.

$$\mathbf{M\times I:\ Y_i = \acute{Y}_{\boldsymbol{i}} + \hat{E}_i} \qquad \mathbf{(1)}$$

$$\mathbf{\acute{Y}_{\boldsymbol{i}} = \beta_0 + \beta_1 \times X_i} \qquad \mathbf{(2)}$$

where: Y is dependent variable, X is independent/predictor variable, β0 is intercept, β1 is slope, MI is risk and Ê is the possible threat.

Table 1 Comparison of existing security standards

The Standard	Objective
common standards	Guarantee of information technology security
ISO 17799:2005	Procedure safety Physical, human-related, and digital privacy, as well as asset and compliance
ISO 27001, 27k	prerequisites for information security management
COBIT 2019	Enterprise information and technology regulation and competitiveness

B. Security Requirements (SR)

In the published studies, SR is a limitation on the system's functionalities that aim to satisfy one or more security requirements [21], [22], [23]. As a constraint, SR will specify urgent remarks or constraints concerning significant security risks to the functional requirements. A functional requirement can indicate that a user must enter their username and password to log in to the system. SR then guarantees that the system validates this information before granting the user access to the system [3].

Since the early days of software development, software security has been a neglected issue. However, this does not indicate that the issues have never been mentioned; rather, it was misinterpreted, taken lightly, misread, and not handled properly. Software security is an important element that must be addressed throughout the software development life cycle [24]. In general, security is regarded as a non-functional requirement, and as such, security tests are typically performed at the end of the Software Development Life Cycle (SDLC) [25], [26], [3]. This suggests that software security requires attention even at the early stages of development [25], [27], [26].

As discussed by the concepts and uses of 5G as well as the security risks involved and have contrasted various cellular technology generations. As 5G delivers Internet Protocol (IP)-based solutions, the authors claim that it will be susceptible to spooling, eavesdropping, masquerade, and phishing assaults. The architecture, modulation methods, multiple access strategies, Energy Efficiency approaches, and protocol stack of the technologies proposed to enable 5G. They have also demonstrated a variety of efforts made in the direction of 5G development [28].

They have provided a summary of the security and privacy issues with 5G. The authors have examined the numerous security issues in the cloud, Software Defined Networking (SDN), and Network Function Virtualization (NFM) approaches with 5G. These concepts allow organizations and users to gain additional benefits through good network management and efficient data services. DDoS is a major security concern in all three models, according to their research, which is conclusive (cloud, SDN, NFV). They have put out ideas for enhancing security in 5G technology [29].

They developed a proactive isolation strategy to combat these assaults in 5G network equipment slices to mitigate attacks like DDoS, which have a significant negative impact on the network. The scalability needs underpinning IoT systems which were not evaluated in this work, even though this isolation mechanism is acceptable for inter- and intraslices. They introduced a new system model for automotive networks that addresses privacy and security concerns for real-time video reporting to ensure network security in 5G vehicle networks. The suggested cryptographic security paradigm seeks to minimize overheads while maintaining privacy for device-to-device connections [30].

However, rather than serving as a modelling tool for IoT systems in a 5G context, the model is focused on a vehicular context. IoT devices will be able to converse and share data more quickly than ever with 5G networks. However, this development is probably going to make the systems more susceptible to security risks, such as those posed by malicious nodes. Researchers have presented novel 5G network-compatible solutions to several of the security challenges. For instance, they suggested an effective access control system that addresses the issue of a single feature bottleneck to prevent unwanted action within the network [31].

DDoS has been listed for SDN and the cloud. Our paper stands out from the crowd because it covers a variety of topics related to DDoS in the 5G network, including legal issues, commercial solutions, anomaly-based detection, an analysis of Intrusion Detection techniques, and an evaluation of statistical, machine learning, and hybrid approaches. A review of SDN's DDoS prevention and mitigation methods which was covered by SDN architecture, several DDoS attack types in SDN, and SDN security problems are detected. Based on the type of detection method and metric employed, it offered DDoS detection techniques. They have not talked about the legal implications, business solutions, taxonomy of DDoS attacks, or methods of detection [32].

