IJARCCE A. ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12634

SURVEY ON NETWORK ALERT SYSTEM

Harshit Handa and Vanishree K

Department of Information Science and Engineering, R V College of Engineering, Bengaluru, Karnataka, India

Abstract: In order to identify potential threats, a network alert system often combines monitoring technologies including intrusion detection systems (IDS), firewalls, and antivirus software. A crucial tool for managing the performance, security, and availability of computer networks is a network alert system. When events or anomalies take place, it continuously monitors network traffic, devices, and services and creates alerts or notifications. The stability and integrity of networks are crucially maintained by this mechanism, especially in complex and dynamic contexts. A network alert system's capacity to give early issue detection is one of its main features. It may detect and report on potential issues including security threats, performance bottlenecks, and device failures by continually monitoring network activity.

Keywords: Network Alert ,Network Intrusion, Artificial Intelligence, Cloud, DNS Alert, DHCP Alert, Authentication Alert

1. INTRODUCTION

A network alert system is a crucial part of network administration and monitoring those aids in preserving the performance, availability, and security of computer networks. It is intended to continuously monitor network usage, hardware, and services, and to send out alerts or notifications if certain occurrences or abnormalities are found. A network alert system gives network managers immediate access to information about the health of the network and any possible problems, enabling them to take timely action to protect the integrity of the network. A network alert system's main objective is to identify and report on various kinds of network events. This comprises security risks including intrusion attempts, malware infections, and suspicious activities that can jeopardise the confidentiality, integrity, or availability of the network. The solution helps administrators to analyse and manage security issues, preventing or minimising damage to the network and its resources, by rapidly warning them of these possible hazards. A network alert system also aids in managing and monitoring network performance. Based on predefined thresholds for parameters like bandwidth usage, latency, packet loss, or device performance, it generates notifications. Administrators are able to quickly identify and fix issues while maximising network resources thanks to these alerts, which offer insightful information about performance bottlenecks, congestion difficulties, or hardware failures. Additionally, by keeping an eye on the availability and state of network servers, devices, and services, network alert systems help to preserve network availability. When devices or services experience disturbances or become unresponsive, they create alerts, allowing managers to quickly respond and troubleshoot in order to reduce downtime. By ensuring users have access to essential resources and services, the network alert system helps avoid productivity losses and customer discontent. In conclusion, a network alert system is a crucial tool for efficient network administration. It allows administrators to manage network security, optimise performance, and guarantee high availability by offering real-time monitoring, prompt alarms, and thorough visibility. A proactive step towards proactively controlling network issues and ensuring a strong and dependable network infrastructure is the implementation of a network alert system. A network alert system's main function is to offer timely alerts and real-time monitoring for network events, security threats, performance problems, and availability disturbances. In order to maintain the security, functionality, and availability of computer networks, it enables network managers to proactively identify and address any issues. The network alert system assists in preventing or minimizing downtime, mitigating security risks, maximizing network resources, and maintaining the overall integrity and effectiveness of the network infrastructure by rapidly alerting administrators of crucial occurrences.

2. NETWORK ALERT SYSTEM

A network alert system helps in monitoring and detecting potential security threats, such as network intrusions or anomalies, in real-time. It generates alerts or notifications to inform system administrators or security teams about suspicious activities, enabling them to take immediate action to mitigate risks, enhance network security, and prevent potential breaches.

In [1], an alert correlation approach for network intrusion detection systems (NIDS) is proposed in this paper. The authors design a correlation technique that discovers connections between alerts in order to alleviate the difficulty of monitoring a high number of alerts provided by NIDS. They suggest a two-step strategy that combines a correlation model and a

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12634

clustering technique. The clustering technique narrows the alert space by combining comparable alerts. The correlation model then calculates the degree of association among various clusters and produces a correlation graph. According to experimental findings, the proposed architecture enhances NIDS accuracy and effectiveness by decreasing false positives and offering a more thorough understanding of network hazards.

In [2] ,it is discussed that in order to detect intrusions, this research focuses on network traffic analysis utilising machine learning methods. The authors suggest a system that uses machine learning methods to distinguish between legitimate and malicious network data. They assess the efficiency of different machine learning techniques, such as decision trees, support vector machines, and artificial neural networks, to identify network intrusions. The experimental results show that machine learning algorithms may efficiently distinguish between legitimate network traffic and malicious traffic, increasing the precision of intrusion detection systems.

