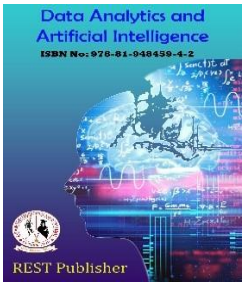
DOI: https://doi.org/10.46632/daai/2/6/15

Data Analytics and Artificial Intelligence

Vol: 2(6), 2022

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/



Advancing Network Security: Assessing Risks and Enhancing Resilience through Visualization and TOPSIS Methodology

Shanker Gangone

Incredible Software Solutions LLC, Research and Development Division, Richardson, TX, USA.

Corresponding author: *Shanksr93940@gmail.com*

***Abstract**: The increasing complexity and interconnectedness of modern communication networks pose significant challenges in ensuring their security and reliability. This research examines essential aspects of network security, such as communication protocols, node security, encryption techniques, monitoring algorithms, and security policies. Using the TOPSIS method, we assess the security risks within energy-managed communication networks, emphasizing the critical need to balance technical, operational, and strategic priorities to effectively secure network operations. As cyberthreats continue to advance, it is imperative that organizations implement proactive measures that include advanced visualization tools and robust security solutions to address emerging risks. Visualization plays a critical role in network security by providing actionable insights that help identify patterns, anomalies, and vulnerabilities in complex datasets. This study underscores the transformative impact of security visualization by categorizing recent advances, pointing out areas that require further research, and providing strategic guidance for future developments. By addressing these gaps and adopting innovative technologies, organizations can strengthen the resilience and reliability of interconnected systems. The research emphasizes the importance of a comprehensive security strategy that includes technological advancements, employee training, and constant monitoring to effectively address emerging cyber threats.*

1. INTRODUCTION

The Internet is a complex and ever-changing system with a complex architecture and rapid technological advancements. Security measures designed for small, static networks fail to address the dynamic and diverse challenges of modern network environments. This shortcoming stems from a lack of expertise in software and security engineering, compounded by tight deadlines and market demands, which often results in poor programming practices. While some security solutions are currently effective, the constant evolution of technology creates new vulnerabilities over time. Therefore, maintaining cybersecurity requires a comprehensive approach that integrates various strategies to effectively address various attack vectors. Continuous monitoring and adaptability are critical to protecting the integrity of the system against evolving threats. The increase in computer misuse and growing concerns about privacy violations related to data storage highlight the need for robust technical safeguards. These measures can be divided into four main categories, each addressing specific and interconnected issues. Access controls manage user permissions to access and modify data, ensuring that only authorized users interact with sensitive information. Flow controls regulate the transfer and distribution of data within and across datasets, maintaining a secure and controlled flow of information. Inference controls are designed to prevent unauthorized inferences from statistical databases by carefully designing queries to avoid revealing confidential data. However, statistical databases often have weaker security than expected, making them vulnerable. Data encryption is an important security measure, protecting sensitive information from unauthorized access during transmission or storage, ensuring both confidentiality and integrity against external threats. Wireless sensor networks (WSNs) have become an exciting technology in areas such as remote environmental monitoring and target tracking. The advancement of small, affordable, and intelligent sensors with wireless capabilities has made it possible to create interconnected networks that can share and analyze data in real time. The architecture of a wireless sensor network (WSN) is influenced by factors such as its purpose, environmental conditions, design objectives, budget, and hardware constraints. These networks play a vital role in a variety of applications, and their deployment presents unique challenges in many areas. We classify these challenges

