Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 127–136, DOI 10.12694/scpe.v25i1.2280

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN ELECTROMECHANICAL INFORMATION SECURITY SITUATION AWARENESS SYSTEM

XIANGYING LIU*, ZHIQIANG LI†, ZHUWEI TANG‡, XIANG ZHANG§, AND HONGXIA WANG¶

Abstract. The information security situational awareness system is proposed in this paper to leverage big data and artificial intelligence (AI) to enhance information security situation prediction. Deep learning techniques, specifically the long short-term memory recurrent neural network (LSTM-RNN), predict security situations using complex non-linear and autocorrelation time series data from current and past system conditions. Additionally, the study incorporates the variant gated recurrent unit (GRU) within the LSTM-RNN framework. A comprehensive experimental analysis is conducted, comparing various methods, including LSTM, GRU, and others, to assess and compare their predictive performance. The experimental results reveal that LSTM-RNN demonstrates a commendable level of predictive accuracy on the test dataset, with a mean absolute percentage error (MAPE) of 8.79%, a root mean square error (RMSE) of 0.1107, and a relative root mean square error (RRMSE) of 8.47%. Both LSTM and GRU exhibit exceptional predictive accuracy, with GRU offering a slightly faster training speed due to its simplified architecture and fewer trainable parameters. Overall, this research highlights the potential of AI-based methodologies in constructing robust information security situational awareness systems.

Key words: Network security, Situational awareness system, LSTM RNN, GRU, Accuracy

1. Introduction. The beginning of the Internet era has led to significant changes in people's lives. Various industries are continually evolving due to the Internet's influence. Concurrently, there is a growing prevalence of network security threats in the Internet age. Consequently, enhancing research on information security situational awareness systems is authoritative. Current research on enterprise information security situational awareness systems and the prevailing state of information security protection highlights that enterprise information security often operates within a passive cycle of detection and remediation. Typically, enterprises install defence systems tailored to their unique operational characteristics and production nature. They proactively identify hidden vulnerabilities and risks within their network systems through risk assessments and penetration tests, followed by targeted mitigation measures [18].

When suspicious activities or attacks are detected, comprehensive investigations and analyses are conducted, encompassing the examination of security device logs and network traffic data. This process aims to determine the behaviour's specific nature and severity and resolve these issues as comprehensively as possible. Within this passive framework of information security defence in enterprises, the predominant focus often lies on the defensive aspects, with limited attention directed toward understanding and analyzing the root causes of attacks. Investment and research in system repair tend to be relatively modest, primarily relying on passive remedies in the form of patches provided by product manufacturers [6].

Simultaneously, enterprises persist in refining and enhancing their defence strategies to bolster their systems' resilience against external threats. Advances in computer technology and the growing understanding of information security have led to effective optimizations in information security defence measures. Many enterprises have implemented integrated security systems encompassing network antivirus, endpoint management, security auditing, access controls, and vulnerability discovery. These integrated systems ensure the secure and reliable

*Tangshan Sanyou Chemical Co., Ltd., Thermoelectric Branch, Tangshan, Hebei, 063305, China (Corresponding author: xiangyingliu8@126.com)
†Tangshan Sanyou Chemical Co., Ltd., Thermoelectric Branch, Tangshan, Hebei, 063305, China
‡Tangshan Sanyou Chemical Co., Ltd., Thermoelectric Branch, Tangshan, Hebei, 063305, China
§Tangshan Sanyou Chemical Co., Ltd., Thermoelectric Branch, Tangshan, Hebei, 063305, China
¶Tangshan Sanyou Chemical Co., Ltd., Thermoelectric Branch, Tangshan, Hebei, 063305, China

operation of enterprise activities, reduce information security risks, enable unified warning systems, centralize management and traceability, and mitigate the impact of information risks on routine business operations [17].

The Internet era has ushered in a surge of various network security threats, with a noticeable upward trajectory. The frequency of cyberattacks targeting countries and political entities is rising annually. Consequently, the need to swiftly address external threats affecting nations, organizations, businesses, and individuals is becoming increasingly urgent. This article primarily focuses on modern enterprises in response to the pressing network security issue. It delves into contemporary challenges, such as network attacks and data breaches, that are prevalent today. Furthermore, it underscores the importance of exploring and proposing solutions for these issues. Given this context, conducting an in-depth examination of the application of big data and artificial intelligence technology in information security situational awareness systems holds significant practical relevance [8].