In [3], An alert fusion architecture for network security monitoring is presented in this paper. The authors provide a technique for combining numerous alarms produced by various intrusion detection systems into a single signal. The framework combines alerts using a number of techniques, including data normalisation, alert categorization, and alert correlation, to present a more thorough and precise picture of network security problems. Experimental analyses show how the suggested approach works to cut down on duplicate alarms while increasing the effectiveness and precision of network security monitoring.

In [4], This research uses graphics processing units (GPUs) to tackle the problem of real-time intrusion detection in high-speed networks. The authors suggest an intrusion detection system (IDS) that takes advantage of the GPUs' parallel processing power to accelerate and optimise network traffic analysis. The IDS uses deep packet inspection methods and machine learning algorithms to quickly identify network intrusions. According to experimental findings, the GPU-based IDS performs better in terms of processing speed and scalability than conventional CPU-based IDSs, making it appropriate for high-speed network situations.

In [5], A collaborative alert management system for network security is presented in this research. The difficulty of monitoring and prioritising a high number of alerts produced by various intrusion detection systems is addressed by the writers. In order to analyse and prioritise alerts, the suggested system uses a collaborative approach in which various security appliances and IDSs communicate and exchange alert data. Techniques like alert aggregation and trust evaluation are used by the system.

In [6], To detect network intrusions, a distributed anomaly detection system is introduced in this paper. To find anomalies in network traffic, the authors suggest a cooperative strategy in which several intrusion detection nodes cooperate. Every node gathers data on the local network traffic, employs algorithms for anomaly detection, and communicates its results to nearby nodes. To combine the data and decide on probable incursions, the distributed system uses a consensus-based technique. Experimental assessments show that the suggested method is efficient and scalable at identifying network intrusions.

In [7], This study focuses on software-defined networks (SDNs) traffic anomaly detection using machine learning approaches. The authors suggest a system that gathers and examines network traffic data by utilising SDN capabilities. To find anomalies in network traffic patterns, they use machine learning algorithms like support vector machines and k-nearest neighbours. To spot unusual behaviour, the system keeps an eye on a number of network indicators, including packet loss, latency, and throughput. The effectiveness of the suggested approach in identifying traffic anomalies and enhancing network security in SDN systems is supported by experimental results.

In [8], The difficulty of alert correlation in network intrusion detection systems (NIDS) is discussed in this research. The authors suggest effective warning correlation techniques with the goal of lowering false positives and enhancing intrusion detection precision. The algorithms take into account the timestamps and source IP addresses of each alert as well as the spatial and temporal relationships between them. The suggested method groups alerts that are similar using clustering algorithms and determines the correlation between clusters. Experimental analyses show how the algorithms can improve the precision and effectiveness of NIDS.

In [9], This study offers a unique intrusion detection system (IDS) based on network traffic analysis that is specifically made for identifying advanced persistent threats (APTs). Traffic analysis, anomaly detection, and signature-based detection methods are all included in the authors' multi-stage detection strategy. In order to find abnormalities and detect potential attacks, the system examines network traffic patterns, spots anomalies, and compares traffic with known APT signatures. The suggested IDS focuses on finding APTs that act stealthily and persistently, frequently eluding

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12634

conventional security procedures. The system is effective in identifying APTs and enhancing network security, according to experimental results.

In [10], This study discusses data stream mining approaches for real-time network intrusion detection. The approach the authors suggest uses machine learning algorithms to analyse real-time network traffic data and identify intrusions. To manage the constant and fast-moving nature of network traffic, the system makes use of data stream mining techniques. As fresh data come in, the intrusion detection model is updated and modified using incremental learning methods. Experimental assessments show the effectiveness.

3. DIFFERENT ALERTS AND FAILURES

DNS Alert: When there is a probable problem or failure with the Domain Name System (DNS), a DNS alert is set off. In order to enable device communication over the internet, the DNS converts domain names into IP addresses. A DNS alert may signal difficulties including unavailable DNS servers, contaminated DNS caches, incorrect DNS settings, or DNS-related network connectivity problems. Monitoring DNS alerts allows administrators to swiftly find and fix DNS-related issues, assuring uninterrupted network service and proper domain name resolution.

DHCP Alert: When there are problems with the Dynamic Host Configuration Protocol (DHCP) service, DHCP alerts are generated. Along with other aspects of network design, DHCP is in charge of allocating IP addresses to devices on a network. DHCP alerts can be a sign of issues such as IP address conflicts, depleted address pools, DHCP server failures, or incorrect DHCP settings. Administrators may quickly resolve these problems by keeping an eye on DHCP notifications, ensuring that devices can get legitimate network settings and keep communication inside the network.

