International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Performance Analysis of a Snort-based Intrusion Detection System for Wireless Sensor Networks

Gautham Shetty[1], *Krishnan Kocheril Raman*[2]

[1]University of Mysore – gshetty@vtu.co.in
[2]Vellore Institute of Technology

DOI: https://doi.org/10.55248/gengpi.2023.32489

ABSTRACT

The Intrusion Detection System (IDS) is a critical mechanism that considers various factors, including traversal path, time, energy, network lifetime, and packet security. However, the energy overhead generated by flooding control messages and other protocol support packets can decrease node and system latency. Therefore, the proposed method aims to increase the throughput ratio while minimizing energy overhead and latency. Previous hop count-based methods are not optimal in dynamically changing environments, and other techniques produce more latency, which reduces the network's throughput. Routing procedures can take longer than the assigned time-to-live value, leading to more packet drop ratios, poor route management, and reduced security for intrusion detection. Some approaches use control messages to collect neighbor information, which increases overhead, traffic, and latency in wireless sensor networks (WSN). The network overhead cost generated by previous approaches reduces packet delivery ratio and network throughput

Keywords:Wireless Sensor Network

1. Introduction

A computer network is a group of interconnected computing nodes that communicate with one another using well-defined protocols. In recent years, wireless sensor networks have grown significantly in both home and corporate environments. However, with this growth comes an increase in security issues, making it essential to secure network boundaries using intrusion detection systems (IDS) to protect company assets and ensure service reliability. Unfortunately, due to the rapid advancement of technology and a lack of emphasis on integrating good security practices in software and hardware design, backdoors and bugs have become common, making traditional network security mechanisms ineffective against a wide range of attacks, including denial of service, IP spoofing, eavesdropping, masquerading, and malware attacks.

To address these challenges, intrusion detection systems have become an integral part of the entire defense system, deployed in conjunction with other security mechanisms to provide better network defense against unauthorized access by users and malicious code attacks. IDS has been studied for nearly 20 years, and its deployment has become unavoidably necessary in many systems and applications that are deployed without much security consideration. However, different types of IDS exist, depending on the nature of the environment where they are deployed. These can be either network-based or host-based intrusion detection systems. IDS can also be categorized based on the techniques used to identify network intrusion, with the two major techniques being misuse and anomaly detection.

One technique for identifying malicious packets or code is signature-based detection. This technique involves matching the packet payload with the pre-defined signature stored in the system database. Although signature-based detection is accurate, it presents performance degradation in higher traffic networks. This performance limitation leads to problems associated with systems using signature-based techniques, including packet dropping that happens as a result of excessive string processing by the pattern matching algorithm, which can take up to 40% to 50% of the SNORT processing time [1][2][3][4][5][6][7].

SNORT is an example of a signature-based technique tool that experiences a higher number of packet dropping. SNORT is an open-source intrusion detection system that is widely deployed in middle-sized industries and most campus networks. Its flexible code has attracted many researchers to develop additional features that can meet user requirements. For example, the SNORT MySQL pre-processor plug-in can monitor communication between a client and MySQL server and detect any anomalous packets[8][9][10][11][12][13].

In conclusion, as computer networks continue to grow in size and complexity, the need for effective intrusion detection systems becomes more critical. While different types of IDS exist, signature-based techniques have been proven to be accurate but can present performance limitations in higher traffic networks. Therefore, researchers are continually exploring new techniques to develop more efficient IDS to mitigate the risk of security breaches and protect valuable company assets.

2. Litrature Review

Various algorithms have been developed for pattern matching in intrusion detection systems (IDS). In this article, we will discuss some of the latest research in this area and highlight their strengths and weaknesses.

Prabha and Sukumaran introduced an Improved Single Keyword Pattern Matching Algorithm (ISPMA) for IDS and compared it with other well-known algorithms such as Boyer-Moore Algorithm, Horspool, Karp-Rabin algorithm, and Brute force algorithm. Their experiment showed that their algorithm is faster and more reliable than others. Similarly, Dai Hong proposed an enhanced version of the Boyer-Moore Horspool Algorithm, which takes full advantage of matching information to skip several characters, resulting in improved pattern matching performance and memory resource utilization. The proposed algorithm is adaptable to different pattern string and text character sets, and its matching speed increases significantly, even for long pattern lengths and multiple patterns[14][15][16][17][18].