into three main domains. First, issues in the underlying platform and its operating system limit the overall performance and efficiency of the network. Second, challenges in the communication protocol layer can affect the network's ability to transmit data securely and reliably. Third, difficulties in network services, provisioning, and deployment hinder large-scale implementation and ongoing maintenance. Our study builds on existing research by taking a top-down approach to explore emerging applications and their associated challenges. We emphasize security as a critical concern, as WSNs are vulnerable to a variety of attacks targeting protocols, software, and hardware, which threaten the security, integrity, and availability of data. Despite efforts to address security at the MAC and network layers, the potential of the visualization layer in improving WSN security remains limited. Visualization techniques can provide valuable insights into network behavior, helping to detect and mitigate security threats. In the field of network security visualization, our study provides a comprehensive review of recent research and categorizes them into five distinct use case categories. These categories cover a wide range of applications and demonstrate the various visualization techniques and data sources used in network security research. We have summarized these findings in a clear table to improve understanding and accessibility.By analyzing current systems, we identify key issues and challenges related to visualizing network security, largely stemming from the complexity of network data and the need for effective tools to understand and act on this information. The architecture of a wireless sensor network (WSN) is influenced by factors such as its purpose, environmental conditions, design objectives, budget, and hardware constraints. These networks play a critical role in a variety of applications, and their deployment presents unique challenges in many areas. We classify these challenges into three main domains. First, issues in the underlying platform and its operating system limit the overall performance and efficiency of the network. Second, challenges in the communication protocol layer can affect the network's ability to transmit data securely and reliably. Third, difficulties in network services, provisioning, and deployment hinder large-scale implementation and ongoing maintenance. Our study builds on existing research by taking a top-down approach to explore emerging applications and their associated challenges. We emphasize security as a critical concern, as WSNs are vulnerable to a variety of attacks targeting protocols, software, and hardware, which threaten the security, integrity, and availability of data. Despite efforts to address security at the MAC and network layers, the potential of the visualization layer in improving WSN security remains limited. Visualization techniques can provide valuable insights into network behavior, helping to detect and mitigate security threats. In the field of network security visualization, our study provides a comprehensive review of recent research and categorizes it into five distinct use case categories. These categories cover a wide range of applications and demonstrate the various visualization techniques and data sources used in network security research. We have summarized these findings in a clear table to improve understanding and accessibility. By analyzing current systems, we identify key issues and challenges related to visualizing network security, largely stemming from the complexity of network data and the need for effective tools to understand and act on this information. Network monitoring systems are essential for ensuring the performance and security of networks. These systems continuously monitor network components, identify slow or faulty components, and resolve issues before they escalate. Effective network monitoring encompasses a variety of factors, including response time, availability, uptime, and security, to ensure uninterrupted operations in both business and public sectors. The reports generated by these systems are tailored to a variety of audiences, including network administrators and management, and provide insights into performance metrics, compliance, and internal security threats. Security-centric monitoring further protects critical data by controlling access points and detecting malicious activity. Our article explores the challenges and opportunities in using visual analytics to improve network security. By reviewing existing tools and techniques, we highlight gaps in current research and propose strategies to address these limitations. Effective network monitoring encompasses a number of critical aspects, including response time, availability, uptime, and security, to ensure uninterrupted operations in both business and public sectors. These systems generate reports tailored to various stakeholders, such as network administrators and management teams, providing valuable insights into performance indicators, regulatory compliance, and potential internal security risks. Security-oriented monitoring adds additional security by controlling access points and detecting malicious activity. This paper examines the challenges and potential of visual analytics in strengthening network security. It reviews existing tools and methodologies, reveals gaps in current research, and proposes solutions to address these issues. Visualization serves as a powerful tool for analyzing complex network data, allowing analysts to identify patterns, detect irregularities, and respond effectively to threats. The ever-changing nature of networks requires continuous advancements in visualization methods to address emerging security challenges. Cybersecurity is a major obstacle to the growth of e-commerce, as modern interconnected business environments require robust protection against cyber threats. Organizations must strike a balance between maintaining connectivity and protecting critical information and systems. Failure to prioritize security can result in significant financial losses and reputational damage, underscoring the need for proactive strategies. By integrating technical safeguards, employee education, and continuous monitoring, organizations can effectively mitigate risks and

strengthen their defenses against cyberattacks. Our study highlights the critical role of network security visualization in securing contemporary networks. By categorizing recent research into specific application groups, we provide a comprehensive overview of the current landscape of the field. This analysis demonstrates the potential of visualization to address new challenges in network security, providing valuable direction for researchers, developers, and practitioners. As technology advances, the need for innovative, adaptable security measures will be critical, ensuring the stability and reliability of interconnected systems.

2. MATERIALS & METHODS

Network Security: Security risk assessment is a critical process for securing modern communication systems, especially energy management and control networks. These systems rely on robust communication networks to ensure uninterrupted data transmission and the operation of critical infrastructure. As vulnerabilities in communication systems can lead to severe financial, operational, and reputational damage, identifying and mitigating security risks is of paramount importance. This paper provides an insightful study of five fundamental factors for assessing security risks in networked systems: communication protocol, node security, network monitoring, cryptography, and security policy. These factors are explored with an illustrative case study that uses the fuzzy TOPSIS method to assess security risks in energy management communication networks.

Communication Protocol (C1): A communication protocol forms the backbone of any network, defining the rules and standards for transmitting data. Protocols enable seamless communication between network devices by specifying procedures for error recovery, synchronization, syntax, and semantics. Reliable communication protocols ensure stable network operations, minimize compatibility issues, and enable efficient data transfer. For energy management systems, protocols must handle critical functions such as real-time data monitoring, secure data transfer, and interoperability between different devices. The robustness of communication protocols is directly linked to network stability, making them a key factor in risk assessment.

Node Security (C2): Node security is essential for wireless sensor networks (WSNs), where small, low-power devices handle sensing, data transmission, and reception. Since these nodes often operate in remote or challenging environments, they are vulnerable to security breaches. Node security management involves implementing measures to protect nodes from unauthorized access, physical damage, or software-based attacks. For example, in energy systems, compromised nodes can lead to inaccurate data measurements or unauthorized control of critical components. Effective node security extends the lifespan of the network and ensures its reliability, making it a key criterion for assessing security risks.

Network Monitoring (C3): Continuous network monitoring provides administrators with insights into network health, performance, and potential vulnerabilities. Monitoring systems track key metrics such as uptime, response time, availability, and data flow, which helps identify problems early. For example, a short network outage in a power management system can disrupt service delivery and impact operations. By providing actionable reports to administrators and management, network monitoring helps maintain high-performance networks with minimal downtime. In addition, security-focused monitoring detects threats such as unauthorized access, ensures the security of critical data, and improves resilience against cyber-attacks.

Cryptography (C4): Cryptography is a cornerstone of information security, using encryption techniques to protect data during storage and transmission. By ensuring that sensitive information is accessible only to authorized entities, cryptography prevents data breaches and unauthorized access. In energy management systems, cryptography secures communication between devices and protects critical operational data. Advanced encryption methods, such as public-key cryptography, provide strong defenses against emerging cyber threats. The versatility and effectiveness of cryptographic measures make them essential in a comprehensive security risk assessment.

Security Policy (C5): A security policy serves as a framework for managing access, implementing security measures, and addressing vulnerabilities in the network. It outlines protocols for handling security incidents, defining roles and responsibilities for stakeholders. For energy management systems, security policies should address regulatory compliance, data privacy, and business continuity. By providing clear guidelines, a well-designed security policy

ensures consistency in the application of security measures and reduces the risks associated with human error or oversight. This fundamental element supports the broader goal of establishing a secure and reliable network environment.