By 2024, there will be 17 million DDoS attacks, with the typical DDoS attack size reaching 1 Gbps. Since it takes a lot of resources to produce efficient attacks, there were not many huge points to point service (PPS) attacks in prior years. The prevalence of IoT devices, the majority of which are unsecured, has led to an increase in high intensity attacks. Multivector attacks using botnets notably Mirai, Brickerbot, Reaper, and so on are becoming more common. It is challenging to detect and mitigate these threats since they change over time. Attackers are using more potent botnets made up of embedded, IoT, and cloud servers that have been misused [33].

3. Methodology

The methodology used in Intrusion Detection mechanisms to detect DDoS attacks in this paper include:
Traffic Volume Analysis which is the method that detects a DDoS attack by monitoring the volume of incoming traffic and raising an alert if it exceeds a certain threshold.

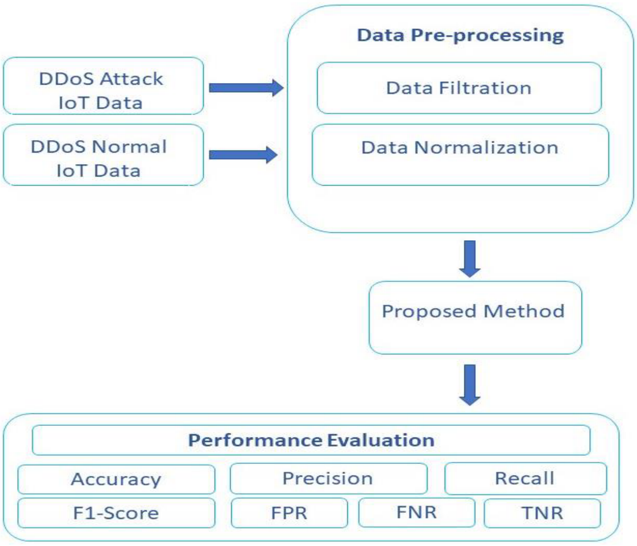

Fig. 1 Methodology Flow

4. Hypothesis

When applying DDoS detection using Intrusion Detection techniques in 5G systems, the hypothesis we focused on was various aspects of improving the Energy Efficiency. Intrusion Detection techniques can effectively detect and mitigate DDoS attacks in 5G systems, reducing the impact on network availability. The use of network slicing in 5G systems enhances the accuracy of Intrusion Detection for DDoS attacks, allowing for more precise identification and mitigation. IoT devices in 5G networks are susceptible to compromise and can be exploited in DDoS attacks, and Intrusion Detection is crucial for protecting these devices and improving Energy Efficiency. Intrusion Detection techniques can provide real-time DDoS detection in low latency 5G networks, ensuring minimal disruption to critical applications. Machine learning algorithms can significantly improve the accuracy of Intrusion Detection for DDoS attacks in 5G systems, enabling faster and more effective response. Intrusion Detection solutions designed for 5G networks can effectively scale to accommodate the increasing volume of devices and traffic, maintaining detection accuracy. Intrusion Detection techniques optimized for 5G systems can effectively detect DDoS attacks while minimizing resource consumption, ensuring efficient network operation. Intrusion Detection systems that adapt to the dynamic nature of 5G networks can consistently identify and mitigate evolving DDoS attack techniques. Incorporating Intrusion Detection techniques in 5G networks contributes to compliance with cybersecurity regulations and legal requirements related to DDoS protection. A comparative study of different Intrusion Detection methods in 5G networks will reveal variations in their effectiveness, leading to the identification of optimal techniques. We take note that our hypothesis is specific, measurable, and testable through empirical research. We chose our hypothesis based on our research objectives, the available data, and the specific aspects of DDoS detection in 5G systems that we aim to investigate i.e the network aspect.

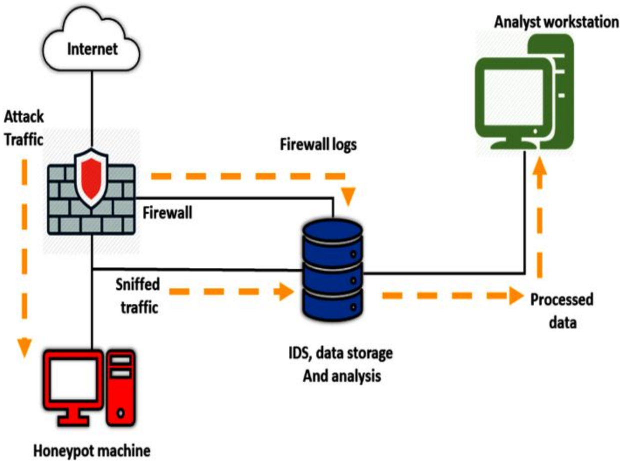

Fig. 2 Intrusion Detection process

Also, Pattern Recognition is a method that uses algorithms to identify patterns in incoming traffic, such as many requests coming from the same IP address and raises an alert if it detects a pattern associated with a DDoS attack.