Authentication Alert: When the authentication process fails or exhibits an anomaly, an alert is generated for authentication. Verifying the identity of persons or devices trying to access a network or system is the process of authentication. Unusual authentication patterns expired or invalid credentials, failed login attempts, or potential unauthorized access attempts can all be indicated via an authentication alert. Administrators can see unusual activity, potential security lapses, or attempts to compromise accounts by watching authentication alerts. Investigating and resolving these problems quickly will improve network security overall and safeguard sensitive resources.

Association Alert: When there are issues with the connection between wireless devices and access points in a Wi-Fi network, an association warning is produced. A device and an access point connect through the association procedure, enabling the device to access the network. A failed association, a weak signal, interference, or incorrectly configured access points may all be indicated by an association alert. Administrators can spot connectivity difficulties, solve issues, and guarantee steady, dependable connections between devices and access points by keeping an eye on association notifications. The Wi-Fi network's overall performance and user experience are enhanced as a result.

Captive Portal Alert: When there are problems with the captive portal authentication mechanisms, a captive portal warning is generated. A captive portal is a device that's frequently used in public Wi-Fi networks and that makes it necessary for users to authenticate themselves or accept terms and conditions before being able to access the internet. An alert for the captive portal server could be generated if there are issues with its availability or functionality, problems with user authentication, efforts to circumvent the captive portal, or incorrect configuration of the captive portal settings. Administrators can ensure the effective operation of the authentication system, restrict unauthorized access to the network, and maintain adherence to usage policies by monitoring captive portal notifications. In public Wi-Fi environments, promptly responding to captive portal notifications aids in offering a seamless and secure user experience.

WPA Handshake Alert: When there are issues or anomalies with the Wi-Fi Protected Access (WPA) handshake procedure, a WPA handshake alert is generated. When a wireless device makes an attempt to join to a Wi-Fi network protected by WPA encryption, the WPA handshake is a security process that takes place. A WPA handshake warning may be generated in response to repeated handshake attempts, atypical handshakes, or unsuccessful or incomplete handshakes. These notifications may indicate Wi-Fi network vulnerabilities or unauthorised access attempts. Administrators can see security problems, catch unauthorised devices trying to join, and take the necessary precautions to reduce risks by keeping an eye on WPA handshake alarms. This guards against unauthorised access and any data breaches and helps preserve the wireless network's integrity and secrecy.

MAC Authentication Alert: When MAC-based authentication procedures fail or exhibit irregularities, a MAC authentication alert is produced. By authenticating devices based on their distinctive Media Access Control addresses, MAC authentication is a technique for restricting network access. A MAC authentication alert could mean that there have

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12634

been attempts to spoof the MAC address, authentication failures, or incorrectly configured MAC authentication settings. Administrators can identify and stop unauthorised devices from connecting to the network by keeping an eye on MAC authentication warnings, ensuring that only authorised devices are given network connectivity. In order to preserve network security, prevent unauthorised access, and safeguard against potential security breaches or unauthorised use of network resources, it is important to promptly respond to MAC authentication notifications. Implementing MAC-based authentication can improve the network's overall security posture by adding another layer of access restriction.

4. CONCLUSION

For monitoring and spotting potential problems, anomalies, and security threats within a network environment, a network alert system is essential. There are several different kinds of network alert systems, each aimed at addressing particular facets of network operations and security. These systems produce alerts that inform administrators or security teams of particular situations, enabling them to react quickly and reduce risks.

These network alert systems generate notifications for a variety of potential problems and failures. Authentication alerts for failed login attempts or unauthorised access attempts, association alerts for Wi-Fi connectivity issues, and 802.1X alerts for network access control failures are a few examples. DNS alerts that indicate DNS server unavailability or poisoning are another.