Methodology: The study used a TOPSIS method to assess security risks in communication networks of energy management and control systems. This approach combines MCDM logic, which is similar to the Order of Preference for Ideal Solution (TOPSIS), with the technique of Similarity by Order of Preference to the Ideal Solution (TOPSIS), to enable decision-making under uncertainty. Thirty-five decision-makers participated in assessing the suitability of six alternative communication networks (CN1, CN2, CN3, CN4, CN5 and CN6) based on five security risk factors: communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4) and security policy (C5). Decision-makers were surveyed using a linguistic variable scale to assess the importance of each factor for the six alternatives. Linguistic variables, such as "very important", "important" or "less important", were converted to fuzzy numbers to accommodate uncertainty and subjectivity in the evaluation process. The TOPSIS method ranks alternatives based on their performance across criteria, calculating the relative closeness of each alternative to an ideal solution.TOPSIS analysis identified the most suitable communication network for energy management systems. Communication protocol (C1) emerged as the most important factor, reflecting the need for robust standards to ensure data reliability and interoperability. Node security (C2) and network monitoring (C3) also received high priority, highlighting their role in maintaining operational continuity and mitigating security risks. Cryptography (C4) and security policy (C5) provided essential safeguards that ensure data confidentiality and regulatory compliance. The study revealed that alternative CN3 outperformed the others, providing a balanced approach to addressing the five criteria. CN3 demonstrated strong capabilities in implementing advanced communication protocols, robust node security measures, and efficient network monitoring systems. In addition, its cryptographic techniques and comprehensive security policy provided enhanced protection against cyber threats. The findings underscore the importance of a multi-faceted approach to security risk assessment in communication networks. Organizations managing energy systems should prioritize the integration of robust protocols, secure node operations, and active monitoring mechanisms. Investing in cryptographic solutions and well-defined security policies will further enhance network resilience against emerging cyber threats. The TOPSIS method was effective in accommodating the inherent uncertainty and subjectivity in decision-making. By leveraging expert opinions and linguistic variables, the approach provided a comprehensive framework for evaluating complex security challenges. The method can be extended to other domains, providing a versatile tool for risk assessment and decision support.

3. RESULT AND DISCUSSION

TABLE 1. Data set for Decision matrix

	Communication protocol (C1)	Node security (C2)	Network monitoring (C3)	Cryptography (C4)	Security policy (C5)
CN1	6.143	6.257	6.6	5.971	5.286
CN2	5.40	5.686	5.4	5.571	5.171
CN3	5.343	5.686	5.229	5.514	5.343
CN4	5.686	6.086	6.086	5.857	5.971
CN5	5.971	6.371	6.314	6.143	6.486
CN6	7.629	7.629	8.086	8.086	8.029

Table 1 The decision matrix for assessing the security risks of communication networks in energy management and control systems includes five important criteria: communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5). Six communication network alternatives (CN1 to CN6) are evaluated based on these criteria. CN1 exhibits a communication protocol score of 6.143, node security 6.257, network monitoring 6.6, cryptography 5.971, and security policy score of 5.286. CN2 scores 5.4, 5.686, 5.4, 5.571, and 5.171 for C1, C2, C3, C4, and C5, respectively. Similarly, CN3 shows scores of 5.343 for C1, 5.686 for C2, 5.229 for C3, 5.514 for C4, and 5.343 for C5. CN4 exhibits improved performance with scores of 5.686 for C1, 6.086 for C2, 6.086 for C3, 5.857 for C4, and 5.971 for C5. Meanwhile, CN5 scores of 5.971 for C1, 6.371 for C2, 6.314 for C3, 6.143 for C4, and 6.486 for C5. Notably, CN6 outperforms all other alternatives, achieving higher scores in all criteria: 7.629 for C1 and C2, 8.086 for C3 and C4, and 8.029 for C5. This dataset provides a comprehensive basis for

further analysis, such as using the TOPSIS method to prioritize these communication networks based on their suitability for reducing security risks.