Statistical Analysis uses statistical models to identify unusual behavior in incoming traffic, such as many requests in a short period of time and raises an alert if it detects an abnormality.

Flow-based Analysis analyzes real-time network traffic analysis to locate and track the flow of data and detect DDoS attacks by looking for unusual traffic patterns. It is important to note that no single method is foolproof, and a combination of methods is often used to achieve the best results. Additionally, it is important to regularly update Intrusion Detection systems to account for new and evolving DDoS attack techniques.

Traffic Volume Analysis is used in Intrusion Detection mechanisms to detect DDoS attacks. In this method, the system monitors the volume of incoming traffic to a target system or network and raises an alert if it exceeds a certain threshold. Here is how it works: The system sets a threshold value for incoming traffic based on normal levels of traffic. The system monitors incoming traffic and tracks the volume of incoming requests. If the volume of incoming traffic exceeds the threshold value, the system raises an alert and starts further analysis to determine if a DDoS attack is underway. If the further analysis confirms a DDoS attack, the system can take defensive measures to mitigate the attack, such as rate limiting incoming traffic or redirecting traffic to a separate server. Traffic Volume Analysis is a simple and effective method for detecting DDoS attacks, as the attack can be easily detected by the sudden increase in incoming traffic. However, it may not be efficient for identifying more advanced DDoS attacks that employ strategies like slow-rate attacks or application-level attacks. In these cases, additional methods such as pattern recognition or statistical analysis may be necessary.

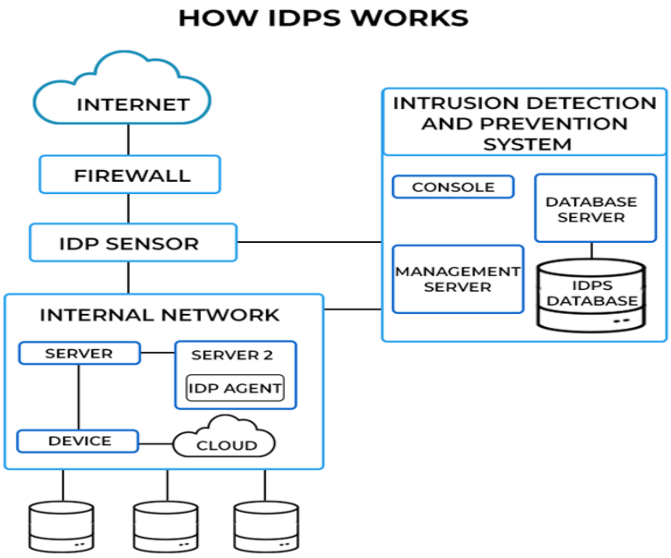

Fig. 3 How Intrusion Detection works

5. Results

The result of traffic volume analysis applied to identify DDoS attacks in an Intrusion Detection system is the identification and alerting of a potential DDoS attack. The following are the outcomes: Detect an increase in incoming traffic: The system will detect an increase in incoming traffic beyond a predetermined threshold, which indicates a DDoS attack. Raise an alert: A DDoS attack is detected, the system raises an alert, notifying the administrators of the attack. Confirm the attack: The system performs further analysis to confirm the attack and determine the type of attack and its severity. Take defensive measures: A DDoS attack is confirmed, the system takes defensive measures by limiting incoming traffic, redirecting traffic to a separate server, or filtering out malicious traffic, to mitigate the attack.

By detecting a DDoS attack and taking defensive measures, the system prevents the attack from disrupting the normal functioning of the targeted system and ensures its availability to its intended users. Traffic volume analysis is an effective method for detecting DDoS attacks, but it should be used in conjunction with other methods, such as pattern recognition and statistical analysis, for a comprehensive approach to Intrusion Detection as used in this paper.