5. REFERENCES

[1] L. Zhou, G. Zeng, and J. Wang, "An Alert Correlation Framework for Network Intrusion Detection Systems," in IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 10, pp. 2197-2210, Oct. 2017.
[2] M. A. Al-Fayoumi and A. A. Al-Ayyoub, "Network Traffic Analysis Using Machine Learning Techniques for Intrusion Detection," in International Journal of Computer Science and Network Security, vol. 15, no. 6, pp. 77-85, June 2015.
[3] Y. Li, Y. Zhang, and J. Wang, "An Alert Fusion Framework for Network Security Monitoring," in Proceedings of the 16th ACM Symposium on Access Control Models and Technologies, pp. 89-98, June 2011.
[4] A. M. Naghibolhosseini and R. Berangi, "Real-Time Intrusion Detection System for High-Speed Networks Using GPUs," in Journal of Network and Computer Applications, vol. 97, pp. 117-129, Jan. 2018.
[5] W. Zhang, X. Chen, and X. Zhu, "A Collaborative Alert Management System for Network Security," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2369-2378, Dec. 2013.
[6] D. Jiang and L. Huang, "A Distributed Anomaly Detection System for Network Intrusion Detection," in Proceedings of the 35th Annual IEEE Conference on Local Computer Networks, pp. 203-210, Oct. 2010.
[7] M. J. Hussain and S. Anwar, "Traffic Anomaly Detection Using Machine Learning Techniques in Software Defined Networks," in International Journal of Computer Networks & Communications, vol. 8, no. 2, pp. 71-88, Mar. 2016.
[8] T. He and Q. Shi, "Efficient Alert Correlation Algorithms for Network Intrusion Detection Systems," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp. 829-840, May 2014.
[9] Z. Li and H. Zhang, "A Novel Intrusion Detection System for Advanced Persistent Threats Based on Network Traffic Analysis," in Journal of Network and Computer Applications, vol. 87, pp. 140-152, Jan. 2017.
[10] A. Karimian and M. A. Hossain, "Real-Time Network Intrusion Detection Using Data Stream Mining," in Proceedings of the 2019 IEEE Conference on Network Softwarization, pp. 1-5, Oct. 2019.
[11] K. Salah, K. Khelifi, and A. Mellouk, "Towards an Adaptive Alert Management Framework for Network Security," 2016 International Conference on High Performance Computing & Simulation (HPCS), Innsbruck, 2016, pp. 809-816, doi: 10.1109/HPCSim.2016.7568399.
[12] S. Jajodia, P. K. Kalapa, and V. G. Vassilovski, "Automated analysis of network security alerts," in Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), Hong Kong, China, 2004, pp. 430-435, doi: 10.1109/CMPSAC.2004.1342774.
[13] R. Perdisci, G. Giacinto, and W. Lee, "A survey of network intrusion detection techniques," in Advances in Information Security and Its Application, ed. by K. Kim and K. Lee, Springer US, 2009, pp. 171-200, doi: 10.1007/978-0-387-78448-0_9.
[14] Y. Zhang, S. Huang, and C. Wang, "Toward scalable network intrusion detection using parallel computing," in 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-6, doi: 10.1109/ICC.2017.7997069.
[15] H. Hassan , M.N. Khan , S.O. Gilani , M. Jamil , H. Maqbool , A.W. Malik , I. Ah- mad , H. 264 encoder parameter optimization for encoded wireless multimedia transmissions, IEEE Access. 6 (2018) 22046–22053
[16] T. H. Kim, H. J. Kim, and J. W. Hong, "Efficient Alert Systems in Wireless Sensor Networks," in Proceedings of the IEEE International Conference on Computer Communications and Networks, 2010, pp. 1-6.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12634

[17] T.K. Kim, J.H. Kwon, E.J. Kim, Categorization-based video streaming for traffic mitigation in content delivery services, Multimed. Tools Appl. 76 (23) (2017) 25495–25510.
[18] K. T. Hsieh, K. R. Wu, and Y. C. Hu, "A Novel Scalable Alert System for Network Intrusion" in Proceedings of the IEEE Global Telecommunications Conference, 2009, pp. 1-6. [19] S. Hu, K. Chitti, F. Rusek, and O. Edfors, "User assignment with distributed large intelligent surface (LIS) systems," in IEEE WCNC, Barcelona, Spain, Apr. 2018, pp. 1–6.13
[20] S. Jajodia, P. K. Kalapa, and V. G. Vassilovski, "Automated analysis of network security alerts," in Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), Hong Kong, China, 2004, pp. 430-435, doi: 10.1109/CMPSAC.2004.1342774.
[21] R. Perdisci, G. Giacinto, and W. Lee, "A survey of network intrusion detection techniques," in Advances in Information Security and Its Application, ed. by K. Kim and K. Lee, Springer US, 2009, pp. 171-200, doi: 10.1007/978-0-387-78448-0_9.
[22] L. Zhang, X. Chen, S. Liu, Q. Zhang, J. Zhao, J. Dai, G. Bai, X. Wan, Cheng Q, G. Castaldi, V. Galdi, and Tie Jun Cui, "Space-time-coding digital metasurfaces," Nat. Commun., vol. 9,, pp. 1–11, Oct. 2018.

.