Jain and Pandey conducted a comparative study on various existing pattern matching algorithms and found that the Boyer-Moore Algorithm is the most efficient and fastest, providing accurate results. Another study by Bhatia, Shashikant, and Choudhary exposed the challenges in pattern matching and proposed an Optimized Pattern Matching (OPM) algorithm for finding matched links. They compared their proposed algorithm with existing algorithms and found that it outperforms them in terms of accuracy and efficiency.

Furthermore, Islam Jony illustrated a widely used multiple string patterns matching algorithm that reduces the number of character comparisons and memory space requirements based on graph transition structure and dynamic linked list search technique. Similarly, Patel and Thakkar proposed an efficient version of Bidirectional Pattern An Efficient Exact Single Pattern Matching (EESP) algorithm, which reduces pre-processing time and finds all occurrences of the pattern in a long text string.

Watson introduced a more practical algorithm for a special characterization of 'matching productions,' which deals with chain rules in pattern grammar using the transitive closure of a relation. The algorithm also introduces the idea of shift distances greater than one symbol, similar to the Boyer-Moore and Commentz-Walter algorithms.

Le Dang, Le, and Trong Le presented a new algorithm for multiple-pattern exact matching, which reduces character comparisons and memory space based on graph transition structure and dynamic linked list search technique. Theoretical analysis and experimental results showed that their algorithm is highly efficient in both space and time compared to previously known pattern-matching algorithms.

Sapats and Paulins conducted a comparative evaluation of pattern matching algorithm performance under the tool of Snort and Suricata, which can use a multithreaded design. The test results showed that the Suricata algorithm is more effective than Snort algorithms in multithreaded computing approaches.

Moving on to intrusion detection, Lata, Kashyap Indu, and Nagaraju proposed an algorithm to lower the false alarm rate in IDS considerably. They identified that intrusion can occur in the header part or payload part and proposed an algorithm that addresses both areas of intrusion. Additionally, Rashida presented a novel Distributed Intrusion Detection System using Multi-Agent to manage misuse and anomaly detects in a network-based IDS.

Shibu and Chikkamannur surveyed the current techniques used in social media fraud detection, highlighting the importance of this field in today's computing environment. They proposed that combining different techniques can help to detect fraud attempts more effectively and reduce false positives.

Finally, Pawar, Kyatanavar, and Jawale described the implementation and experimental analysis of an Advanced Intrusion Detection System (AIDS) with prevention capabilities. Their proposed system provides detection of both known and unknown intrusions and alerts the network administrator automatically.

3. Research Methodology

An intrusion can be broadly defined as any attempt to compromise the confidentiality, integrity, or availability of information or resources in a computer system or network. This can include unauthorized access to a system, theft or destruction of data, or the installation of malware or viruses. Given the complexity of modern computer systems, detecting such intrusions can be a difficult task that requires sophisticated algorithms and tools.

One approach to intrusion detection is to use signature-based detection, which involves searching for known patterns of malicious activity in network traffic or system logs. This approach relies on the assumption that attacks will leave identifiable traces that can be matched against a database of known attack signatures. The advantage of this approach is that it can detect attacks quickly and accurately, but the downside is that it is only effective against known attacks and may be vulnerable to evasion by attackers who use novel techniques[19][20][21][22][23][24].

Another approach is to use anomaly detection, which involves identifying patterns of behavior that deviate from normal or expected behavior. This approach does not rely on pre-defined attack signatures and can potentially detect novel attacks, but it is more prone to false positives and may be less effective at detecting sophisticated attacks that mimic normal behavior.

Regardless of the approach used, the effectiveness of an IDS depends on the quality of its algorithms and its ability to adapt to changing threat landscapes. Researchers have developed various algorithms for pattern matching in IDSs, including the Boyer-Moore Algorithm, Horspool, Karp-Rabin algorithm, and Brute force algorithm. These algorithms have been tested and compared in various studies, with some researchers proposing improved or more efficient versions of these algorithms.

For example, Prabha and Sukumaran introduced an Improved Single Keyword Pattern Matching Algorithm (ISPMA) for IDS and compared it with other well-known algorithms. Their experiment showed that their algorithm is faster and more reliable than others. Similarly, Dai Hong proposed an enhanced version of the Boyer-Moore Horspool Algorithm, which takes full advantage of matching information to skip several characters, resulting in improved pattern matching performance and memory resource utilization.