Were, Total $_{\text{attack}}$ -Probability of total attack.
p^{FPR} -Probability of false positive rate, p^{FNR-} Probability of false negative rate.

$$\mathbf{Total_{attack}= 1-(1-p^{FPR})\,(1-p^{FNR})} \qquad (3)$$

C-Number of channels

$$\mathbf{p^{FPR}\alpha\frac{1}{C}} \qquad (4)$$

σ-packet size

T_{BA}- Inter-arrival rate

$$\mathbf{p^{FPR}\ \alpha\ \sigma\ \alpha\ \frac{1}{T_{BA}}} \qquad (5)$$

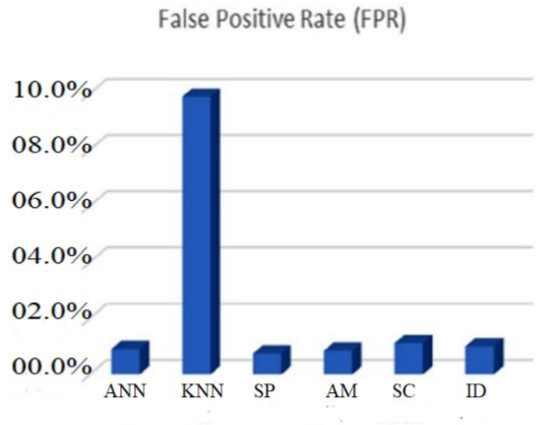

Fig. 4 percentage rate (FPR) of ID in different methods

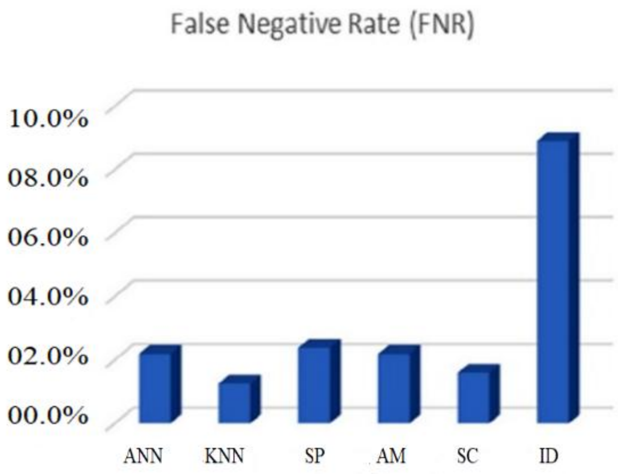

Fig. 5 percentage rate (FNR) of ID in different methods

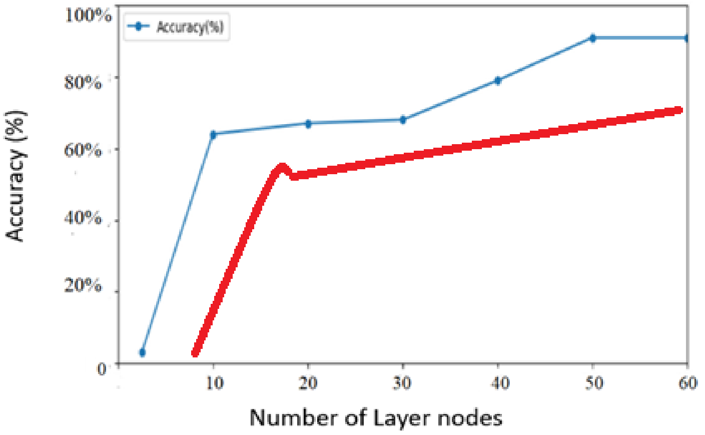

Fig. 6 Accuracy of ID technique in detecting DDoS attack.

To take advantage of their complementing strengths, several DDoS detection systems incorporate numerous Intrusion Detection algorithms. By combining both signature-based and anomaly-based techniques, hybrid systems can improve detection accuracy. These systems can lessen the drawbacks of individual approaches and offer a more effective defence against DDoS attacks by combining the benefits of many detection techniques.