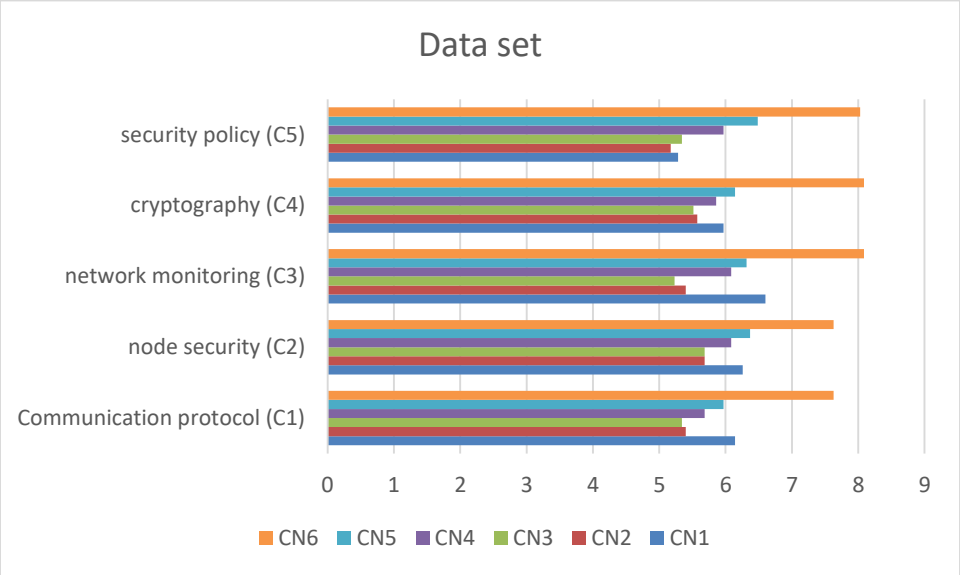


FIGURE 1. Graph for Data set

Figure 1 presents a decision matrix that evaluates six communication nodes (CN1 to CN6) across five criteria critical to cybersecurity and network operations. These criteria include communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5). Each communication node was rated with real-valued scores that reflect their performance or compliance with these criteria. With the highest scores of 7.629 in communication protocol and 8.086 in both network monitoring and cryptography, CN6 outperforms the other nodes across all criteria, underscoring its strong security and monitoring capabilities. In contrast, CN2 and CN3 exhibit lower scores, highlighting areas for potential improvement. Notably, CN5 exhibits strong performance, particularly in security policy (6.486), suggesting that it is well suited for secure policy implementations. The matrix provides a comprehensive framework for evaluating and comparing the security aspects of communication nodes, which aids in decision-making for optimal network security strategies.

TABLE 2. Normalized Data

	C1	**C2**	**C3**	**C4**	**C5**
CN1	0.4126	0.4042	0.4240	0.3899	0.3521
CN2	0.3627	0.3673	0.3469	0.3638	0.3444
CN3	0.3589	0.3673	0.3359	0.3601	0.3559
CN4	0.3819	0.3931	0.3909	0.3825	0.3977
CN5	0.4011	0.4116	0.4056	0.4011	0.4320
CN6	0.5125	0.4928	0.5194	0.5280	0.5348

Table 2 presents the normalized result matrix, in which the performance scores from Table 1 have been normalized to a common scale, which enables the comparison of the six communication nodes (CN1 to CN6) across the five criteria. CN6 emerges as the best performing node, achieving the highest normalized values across all criteria, 0.5125 for Communication Protocol (C1), 0.4928 for Node Security (C2), 0.5194 for Network Monitoring (C3), 0.5280 for Cryptography (C4), and 0.5348 for Security Policy (C5). CN5 follows closely, with notable values of 0.4011 for Communication Protocol (C1) and 0.4320 for Security Policy (C5), indicating strong overall performance. In contrast, CN1 has moderate normalized scores, including 0.4126 for Communication Protocol (C1) and 0.3521 for Security Policy (C5). CN2 and CN3, although similar in performance, have lower values such as 0.3627 for communication protocol (C1) and 0.3359 for network monitoring (C3), suggesting the need for improvement in these areas. CN4

shows consistent performance with values such as 0.3931 for node security (C2) and 0.3909 for network monitoring (C3). The normalized data provides an insightful comparative analysis, elevating CN6 as the most efficient node and guiding the priority for improving network security and performance.

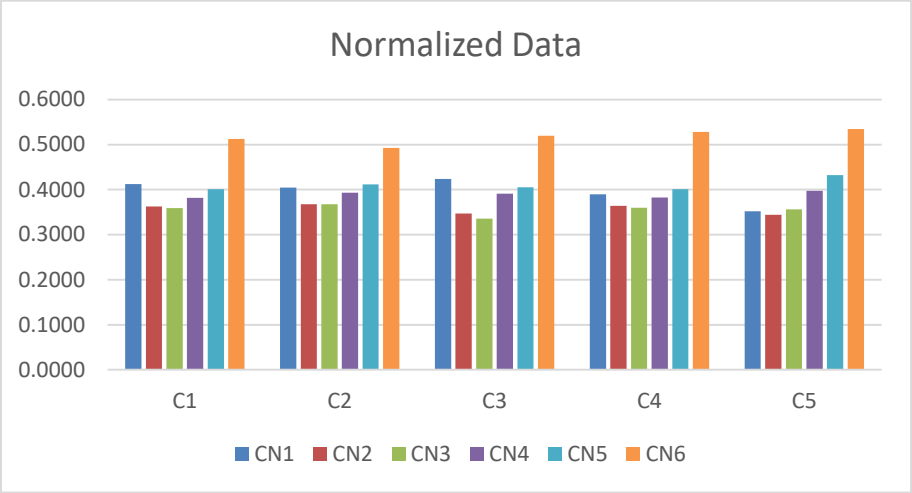


FIGURE 2. Normalized Data

Figure 2 shows the normalized decision matrix for six interaction nodes (CN1 to CN6) across five criteria. CN6 outperforms the others, showing its strength, with the highest values of 0.5125 for C1, 0.5194 for C3, and 0.5348 for C5. CN5 follows closely, excelling especially in C5 (0.4320). CN1 shows moderate performance, with 0.4126 for C1 and 0.3521 for C5, while CN2 and CN3 have lower values, such as 0.3627 for C1. CN4 exhibits balanced results, highlighting areas for improvement in specific criteria.

TABLE 3. Weight

	C1	**C2**	**C3**	**C4**	**C5**
CN1	0.2	0.2	0.2	0.2	0.2
CN2	0.2	0.2	0.2	0.2	0.2
CN3	0.2	0.2	0.2	0.2	0.2
CN4	0.2	0.2	0.2	0.2	0.2
CN5	0.2	0.2	0.2	0.2	0.2
CN6	0.2	0.2	0.2	0.2	0.2

Table 3 outlines the weight matrix for the decision-making process involving six communication nodes (CN1 to CN6) and five evaluation criteria. Each criterion is assigned an equal weight of 0.2 across all nodes, reflecting an unbiased approach where all criteria are considered equally important in evaluating the performance of the nodes. This uniform weighting ensures a balanced evaluation, emphasizing that no single criterion dominates the decision-making process. By using equal importance, the decision-making model promotes fairness in determining the most appropriate communication node based on the normalized performance values.