In recent years, modern enterprises have increasingly relied on networks for their day-to-day operations. They depend on high-speed and secure information technology, significantly boosting work efficiency. However, a traditional approach of "defence, detection, and remediation" prevails when managing and controlling enterprise information security. Indeed, this approach proves valuable, especially in scenarios like information security penetration tests or risk assessments. However, it's noteworthy that during the optimization of information security processes, most enterprises allocate over 95% of their resources to defence, leading to a predominantly reactive approach to information security [10].

In daily operations and maintenance, enterprise information security initiatives continue to expand. Various security systems, including terminal controls, network antivirus software, and vulnerability scanning tools, are continually being implemented to safeguard business operations. However, a critical issue arises from the lack of a unified and integrated prevention and control system across these disparate security systems. This fragmentation hinders the achievement of unified management for early warning of information security threats and traceability of security issues. Data collection and perception systems rely on various network traffic and logs in enterprise information security management. During specific data collection, it's crucial to tailor the process to the unique scale and circumstances of the enterprise. This entails selecting and gathering different well-suited data types and enhancing the effectiveness and accuracy of the data collection process. Moreover, when dealing with specific traffic processing tasks, the system can leverage its technology to reconstruct data, conduct precise data analysis, and disseminate the acquired specific data. This approach facilitates other enterprises' data storage and utilization through the enterprise platform, fostering collaboration and knowledge sharing in information security [13].

After processing diverse types of network traffic data and other information, it becomes imperative to delve deeply into the data's content, proactively identifying internal issues and risks within the enterprise while promptly resolving them. This process involves two key components: Artificial Intelligence Detection of Malicious Code Technology: This technology is constructed through artificial search engines, drawing from an extensive pool of malicious and normal software samples. It seeks to identify standard information data features across different samples and build effective machine-learning models for the security scanning of unknown programs [5].

Application of Artificial Intelligence Virus Detection Technology: This application within enterprise information security situational awareness systems enables efficient identification and timely detection of viruses. It plays a pivotal role in mitigating computer system damage caused by viruses. Computer viruses have evolved and diversified in recent years, posing a significant threat to normal computer system operations. By integrating artificial intelligence virus detection technology with big data technology, enterprises can enhance their ability to detect and respond to viruses. Employing multiple virus localization methods further elevates the efficiency and accuracy of virus detection, rendering it a more precise and scientifically driven process [2].

The network security situational awareness model represents a comprehensive framework encompassing various steps and processes in achieving situational awareness within a network security context. Figure 1.1 visually illustrates this ecological framework, comprehensively representing the complex processes involved in understanding network security situations. This illustration is a valuable reference point for grasping the complexity and interconnectedness of various network security situational awareness elements. As technology and our understanding of network security continue to evolve, the development and refinement of this model

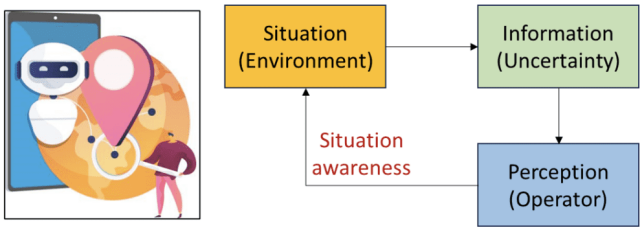

Fig. 1.1: Framework of situation awareness model

remain an ongoing and dynamic process. This continuous development reflects the ever-changing landscape of network security challenges and the need for adaptive strategies and tools to address them effectively [3].

The paper is systematically structured into five primary sections, including an introduction. Section 2 conducts an extensive literature review, providing a comprehensive understanding of previous research in information security situational awareness and the utilization of artificial intelligence within electromechanical systems. In Section 3, the paper investigates the proposed methodology, explicitly focusing on implementing the LSTM RNN with GRU within electromechanical information security. Section 4 is dedicated to the presentation and thorough discussion of the results obtained from the experimentation and analysis, explaining the efficacy of the proposed approach. Finally, Section 5 offers concluding remarks summarizing the study's primary findings and contributions.

2. Literature Review. In recent years, information security practices within enterprise units have exhibited remarkable consistency, marked by a recurring and passive pattern encompassing defence, detection, and remediation. This established procedure typically commences with the execution of penetration tests or extensive risk assessments meticulously devised to unearth vulnerabilities and latent risks lurking within information and network systems. Once these vulnerabilities are pinpointed, they trigger precise remedial actions to fortify the system's defences. A comprehensive response protocol is initiated in the unfortunate event of a cyberattack. This entails thoroughly recording and analyzing pertinent network traffic data and security device logs to unveil the intricate intricacies of attack behaviours [1].