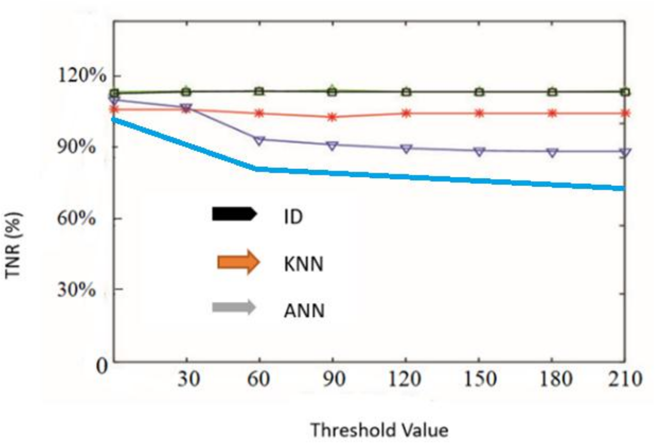

Fig. 7 Comparison of ID technique with other methods in DDoS attack

To detect DDoS assaults, traffic analysis tools keep an eye on network traffic at many layers, including the network, transport, and application layers. This method involves looking at packet headers, payload information, or flow traits. Traffic analysis tools can spot unusual traffic patterns, high traffic volumes, or anomalies in packet headers that might point to a DDoS attack by examining traffic behaviour. This information aids in separating harmful from normal communications.

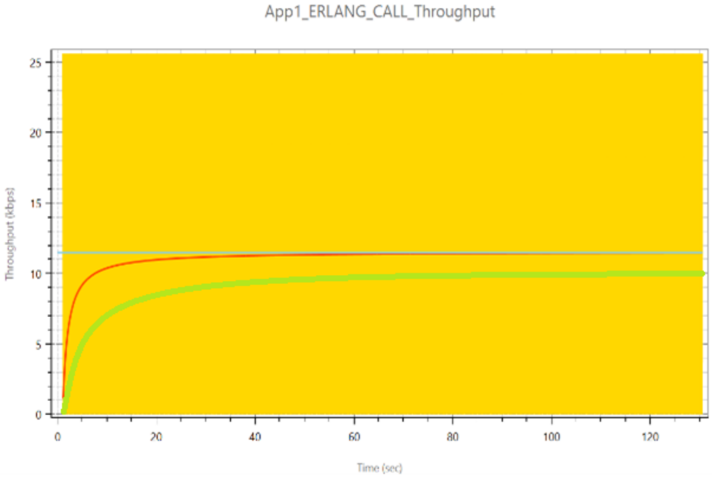

Fig. 8 Throughput vs Time series

6. Discussion

Techniques for identifying and reducing DDoS assaults are extremely important. Network managers can efficiently recognize and respond to DDoS attacks by combining anomaly detection, signature-based detection, traffic analysis, behavior-based detection, or hybrid approaches. The effectiveness of DDoS detection systems is continuously being improved by ongoing research and advancements in Intrusion Detection technologies, enabling more effective protection for networks and online services. However, challenges like scalability, false positives, evolving attack techniques, and resource requirements still exist. To process and analyze network traffic, Intrusion Detection systems may require significant processing and storage capacity. This can be difficult, especially in contexts with limited resources or on fast networks where real-time processing is crucial. Attackers constantly develop new attack vectors and evasion strategies, which leads to a continuous evolution of DDoS attacks. To properly identify new attack patterns, Intrusion Detection systems must be updated and adaptive. False positives from Intrusion Detection systems might mark innocent traffic as harmful. False positives might cause unneeded alarm triggers and impair the usability of the system. Effective DDoS detection systems must strike a compromise between minimizing false positives and accurate detection. DDoS assaults have the potential to produce a significant amount of network traffic, which makes it difficult to process and analyze data in real time. Scalable Intrusion Detection systems can manage high-speed networks and heavy traffic flows without causing noticeable delays.

7. Conclusion

Security is a must have feature in today’s software. To avoid the security issue in the later stage of SDLC it must be tackled in the requirement stage. It helps to identify the security risk and threats; still security requirements need to be handled effectively in cyber systems to overcome the security risks in software development. DDoS (Distributed Denial of Service) attacks are among the most frequent categories of cyberattacks that can be very detrimental to businesses, organizations, and individuals. Intrusion Detection is a technique used to detect and prevent such attacks. Here are the steps you can take to deal with DDoS using Intrusion Detection technique: Install an Intrusion Detection system (IDS): An IDS is a piece of software that scans network traffic for anomalies of suspicious behavior. It can help identify DDoS assaults with analysis of the Network function and pattern recognition that match those of DDoS attacks. Configure the IDS: Configure the IDS to detect DDoS attacks. This can be done by defining the types of DDoS attacks that the IDS should look for and setting thresholds for detecting abnormal traffic. Monitor network traffic: Monitor network traffic continuously to detect any abnormal activity.