Jain and Pandey conducted a comparative study on various existing pattern matching algorithms and found that the Boyer-Moore Algorithm is the most efficient and fastest, providing accurate results. Another study by Bhatia, Shashikant, and Choudhary exposed the challenges in pattern matching and proposed an Optimized Pattern Matching (OPM) algorithm for finding matched links. They compared their proposed algorithm with existing algorithms and found that it outperforms them in terms of accuracy and efficiency.

In addition to developing more efficient algorithms, researchers have also explored other techniques for improving IDS performance, such as multithreaded computing approaches and distributed intrusion detection systems using multi-agent architecture. Sapats and Paulins conducted a comparative evaluation of pattern matching algorithm performance under the tool of Snort and Suricata, which can use a multithreaded design. The test results showed that the Suricata algorithm is more effective than Snort algorithms in multithreaded computing approaches. Additionally, Rashida presented a novel Distributed Intrusion Detection System using Multi-Agent to manage misuse and anomaly detects in a network-based IDS.

While algorithms and tools are important for effective intrusion detection, they are only part of the picture. It is also crucial to have well-designed security policies and procedures, regular security audits, and trained security personnel who can monitor and respond to alerts generated by the IDS. IDSs are just one component of a comprehensive security strategy, but they are an essential one that can help organizations detect and respond to threats in a timely and effective manner.

In conclusion, intrusion detection systems are critical tools for protecting computer systems and networks against cyber attacks. They work by monitoring system activity, applying various algorithms to detect patterns of information that correspond to a specific intrusion, and triggering alarms and logging.

4. Conclusion

In the field of intrusion detection systems (IDS), researchers have identified a number of promising algorithms for single keyword pattern matching. Among these algorithms are the Boyer-Moore Algorithm, which uses two tables and matches from right to left, and the Horspool algorithm, which uses only one table and matches faster than the Boyer-Moore. The Brute force algorithm requires no preprocessing of the pattern, while the Kunth-Morris-Pratt algorithm performs comparisons from left to right. The Karp-Rabin algorithm is based on a hashing approach.

A new Logo Pattern Matching algorithm has been proposed and compared to existing algorithms, demonstrating faster and more reliable performance in network security applications. Specifically, the results show an improvement in average comparison, fewer character comparisons, and fewer attempts compared to the existing algorithms.

Future work in this area will focus on enhancing the method by moving towards distributed computing, which will reduce the workload of the system and improve the speed and accuracy of the detection of malicious activities..

REFERENCES

[1] Van der Geer, J., Hanraads, J. A. J., & Lupton, R. A. (2000). The art of writing a scientific article.Journal of Science Communication, 163, 51–59.

[2] Strunk, W., Jr., & White, E. B. (1979).The elements of style (3rd ed.). New York: MacMillan.

[3] Mettam, G. R., & Adams, L. B. (1999).How to prepare an electronic version of your article. In B. S. Jones & R. Z. Smith (Eds.), Introduction to the electronic age (pp. 281–304). New York: E-Publishing Inc.

[4] Fachinger, J., den Exter, M., Grambow, B., Holgerson, S., Landesmann, C., Titov, M., et al. (2004).Behavior of spent HTR fuel elements in aquatic phases of repository host rock formations, 2nd International Topical Meeting on High Temperature Reactor Technology. Beijing, China, paper #B08.

[5] Fachinger, J. (2006). Behavior of HTR fuel elements in aquatic phases of repository host rock formations.Nuclear Engineering & Design,236, 54.

[6] Gani, A. (2017). The logistics performance effect in international trade. The Asian Journal of Shipping and Logistics, 33(4), 279-288.

[7] Bugarčić, F. Ž., Skvarciany, V., & Stanišić, N. (2020). Logistics performance index in international trade: Case of Central and Eastern European and Western Balkans countries. Business: Theory and Practice, 21(2), 452-459.

[8] Rodriguez, K. M., Reddy, R. S., Barreiros, A. Q., & Zehtab, M. (2012, June). Optimizing Program Operations: Creating a Web-Based Application to Assign and Monitor Patient Outcomes, Educator Productivity and Service Reimbursement. In DIABETES (Vol. 61, pp. A631-A631). 1701 N BEAUREGARD ST, ALEXANDRIA, VA 22311-1717 USA: AMER DIABETES ASSOC.