TABLE 4. Weighted normalized decision matrix

	C1	**C2**	**C3**	**C4**	**C5**
CN1	0.0825	0.0808	0.0848	0.0780	0.0704
CN2	0.0725	0.0735	0.0694	0.0728	0.0689
CN3	0.0718	0.0735	0.0672	0.0720	0.0712
CN4	0.0764	0.0786	0.0782	0.0765	0.0795
CN5	0.0802	0.0823	0.0811	0.0802	0.0864
CN6	0.1025	0.0986	0.1039	0.1056	0.1070

Table 4 presents the weighted normalized decision matrix, combining the normalized scores from Table 2 with equal weights (0.2 for all criteria) from Table 3. This matrix evaluates six interaction nodes (CN1 to CN6) across five criteria. CN6 receives the highest weighted values, such as 0.1025 for C1, 0.1039 for C3, and 0.1070 for C5, highlighting its superior performance across all criteria. CN5 follows, especially excelling in C5 (0.0864). CN4 exhibits balanced performance with values such as 0.0786 for C2 and 0.0795 for C5. CN1 has moderate scores of 0.0848 for C3, while CN2 and CN3 have relatively low values, including 0.0725 for C1 and 0.0672 for C3, respectively. This matrix provides a comprehensive comparison, enabling informed decision-making by emphasizing the relative importance of performance normalized across equally weighted criteria.

TABLE 5. Positive Matrix

	C1	C2	C3	C4	C5
CN1	0.1025	0.0986	0.1039	0.1056	0.1070
CN2	0.1025	0.0986	0.1039	0.1056	0.1070
CN3	0.1025	0.0986	0.1039	0.1056	0.1070
CN4	0.1025	0.0986	0.1039	0.1056	0.1070
CN5	0.1025	0.0986	0.1039	0.1056	0.1070
CN6	0.1025	0.0986	0.1039	0.1056	0.1070

Table 5 represents the positive best solution matrix for the decision-making process involving six communication nodes (CN1 to CN6) in five criteria. The matrix shows the maximum values obtained for each criterion from Table 4, where all nodes are compared to the positive best solution. Each value, 0.1025 for C1, 0.0986 for C2, 0.1039 for C3, 0.1056 for C4, and 0.1070 for C5, represents the best performance achievable under the evaluation framework. This matrix serves as a benchmark for assessing the performance gap between each communication node and the best scenario, thereby guiding the selection process for the most effective communication node.

TABLE 6. Negative matrix

	C1	C2	C3	C4	C5
CN1	0.0718	0.0735	0.0672	0.0720	0.0689
CN2	0.0718	0.0735	0.0672	0.0720	0.0689
CN3	0.0718	0.0735	0.0672	0.0720	0.0689
CN4	0.0718	0.0735	0.0672	0.0720	0.0689
CN5	0.0718	0.0735	0.0672	0.0720	0.0689
CN6	0.0718	0.0735	0.0672	0.0720	0.0689

Table 6 illustrates the negative best solution matrix for evaluating six interacting nodes (CN1 to CN6) on five criteria. This matrix reflects the minimum performance values for each criterion obtained from Table 4. For example, the minimum values for all criteria are the same across nodes: 0.0718 for C1, 0.0735 for C2, 0.0672 for C3, 0.0720 for C4, and 89 for C5. These values serve as a reference for identifying deviations from the minimum desirable performance. By comparing the performance of each node to the negative best solution, decision makers can better assess how far a node is from the worst-case scenario, thus highlighting the relative strengths and weaknesses within the decision-making framework.

TABLE 7. SI Plus, Si Negative, and Ci value

	SI Plus	Si Negative	Ci
CN1	0.0563	0.0228	0.2877
CN2	0.0724	0.0024	0.0326
CN3	0.0730	0.0023	0.0304
CN4	0.0578	0.0174	0.2315
CN5	0.0484	0.0268	0.3562
CN6	0.0000	0.0742	1.0000

Table 7 presents the final evaluation metrics for the six communication nodes (CN1 to CN6), including SI Plus, SI Negative, and Ci values. These values are derived from the relative distance of each node to the positive and negative ideal solutions. SI Plus indicates the distance of each node from the positive ideal solution, with smaller values indicating better proximity. CN6 has the smallest SI Plus (0.0000), indicating perfect alignment with the ideal solution. SI Negative measures the distance from the negative ideal solution, with higher values indicating better performance. CN6 scores higher (0.0742), further confirming its superiority. This analysis identifies CN6 as the most effective

communication node, with CN5 and CN1 as subsequent performers. Nodes CN2 and CN3, with Ci values of 0.0326 and 0.0304, respectively, show the lowest alignment with the ideal solution, suggesting areas for improvement.