The IDs will analyze the traffic to identify any signs of a DDoS attack. Generate alerts: Set up the IDS to generate alerts when it detects a DDoS attack. The alerts can be sent to network administrators or other security personnel, who can take immediate action to mitigate the attack. Mitigate the attack: Once a DDoS attack is detected, take steps to handle the attack. This can include preventing traffic from the source of the attack, filtering traffic based on certain characteristics, or even shutting down the affected service. Review and update security policies: Finally, review and update your security policies to ensure that your systems are protected against future DDoS attacks. This may include implementing additional security measures, such as firewalls, load balancers, and content delivery networks. In summary, to deal with DDoS attacks using Intrusion Detection techniques, you need to install an upto date IDs, configure it, monitor network traffic, generate alerts, mitigate the attack, and review and update your security policies. ID was very low in percentage rate of false positive rate while high in percentage rate of false negative rate because of the accuracy it provides as seen in figure 5. As the number of nodes increases so does the accuracy increases, that is why it is more accurate than other methods.

8. Contribution

DDoS (Distributed Denial of Service) detection using intrusion detection techniques in 5G systems is significant and can have a profound impact in improving Energy Efficiency on the security and reliability of 5G networks. DDoS attacks are a major threat to 5G networks due to their high bandwidth capabilities/speed. Implementing intrusion detection techniques specifically tailored for 5G can provide a robust layer of security, helping to identify and mitigate DDoS attacks in real-time systems. Intrusion detection techniques can provide rapid detection of DDoS attacks as they unfold. This early detection is crucial in 5G networks, where low latency and real-time communication are essential for applications like autonomous vehicles, pipelines and remote surgery. DDoS attacks can disrupt 5G services, causing downtime and financial losses. By quickly identifying and mitigating attacks, intrusion detection can minimize service interruptions, ensuring a more reliable network and improve Energy Efficiency. Intrusion detection can help 5G networks dynamically allocate resources in response to DDoS attacks. This ensures that network resources are efficiently used, even under attack conditions, which is vital for maintaining the quality of service. 5G networks support massive IoT deployments. Intrusion detection can safeguard IoT devices from being compromised and used as part of botnets in DDoS attacks. Protecting the integrity of IoT devices is crucial for maintaining network security. DDoS attacks can be used as a diversion tactic to breach network security and steal sensitive data. Intrusion detection helps in thwarting such attacks, thus contributing to data privacy and integrity in 5G systems. 5G networks are highly dynamic, with network slicing and edge computing. Intrusion detection can adapt to these dynamic environments, ensuring that security measures remain effective as the network evolves. Compliance with cybersecurity regulations is essential for 5G networks. Intrusion detection can assist in meeting regulatory requirements and demonstrating a commitment to cybersecurity, which is crucial for maintaining public trust. Intrusion detection can provide insights into the evolving tactics and techniques used in DDoS attacks targeting 5G networks. This information can be valuable for security professionals and researchers, helping to develop more effective countermeasures. As 5G evolves and paves the way for future generations of wireless networks, the knowledge gained from DDoS detection research can contribute to the development of even more secure and resilient network infrastructures. DDoS detection using intrusion detection techniques in 5G systems is crucial for safeguarding the integrity, availability, and security of these advanced networks. It helps ensure that 5G can deliver on its promises of low latency, high bandwidth, and connectivity for a wide range of applications while protecting against the growing threat of DDoS attacks.

Acknowledgement

The authors wish to acknowledge Universiti Teknologi PETRONAS and Prince Sattam bin Abdulaziz University. This study is supported via funding from Prince Sattam in Abdulaziz University project number (PSAU/2023/R/1445)" because the funding was made by the above funder.

Conflict Of Interest

There is no conflict of interest between the authors and with the submission of this manuscript.

