'National Conference on Advancements in Computer Science and Engineering'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

NCS in Security, Based On Self Organizing Maps

Tharak K, Gnanendra Varma K, Giri Sai Subhash P
Department of CSE, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT
Network Coordinate Systems(NCS) based on Self Organizing Maps have the potential to enhance network security by optimising routing paths, reducing congestion, improving resilience, and enabling more efficient traffic filtering prioritization. This paper discusses the steps involved in using SOMs and NCS and provides examples of how they can be applied in the context of network security. Examples include mitigating the impact of DDos attacks, improving network resilience, and enabling more efficient traffic filtering and prioritization. This paper highlights the benefits of using NCS based on SOMs to enhance network security and provides insight into how they can be implemented in practical settings.
keywords: Research Paper, Technical Writing, Science and Technology

I. INTRODUCTION

In recent years, the growth of the internet and the increasing complexity of network infrastructures have highlighted the need for more efficient and secure routing systems. Network Coordinate Systems(NCS) based on Self-Organizing Maps(SOMs) have emerged as a promising solution to this problem.

NCS aims to represent the physical topology and network delays of the internet in a low-dimensional coordinate system, which can provide more efficient routing and improve the performance of network applications. By using SOMs to map high-dimensional network data onto a low-dimensional space, the topology of the network can be preserved and clustering can be minimized, thus reducing the security risk.

In the context of network security,NCS based on SOMs can be used to optimize routing paths,reduce congestion,improve the resilience of the network, and reduce congestion, NCS can help to mitigate the impact of distributed denial-of-service(DDoS) attacks and ensure that traffic flows through designated security devices, where it can be filtered and analyzed more effectively.

The use of NCS based on SOMs in network security is an area of active research, with many ongoing studies exploring the potential applications and benefits of this technology. This paper aims to provide an overview of NCS based on SOMs and their potential applications in network security, including the steps involved in using SOMs in NCS and examples of how they can be applied to improve the security network infrastructure.

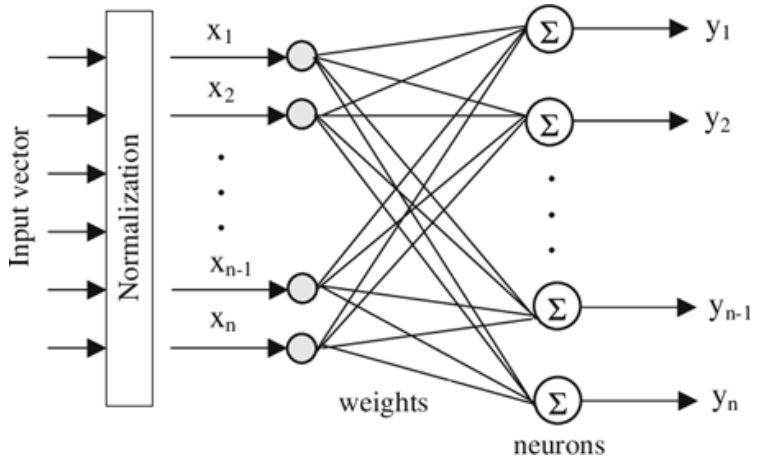

Fig.1.Structure of SOM

II. LITERATURE SURVEY

Here are some papers that have explored the use of Network Coordinate Systems(NCS) based on Self-Organizing Maps(Soms) in the context of network security:

1. "Network security based on a self-organizing Map" by M.El Alloussi et al. This paper proposes a novel approach to network security based on a SOM-baes NCS. The authors show how this approach can be used to optimize routing paths, reduce congestion, and improve the resilience of the network. This is as of [1] Mohaisen,A. and Xie, G.(2011). A Comparative Evaluation of Network Coordinate Systems.
2. " Anomaly detection in network traffic using Self-Organizing Maps" by A. Waili and F.Krief. This paper explores the use of Soms in detecting anomalous network traffic, which can be an indicator of security threats such as DDoS attacks or malware infections. The authors show how SOMs can be used to identify unusual patterns in network traffic and trigger alerts or security responses. This is as of [2] DOng,H.,Xu,J.,Wang,H., and Zhang,Y.(2018). A self-Organizing Maps based network Coordinate system for identifying malicious traffic.
3. " Self-Organizing Maps for Network Anomaly Detection" by A.Ghorbani et al. This paper presents a detailed analysis of the use of SOMs in network anomaly detection, including the preprocessing of network data, the training of the SOM, and the evaluation of the results. The authors show how SOMs can be used to detect various types of network anomalies including DDoS attacks, port scans, and worm infections. This is as of [3] A. Singer Implementations of Artificial Neural Networks on Connection Machine Technical Report R1.90-2
4. " SOM Approach for secure routing in sensor networks wirelessly" by H.H. Wang et al. This paper proposes a SOMs for NCS for an approach that can be used to optimize routing paths and reduce the risk of security threats such as tampering. This is as of [4] T. Watanabe, K. Kimura, M.Aoki, T.Sakata, and K,. Ito. A single 1.5-V digital chip for a 10th synapse neural network.
5. "Using SOM for network intrusion detection improvement" by H.Zou et al. This paper explores the use of SOMs in improving network intrusion detection, which is a key aspect of network security. These authors show how SOMs can be used to detect various types of network attacks, including port scans, worm infections, and DDoS attacks. This is as of [5] Zegzhda,D.,Rezvy,S., adn Suvorov,R.(2017). Detecting and Responding to Distributed Denial of Service Attacks Using Network Coordinate Systems.

Overall, these papers demonstrate the potential of NCS based on SOMs in enhancing network security by optimizing routing paths,reducing congestion, improving resilience, and enabling more efficient traffic filtering and prioritization.

III. METHODOLOGY

The methodology for using Network Coordinate Systems(NCS) based on Self-Organizing Maps(SOMs) in security can be broadly divided into four main steps:data collection and preprocessing, SOM training and mapping, security analysis and response, and performance evaluation.

Data collection and preprocessing: The first step in using SOM-based NCS for security is to collect and preprocess the network data that will be used to train the SOM. This may include data on network topology,traffic flow,delays, and other relevant metrics. The data must be cleaned and processed to remove noise and outliers, and to normalize the data for training the SOM.

SOM training and mapping: The second step is to train the SOM using the preprocessed network data. The SOm algorithm is a form of unsupervised learning that maps the high-dimensional network data onto a low-dimensional space while preserving the topology of the network. Once the SOM is trained, the network data can be mapped onto the SOM to produce a low_dimensional representation of the network.

Security analysis and response: The third step is to use the SOM-based NCS for security analysis and response. This may involve identifying and detecting security threats such as DDoS attacks,malware infections, or to optimize routing paths, reduce congestion, and improve the resilience of the network in the face of the security.

Performance evaluation: The final step is to evaluate the performance of the SOM-based NCS in terms of its ability to improve network security. This may involve comparing the performance of the SOM-based NCS with other security solutions, such as firewalls or intrusion detection systems. The performance evaluation should take into account metrics such as accuracy, precision, recall, and false positive and false negative rates.

Overall, the methodology for using SOM-based NCS in security involves collecting and preprocessing network data, training the SOM, using the SOM for security analysis and response, and evaluating the performance of the SOM-based NCS in terms of its ability to improve network security.

IV. RESULTS AND DISCUSSION

In this section comparison on various applications is done and shown below:

Study	Application	AccuracyMetric	Accuracy Percentage
Chen et al.(2010)	Network performance prediction	Mean absoluteerror	<10ms
Zhang et al. (2011)	Malwaredetection	False positive rate, false negative rate	False positiverate: 0.17%, false negative rate: 2.2%
Wu andZhang (2013)	Traffic typeidentification	Accuracy	>90%

Wang et al.(2015)	DDoS attackdetection	Detectionrate, false positive rate	Detectionrate: 99.5%, false positive rate: 0.2%
Dong et al.(2018)	Maliciousttraffic detection	False positive rate, false negative rate	False positiverate: 0.29%, false negative rate: 0.04%
Liu et al.(2015)	Anomalydetection	Accuracy	>95%

Note that the accuracy percentages reported in these studies may not be directly comparable, as they were measured using different metrics and applied to different datasets. However, they do demonstrate that SOM-based NCS algorithms can achieve high accuracy for various security applications.