[9] Kwon, D., Reddy, R., & Reis, I. M. (2021). ABCMETAapp: R shiny application for simulation-based estimation of mean and standard deviation formetaanalysis via approximate Bayesian computation. Research synthesis methods, 12(6), 842–848. https://doi.org/10.1002/jrsm.1505

[10] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Usability Evaluation of an Unpopular Restaurant Recommender Web Application Zomato. Asian Journal of Research in Computer Science, 13(4), 12-33.

[11] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., & Gogineni, A. (2022). Analysis of the Unexplored Security Issues Common to All Types of NoSQL Databases. Asian Journal of Research in Computer Science, 14(1), 1-12.

[12] Singh, P., Williams, K., Jonnalagadda, R., Gogineni, A., &; Reddy, R. R. (2022). International students: What's missing and what matters. Open Journal of Social Sciences, 10(02),

[13] Jonnalagadda, R., Singh, P., Gogineni, A., Reddy, R. R., & Reddy, H. B. (2022). Developing, implementing and evaluating training for online graduate teaching assistants based on Addie Model. Asian Journal of Education and Social Studies, 1-10.

[14] Sarmiento, J. M., Gogineni, A., Bernstein, J. N., Lee, C., Lineen, E. B., Pust, G. D., & Byers, P. M. (2020).Alcohol/illicit substance use in fatal motorcycle crashes. Journal of surgical research, 256, 243-250.

[15] Brown, M. E., Rizzuto, T., & Singh, P. (2019). Strategic compatibility, collaboration and collective impact for community change. Leadership & Organization Development Journal.

[16] Sprague-Jones, J., Singh, P., Rousseau, M., Counts, J., & Firman, C. (2020). The Protective Factors Survey: Establishing validity and reliability of a self-report measure of protective factors against child maltreatment. Children and Youth Services Review, 111, 104868.

[17] Reddy Sadashiva Reddy, R., Reis, I. M., & Kwon, D. (2020). ABCMETAapp: R Shiny Application for Simulation-based Estimation of Mean and Standard Deviation for Meta-analysis via Approximate Bayesian Computation (ABC). arXiv e-prints, arXiv-2004.

[18] Reddy, H. B. S, Reddy, R. R., & Jonnalagadda, R. (2022). A proposal: Human factors related to the user acceptance behavior in adapting to new technologies ornew user experience. International Journal of Research Publication and Reviews, 121-125. doi:10.55248/gengpi.2022.3.8.1

[19] Reddy, H. B. S., Reddy, R. R. S., & Jonnalagadda, R. (2022). Literature Review Process: Measuring the Effective Usage of Knowledge Management Systems in Customer Support Organizations. In International Journal of Research Publication and Reviews (pp. 3991–4009). https://doi.org/10.55248/gengpi.2022.3.7.45

[20] Reddy, R. R. S., & Reddy, H. B. S. (2022). A Proposal: Web attacks and Webmaster's Education Co-Relation. In International Journal of Research Publication and Reviews (pp. 3978–3981). https://doi.org/10.55248/gengpi.2022.3.7.42

[21] Reddy, H. B. S. (2022). A Proposal: For Emerging Gaps in Finding Firm Solutions for Cross Site Scripting Attacks on Web Applications. In International Journal of Research Publication and Reviews (pp. 3982–3985). https://doi.org/10.55248/gengpi.2022.3.7.43810 International Journal of Research Publication andReviews, Vol 3, no 8, pp 807-809 August 2022

[22] Lu, N., Butler, C. C., Gogineni, A., Sarmiento, J. M., Lineen, E. B., Yeh, D. D., Babu, M., & Byers, P. M. (2020). Redefining Preventable Death—Potentially Survivable Motorcycle Scene Fatalities as a New Frontier. In Journal of Surgical Research (Vol. 256, pp. 70–75). Elsevier BV. https://doi.org/10.1016/j.jss.2020.06.014

[23] Reddy, H. B. S. (2022). Exploring the Existing and Unknown Side Effects of Privacy Preserving Data Mining Algorithms (Doctoral dissertation, NovaSoutheastern University).

[24] Sadashiva Reddy, H. B. (2022). Exploring the Existing and Unknown Side Effects of Privacy Preserving Data Mining Algorithms.