References

1. Anthi, E., et al., *A Supervised Intrusion Detection System for Smart Home IoT Devices*. IEEE Internet of Things Journal, 2019. **6**(5): p. 9042-9053.
2. Mishra, N. and S. Pandya, *Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review*. IEEE Access, 2021. **9**: p. 59353-59377.
3. Mufti, Y., et al., *A Readiness Model for Security Requirements Engineering*. IEEE Access, 2018. **6**: p. 28611-28631.
4. Villamizar, H., et al., *A Systematic Mapping Study on Security in Agile Requirements Engineering*, in *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. 2018. p. 454-461.
5. MUSTAFA, N., et al., *SECURITY REQUIREMENTS TEMPLATE-BASED APPROACH TO IMPROVE THE WRITING OF COMPLETE SECURITY REQUIREMENTS*. Journal of Theoretical and Applied Information Technology, 2021. **99**(01).
6. Lal, B. and C.R. Chavan, *Analysis Report on Attacks and Defence Modeling Approach to Cyber Security*. International Journal of Scientific Research in Science and Technology, 2019: p. 52-60.
7. Anderson, R., *Security engineering: a guide to building dependable distributed systems*. 2020: John Wiley & Sons.
8. Rehman, S.u., C. Allgaier, and V. Gruhn, *Security Requirements Engineering: A Framework for Cyber-Physical Systems*, in *2018 International Conference on Frontiers of Information Technology (FIT)*. 2018. p. 315-320.
9. Khan, R.A. and S.U. Khan. *A preliminary structure of software security assurance model*. in *Proceedings of the 13th International Conference on Global Software Engineering*. 2018.
10. Hu, Y., et al., *A survey of intrusion detection on industrial control systems*. International Journal of Distributed Sensor Networks, 2018. **14**(8).
11. Nicholson, P., *Five most famous DDoS attacks and then some*. A10 Networks. Source: https://www. a10networks. com/blog/5-most-famous-ddos-attacks/[accessed 3rd February 2021], 2020.
12. Sharafaldin, I., et al. *Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy*. in *2019 International Carnahan Conference on Security Technology (ICCST)*. 2019. IEEE.
13. Zeebaree, S.R., K. Jacksi, and R.R. Zebari, *Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers*. Indones. J. Electr. Eng. Comput. Sci, 2020. **19**(1): p. 510-517.
14. Sreeram, I. and V.P.K. Vuppala, *HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm*. Applied computing and informatics, 2019. **15**(1): p. 59-66.
15. Tuan, T.A., et al., *Performance evaluation of Botnet DDoS attack detection using machine learning*. Evolutionary Intelligence, 2020. **13**: p. 283-294.
16. Poongodi, M., et al., *Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics*. IEEE Access, 2019. **7**: p. 158481-158491.
17. Angrishi, K., *Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets*. arXiv preprint arXiv:1702.03681, 2017.
18. Rhodes-Ousley, M., *Information security the complete reference*. 2013: McGraw Hill Professional.
19. Mcgraw, G., *Software Security: Building Security In, ser*. 2006, Addison-Wesley Software Security Series. Addison-Wesley.

20. Zareen, S., A. Akram, and S. Ahmad Khan, *Security Requirements Engineering Framework with BPMN 2.0.2 Extension Model for Development of Information Systems.* Applied Sciences, 2020. **10**(14).
21. El-Hadary, H. and S. El-Kassas, *Capturing security requirements for software systems.* J Adv Res, 2014. **5**(4): p. 463-72.
22. Haley, C.B., *Arguing security: a framework for analyzing security requirements*. 2007, The Open University.
23. Salini, P. and S. Kanmani, *Survey and analysis on Security Requirements Engineering.* Computers & Electrical Engineering, 2012. **38**(6): p. 1785-1797.
24. Khan, R.A. and S.U. Khan, *A preliminary structure of software security assurance model*, in *Proceedings of the 13th International Conference on Global Software Engineering*. 2018. p. 137-140.
25. Sharma, A. and P.K. Misra, *Aspects of enhancing security in software development life cycle.* Advances in Computational Sciences and Technology, 2017. **10**(2): p. 203-210.
26. Karim, N.S.A., et al., *The practice of secure software development in SDLC: an investigation through existing model and a case study.* Security and Communication Networks, 2016. **9**(18): p. 5333-5345.
27. Lee, Y. and G. Lee, *HW-CDI: Hard-wired control data integrity.* IEEE Access, 2019. **7**: p. 10811-10822.
28. Hussain, B., et al., *Deep learning-based DDoS-attack detection for cyber–physical system over 5G network.* IEEE Transactions on Industrial Informatics, 2020. **17**(2): p. 860-870.
29. Rezvy, S., et al. *An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks*. in *2019 53rd Annual Conference on information sciences and systems (CISS)*. 2019. IEEE.
30. Alladi, T., et al., *Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles.* IEEE Wireless Communications, 2021. **28**(3): p. 144-149.
31. Chettri, L. and R. Bera, *A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems.* IEEE Internet of Things Journal, 2019. **7**(1): p. 16-32.
32. Dong, S., K. Abbas, and R. Jain, *A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments.* IEEE Access, 2019. **7**: p. 80813-80828.
33. Gurusamy, D., et al., *DDoS risk in 5G enabled IoT and solutions.* International Journal of Engineering and Advanced Technology, 2019. **8**(5): p. 1574-1578.