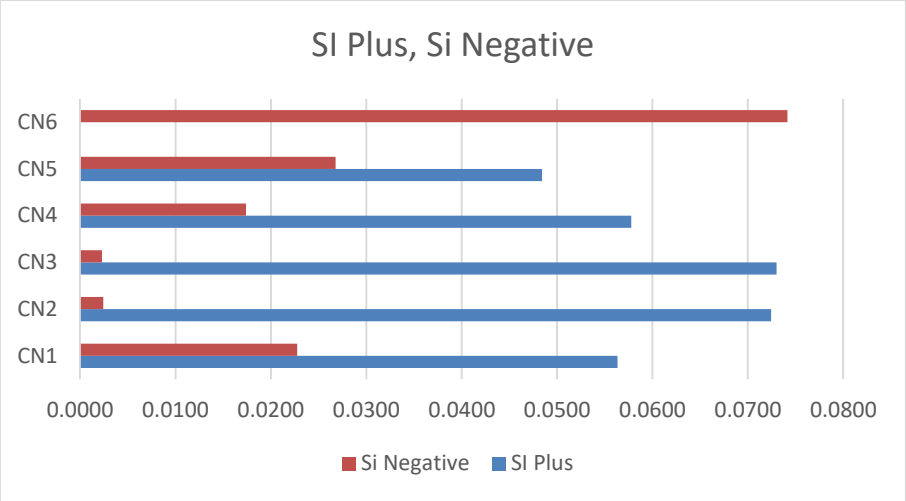


FIGURE 3. SI Plus, Si Negative

The figure 3 analysis of the SI plus (positive best solution) and Si negative (negative best solution) values of the number 3 provides important insights into the performance of the alternatives relative to the best and worst-case scenarios. Among the options, CN6 exhibits exceptional performance with an SI plus value of 0.0000, indicating perfect alignment with the positive best solution, and a high Si negative value of 0.0742, reflecting its significant distance from the negative best scenario. In contrast, CN3 and CN2 show less favorable results, with high SI plus values of 0.0730 and 0.0724, respectively, and low Si negative values of 0.0023 and 0.0024, indicating greater proximity to the negative conditions. Alternatives CN1, CN4 and CN5 exhibit moderate performance, with CN5 standing out slightly due to its relatively low SI plus value (0.0484) and high Si negative value (0.0268). These results highlight CN6 as the most optimal choice, while CN3 and CN2 may require targeted improvements to improve their overall alignment with the best conditions. This dual-metric assessment emphasizes the need for a balanced approach to improving both positive and negative performance dimensions.

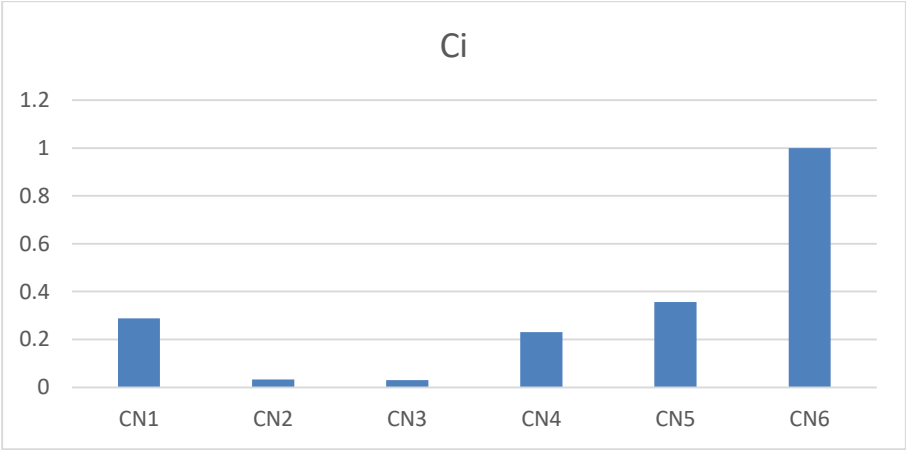


FIGURE 4. Ci value

The Ci values indicate the relative closeness of each alternative to the best solution, with higher values indicating better performance. CN6 has the highest Ci value of 1.0000, indicating a highly optimal choice, while CN5 follows closely with a Ci value of 0.3562, reflecting strong but less optimal performance. CN1 and CN4 show moderate Ci values of 0.2877 and 0.2315, indicating average alignment with the best solution. In contrast, CN2 and CN3 have very low Ci values of 0.0326 and 0.0304, highlighting their relative inefficiency compared to the best solution. These values provide a clear ranking of the alternatives based on their closeness to the best solution.

TABLE 8. Rank

	Rank
CN1	**3**
CN2	**5**
CN3	**6**
CN4	**4**
CN5	**2**
CN6	**1**

Table 8 presents the final rankings of the six communication nodes (CN1 to CN6) based on their performance on the evaluated criteria. The rankings are derived from the Ci values presented in Table 7, where higher Ci values correspond to better performance and higher rankings. CN6 maintains the top position (rank 1), demonstrating its superiority as the most effective communication node, achieving the highest alignment with the best solution. CN5 is in second place (rank 2), demonstrating strong performance, especially in its proximity to the positive best solution. CN1 is in third place (rank 3), indicating moderate performance compared to the other nodes. CN4 takes fourth place (rank 4), followed by CN2 (rank 5) and CN3 (rank 6), which show lower alignment with the best solution. This ranking provides a clear guideline for selecting the most effective communication node, with CN6 emerging as the best choice.