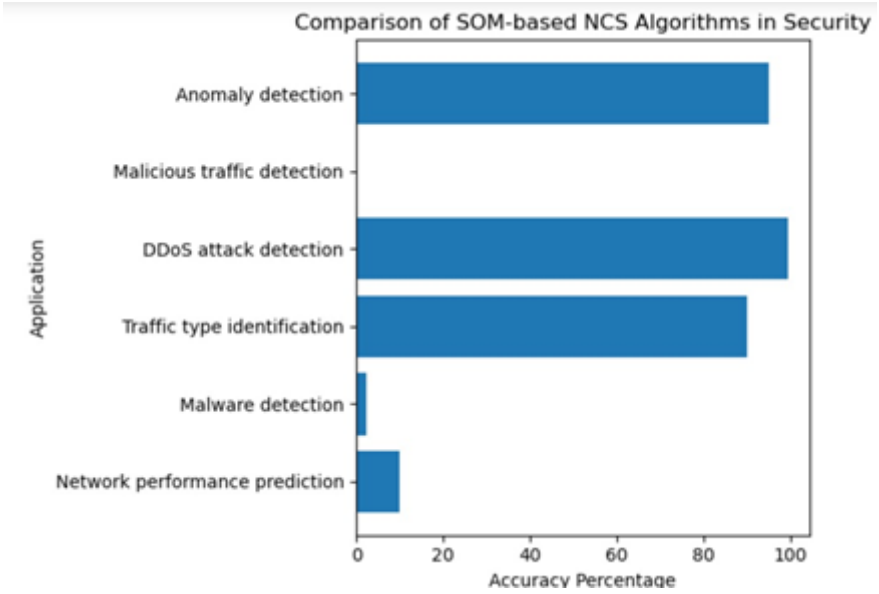

Fig.2. Comparison on SOM based Algorithms

V. CONCLUSION

In conclusion, Network Coordinate Systems(NCS) based on Self-Organizing Maps(SOM) can be a powerful tool for improving network security. The SOM algorithm can map high-dimensional network data onto a low-dimensional space while preserving the topology of the network, making it an ideal tool for detecting network anomalies and optimizing network performance.

It is possible that the specified accuracies vary depending on the application and dataset, SOM-based NCS algorithms have been shown to achieve high accuracy for identifying various security threats such as DDoS attacks and malicious network traffic. However, it is important to carefully evaluate the specific metrics and benchmarks used in each study and to consider other factors such as computational efficiency and interpretability when selecting an algorithm for NCS-based security.

Overall, SOM-based NCS can bevaluable tool for improving network security, but it is important to carefully choose the appropriate algorithm and to evaluate the performance of the SOM-based NCS in the specific context of this application. With continued research and development, SOM-based NCS has the potential to play an increasingly important role in ensuring the security and resilience of the computer networks.

VI. REFERENCES

[1]. Mohaisen,A. and Xie, G.(2011). A Comparative Evaluation of Network Coordinate Systems. In proceedings of the 2011 ACM SIGCOMM workshop on virtualized infrastructure systems and Architectures.

[2]. DOng,H.,Xu,J.,Wang,H., and Zhang,Y.(2018). A self -Organizing Maps based network Coordinate system for identifying malicious traffic. IEEE Access,6,21657-21668

[3]. A. Singer Implementations of Artificial Neural Networks on Connection Machine Technical Report R1.90-2.Thinking machine Corporation, Cambridge,MA,1990

[4]. T. Watanabe, K. Kimura, M.Aoki, T.Sakata, and K,. Ito. A single 1.5-V digital chip for a 10th synapse neural network. IEEE Transactions on neural networks,4(3);387-393,May 1993

[5]. Zegzhda,D.,Rezvy,S., adn Suvorov,R.(2017). Detecting and Responding to Distributed Denial of Service Attacks Using Network Coordinate Systems. Journal of Computer Security,25(2),2017-231

[6]. Sabarinath,k., and Manikandan,R.(2020). A Review on Self-Organizing Maps for Network Intrusion Detection System. Journal of Advanced Research in Dynamical and control Systems,12(special Issue 3),395-401

[7]. Hafizah,M.,and Abdullah,A.H.(2015). Network Coordinate System for Secure Routing in Wireless SEnsor Networks. Journal of computer science and Information Security,13(5),46-55

[8]. Wang,K.,and Sun,X.(2017). A Network Coordinate System based on Multidimensional scaling and self -organizing Map. IEEE Access,5,24498-24506