Authors

UMAR DANJUMA MAIWADA *received Bsc. Computer Science from Bayero University Kano. Msc Computer Science Jodhpur National University, India. Persuing PhD at Universiti teknologi PETRONAS (UTP) in CIS dept. currently working at Umaru Musa Yaradua University Katsina as Lecturer I. His research interests include Computer Networking, Programming with c++, Data Science, Communication, Digital Twin's Network and IoT.*

KAMALUDDEEN USMAN DANYARO *is a lecturer at the Computer and Information Science Department, Universiti Teknologi PETRONAS. He received his Ph.D. from Universiti Teknologi PETRONAS, Malaysia. He obtained his M.Sc. in Business IT from Northumbria University, UK. He also received his B.Sc. in Mathematical Science from Bayero University, Kano. His research interests include Computer Networking, Blockchain, Data Science, Semantic Web and Web Intelligence. Ts. Dr. Kamaluddeen is a researcher with the Center of Data Science (CeRDaS). He is a reviewer in many conferences and journals.*

AFTAB ALAM JANISAR *is a Software Engineer with a demonstrated history of working in the information technology and services industry. Introduction Skills and Expertise Human-Computer Interaction Mutation Software Testing Current institution Bahria University Department of Computer and Software Engineering Islamabad, Pakistan.*

M. S. LIEW *received the B.S.C.E. and Ph.D. degrees from Texas, USA, in 1983 and 1988, respectively. Having been practicing in the offshore industry for 23 years, he is currently the Head of the Offshore Engineering Center and the Deputy Vice Chancellor of Research and Innovation, Universiti Teknologi PETRONAS, Malaysia, where he is also a Professor with the Department of Civil and Environmental Engineering. His focus is on MetOcean, the design of offshore facilities, and on the dynamic aspects of offshore facilities.,He is currently supporting several business units of PETRONAS Carigali, and other oil and gas outfits. PhD. Deputy Vice Chancellor - Research and Innovation at Universiti Teknologi PETRONAS Malaysia. Skills and expertise: Waves Dynamics Semantic Web Steel Offshore Engineering Structural Design Electrodeposition Structural Reliability subsea engineering Hydrodynamics Construction Civil Engineering Structural Engineering Membranes.*

KHAIRUL SHAFEE KALID *obtained his degree in 1998, Degree in Business Administration majoring in Computer Information System by Western Michigan University. 2002, Master in Information Technology by Queensland University of Technology. 2015, PhD in Information Technology by Universiti Teknologi PETRONAS. A senior lecturer from the Department of Computer and Information Sciences under the Faculty of Science and Information Technology, Universiti Teknologi PETRONAS. My area of expertise on knowledge management tools and it use in organizations.*

ANAS A. SALAMEH *is an associate professor at department of management information systems college of business administration Prince Sattam Abdulaziz University since 2016, and the current deputy director of the student's activity committee as well as a member of the exams scheduling committee PSAU. Hus major research area of interest focusing* *on the area such as e-commerce (m-commerce), e-business, e-marketing, technology acceptance/adoption, e-learning, e-CRM, service quality in many areas related to e-service aspects.*

ALIZA Bt SARLAN *received the Bachelor. degree in IT from Universiti Utara Malaysia in 1996, Master in IT from Queensland University, Australia in 2002 and the Ph.D degree in IT from Universiti Teknologi PETRONAS (UTP), Malaysia in 2015. Her research areas of interests include human behavior & technology adoption, information system analysis and modelling, software reliability as well as software testing. She has contributed to the areas of human factors in software development, understanding the use of technologies, and how this use can improve people's lives and their quality of life. She is now embarking into new research area of data analytics, sentiment analysis and data visualization. Dr. Aliza is currently a researcher with the Center of Data Science (CeRDaS), UTP, where she focuses in solving complex upstream oil and gas (O&G) industry from the view point computer sciences. She currently serves as the Chair of the Computer and Information Sciences Department, UTP since 2019. She is also active in conducting professional training in data analytic for public and industry. She has also bee*