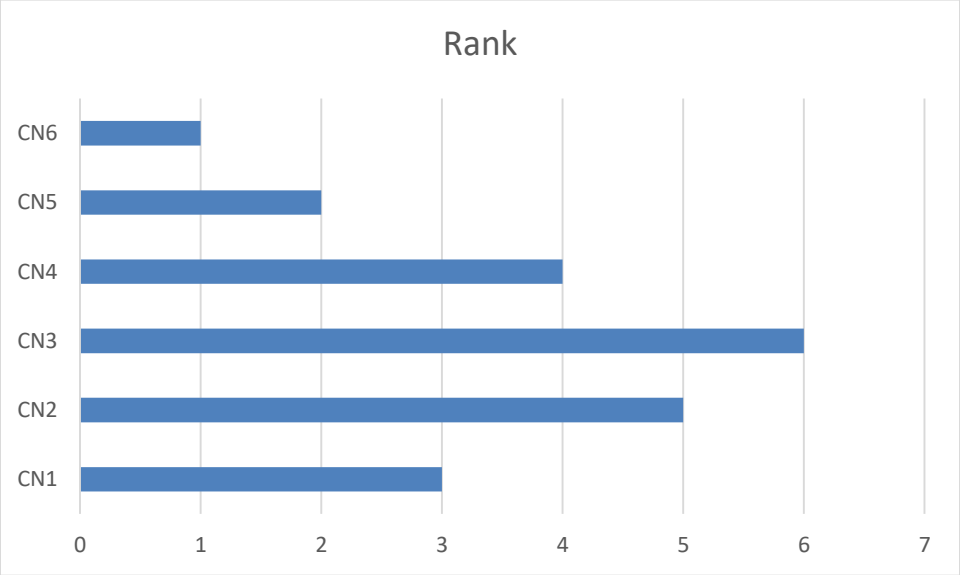


FIGURE 5. Rank

In Figure 5, the rankings of the alternatives are presented based on their Ci values. CN6 is ranked highest (1), indicating that it is the most optimal alternative. CN5 follows with rank 2, showing strong performance but slightly less optimal than CN6. CN1 is ranked 3, showing a moderate performance, while CN4 is ranked 4, indicating a slightly weaker performance compared to CN1. CN2 and CN3 are ranked 5 and 6, respectively, indicating that they are the least optimal choices in this comparison. This ranking further highlights the relative performance of each alternative.

4. CONCLUSION

To assess security risks in communication networks, a comprehensive understanding of critical elements such as communication protocols, node security, network monitoring, cryptography, and security policies is essential. This study used the TOPSIS method to assess security risks in energy management communication networks, emphasizing the need to balance technical, operational, and strategic aspects for secure and reliable network operation. As cyber threats continue to grow in complexity, organizations must proactively secure their communication infrastructure by adopting advanced algorithms and technologies to effectively address emerging vulnerabilities. The dynamic and

interconnected nature of contemporary networks demands innovative strategies to ensure their security and reliability. Visualization has proven to be an invaluable tool for analyzing complex network data, identifying patterns, detecting anomalies, and providing actionable insights to detect vulnerabilities. However, as technology evolves, the challenges posed by cyber threats also increase. To address these challenges, organizations must adopt a comprehensive approach to security, which includes leveraging advanced visualization tools, implementing robust technology measures, fostering a culture of security awareness among employees, and maintaining continuous monitoring to proactively mitigate risks. This study underscores the transformative potential of network security visualization, provides a structured categorization of recent advances, and identifies areas for further research. By addressing these gaps, researchers and practitioners can develop more adaptive and robust solutions to address emerging threats. Looking ahead, integrating visualization with advanced technologies will play a key role in strengthening the security, integrity, and reliability of interconnected systems, thereby safeguarding private and public sector operations in an increasingly digital world.

REFERENCES

[1]. Shiravi, Hade, Ali Shrive, and Ali A. Ghorbanifar. "A survey of visualization systems for network security." IEEE Transactions on visualization and computer graphics 18, no. 8 (2011): 1313-1329.

[2]. Sharafaldin, Imam, ArishAbebi Lashkari, and Ali A. Ghorbanifar. "An evaluation framework for network security visualizations." Computers & Security 84 (2019): 70-92.

[3]. Antipode, Antoinette E., Jibe Yan, Claude Turner, and Dwight Richards. "Visualization tools for network security." Electronic Imaging 28 (2016): 1-8.

[4]. Zhang, Yanking, Yang Xiao, Min Chen, Jungian Zhang, and Hangmen Deng. "A survey of security visualization for computer network logs." Security and Communication Networks 5, no. 4 (2012): 404-421.

[5]. Harrison, Lane, and Aiding Lu. "The future of security visualization: Lessons from network visualization." IEEE Network 26, no. 6 (2012): 6-11.

[6]. Kasemsri, Ramiro Robert. "A survey, taxonomy, and analysis of network security visualization techniques." (2006).

[7]. Nunn ally, Troy, Fulsome Abdullah, A. Seljuk Uluagac, John A. Copeland, and RacemeBeach. "Naves: A recommender system for 3d network security visualizations." In Proceedings of the Tenth Workshop on Visualization for Cyber Security, pp. 41-48. 2013.

[8]. Zhou, Fang fang, Songhua Shi, Ying Zhao, Yeti Huang, and Xing Liang. "Netsecradar: A visualization system for network security situational awareness." In Cyberspace Safety and Security: 5th International Symposium, CSS 2013, Zhangjiajie, China, November 13-15, 2013, Proceedings 5, pp. 403-416. Springer International Publishing, 2013.

[9]. Manxman, Florien, Lorenz Meier, and Daniel A. Kim. "Visualization of host behaviour for network security." In Vessel 2007: Proceedings of the Workshop on Visualization for Computer Security, pp. 187-202. Springer Berlin Heidelberg, 2008.

[10]. Conti, Greg. Security data visualization: graphical techniques for network analysis. No Starch Press, 2007.

[11]. Halo, Lihue, Christopher G. Healey, and Steve E. Hutchinson. "Flexible web visualization for alert-based network security analytics." In Proceedings of the Tenth Workshop on Visualization for Cyber Security, pp. 33-40. 2013.

[12]. Li, Xiao an, Qingxian Wang, Lin Yang, and XiangtanLou. "The research on network security visualization key technology." In 2012 Fourth International Conference on Multimedia Information Networking and Security, pp. 983-988. IEEE, 2012.

[13]. Inert, Michal, Branislav Made, and Susana Dudlákovà. "Data visualization of network security systems." Act Electrotechnica et Informatica 14, no. 4 (2014): 13-16.

[14]. Lakkaraju, Karan, William Yuck, Rant Bearavolu, and Adam J. Lee. "NVisionIP: an interactive network flow visualization tool for security." In 2004 IEEE

[15]. International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583), vol. 3, pp. 2675-2680. IEEE, 2004.

[16]. Yuck, William, and Yean Li. "Internet security visualization case study: Incrementing a network for Net Flow security visualization tools." In 21st Annual Computer Security Applications Conference (ACSAC). 2005.

[17]. Liao, I, Aaron Stiegel, and NitsChula. "Visualizing graph dynamics and similarity for enterprise network security and management." In Proceedings of the seventh international symposium on visualization for cyber security, pp. 34-45. 2010.

[18]. Chen, Honda, Gens he Chen, Erik Blanch, Martin Kruger, and Irma Sitar. "Analysis and visualization of large complex attack graphs for networks security." In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2007, vol. 6570, pp. 32-42. SPIE, 2007.

[19]. Good all, John R. "Introduction to visualization for computer security." In Vessel 2007: Proceedings of the Workshop on Visualization for Computer Security, pp. 1-17. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.
[20]. Alhakami, Wajdi. "Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method." Processes 11, no. 5 (2023): 1366.
[21]. Halo, Lihue, Christopher G. Healey, and Steve E. Hutchinson. "Ensemble visualization for cyber situation awareness of network security data." In 2015 IEEE Symposium on Visualization for Cyber Security (Vessel), pp. 1-8. IEEE, 2015.
[22]. Ball, Robert, Glenn A. Fink, and Chris North. "Home-centric visualization of network traffic for security administration." In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 55-64. 2004.
[23]. Landstorfer, Johannes, Ibo Herrmann, Jan-Erik Stanger, Marian Dark, and Recto Wettach. "Weaving a carpet from log entries: A network security visualization built with co-creation." In 2014 IEEE Conference on Visual Analytics Science and Technology (VAST), pp. 73-82. IEEE, 2014.
[24]. Li, Xiao an, Qingxian Wang, Lin Yang, and Xiangtan Lou. "Network security situation awareness method based on visualization." In 2011 Third International Conference on Multimedia Information Networking and Security, pp. 411-415. IEEE, 2011.
[25]. AbdelMouty, Ahmed M., and Ahmed Abdel-Monem. "Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management." Neutrosophic Systems with Applications 3 (2023): 53-61.
[26]. Nunn ally, Troy. "Advanced visualizations for network security." PhD diss., PhD dissertation, Georgia Institute of Technology, 2014.
[27]. Liu, Xiamen, Yong Sun, Liang Fang, Junpeng Liu, and Longing Yu. "A survey of network traffic visualization in detecting network security threats." In Trustworthy Computing and Services: International Conference, ISCTCS 2014, Beijing, China, November 28-29, 2014, Revised Selected papers, pp. 91-98. Springer Berlin Heidelberg, 2015.
[28]. Alyami, Hashem, Md Tarique Jamal Ansari, Abdullah Alharbi, Wael Alosaimi, Majid Alshammari, Dhirendra Pandey, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Effectiveness evaluation of different IDSs using integrated fuzzy MCDM model." Electronics 11, no. 6 (2022): 859.
[29]. Lu, Liang Fu, Jiao Wan Zhang, Mao Lin Huang, and Lei Fu. "A new concentric-circle visualization of multi-dimensional data and its application in network security." Journal of Visual Languages & Computing 21, no. 4 (2010): 194-208.
[30]. Dymova, Ludmila, Pavel Sevastjanov, and Anna Tikhonenko. "An approach to generalization of fuzzy TOPSIS method." Information Sciences 238 (2013): 149-162.
[31]. Chu, T-C., and Y-C. Lin. "A fuzzy TOPSIS method for robot selection." The International Journal of Advanced Manufacturing Technology 21 (2003): 284-290.
[32]. Karim, Rubayet, and C. L. Karmaker. "Machine selection by AHP and TOPSIS methods." American Journal of Industrial Engineering 4, no. 1 (2016): 7-13.
[33]. Chen, Pengyu. "Effects of normalization on the entropy-based TOPSIS method." Expert Systems with Applications 136 (2019): 33-41.
[34]. Chakraborty, Subrata. "TOPSIS and Modified TOPSIS: A comparative analysis." Decision Analytics Journal 2 (2022): 100021.
[35]. Bhutia, Pema Wangchen, and Ruben Phipon. "Application of AHP and TOPSIS method for supplier selection problem." IOSR Journal of Engineering 2, no. 10 (2012): 43-50.
[36]. Monjezi, Masoud, Hadi Dehghani, T. Narain Singh, Ahmed Reza Sayadi, and Ahamad Gholinejad. "Application of TOPSIS method for selecting the most appropriate blast design." Arabian journal of geosciences 5, no. 1 (2012): 95.