In the framework of passive information security defence, it's worth highlighting that 95% of resources are allocated towards bolstering defensive measures. These measures are meticulously architected and implemented to thwart potential threats. However, only a meagre 5% of resources are dedicated to delving into the multifaceted realm of attack defence. This disproportionate resource distribution underscores the predominant emphasis on safeguarding against potential threats while often sidelining the comprehensive understanding and proactive management of the root causes behind these threats. It is within this context that the cybersecurity practices of the industry have predominantly unfolded in recent times [9].

The remediation process primarily revolves around applying various patches provided by the original manufacturers of the products or equipment. These patches are essential for addressing and rectifying vulnerabilities and weaknesses identified within the system. However, it's important to note that remediation efforts extend beyond patch management. They encompass an ongoing commitment to refine and fortify defensive measures, continually enhancing the overall security posture of enterprise units. Within the landscape of traditional IT network security situational awareness technology, there has been notable progress and research advancement. Assessment methods in this domain have matured considerably, offering a solid theoretical foundation for conducting security situation assessments, especially within industrial control networks. These well-established methods provide valuable guidance for assessing the security posture of networks [16].

One of the prominent drawbacks of these methods is their reliance on a single source of information, which can lead to a narrow perspective on the security landscape. Additionally, implementing these methods often entails significant time and resource investments, making them resource-intensive. Moreover, subjectivity can creep into the assessment process, introducing potential biases. Lastly, while these methods are valuable, they may exhibit limited accuracy in assessing modern network security threats' complex and dynamic nature. Many of these methods rely on manual parameter configuration or calculate overall network risk based solely on host

nodes, which can oversimplify the intricate nuances of network security [4].

This article embarks on its investigative journey by predicting the network security situations. The initial step involves scrutinizing whether it is indeed possible to forecast these situations accurately. Once the feasibility of prediction is established, the article proceeds to assess the limitations inherent in traditional prediction methodologies. A sophisticated solution called Long Short-Term Memory Recurrent Neural Networks (LSTM RNN) is introduced to address the limitations. LSTM, a deep learning model, is harnessed to predict network security situations. In parallel, the article incorporates the Gated Recurrent Unit (GRU) algorithm, renowned for its efficiency in achieving results comparable to LSTM but with significantly shorter training times [14].

Following the implementation of LSTM, GRU, and other widely used prediction techniques, the article rigorously conducts experiments and analyses the results. This comprehensive assessment reveals that LSTM and GRU outperform their counterparts in terms of prediction accuracy. These two models shine in their ability to not only account for the inherent nonlinearity of the data but also to consider the crucial aspects of autocorrelation and timing within the data. In contrast, other methods are constrained by data stationarity, the degree of data correlation, model parameter selection, noise levels, and the choice of prediction step size. Notably, LSTM and GRU excel in prediction accuracy and exhibit remarkable training speed efficiency, making them capable of real-time prediction – a highly sought-after quality in network security prediction [7].

A novel methodology in big data and artificial intelligence technology approach lies in handling complex nonlinear and autocorrelation time series data derived from current and historical values about system situations. To achieve its predictive goals, the study harnesses the power of the long short-term memory recurrent neural network (LSTM-RNN), a prominent component of deep learning known for its aptitude in handling sequential data. Furthermore, to enhance the predictive capabilities within the LSTM framework, the study incorporates the variant Gated Recurrent Unit (GRUs). This addition is noteworthy as it contributes to refining and optimizing the prediction process, particularly in scenarios where efficiency and accuracy are paramount [12].

A series of experiments are conducted to validate and benchmark the effectiveness of the proposed methodology. These experiments facilitate a comprehensive comparative analysis of the prediction outcomes obtained from LSTM, GRU, and other established prediction methods. Through this rigorous assessment, the study aims to provide insights into each method's relative strengths and weaknesses, shedding light on their applicability and potential contributions to the information security situational awareness field.

3. Investigation Methods.

3.1. Network security situation prediction based on LSTM. Network security situation prediction represents the pinnacle of situational awareness, and its precision empowers administrators to enact appropriate security measures. This prediction hinges on a foundation of situation assessment, which produces a situational value. These situational values accumulate into a time series through continual assessments over time. Given the intricate nature of network security situations and the inherent unpredictability of attacks, this situational sequence takes the form of a non-linear sequence. It is essential to acknowledge that this situational sequence is both non-linear and characterized by autocorrelation. Recognizing these features within the prediction data aids in selecting accurate prediction methods.

Traditional neural network methods like BP and RBF exhibit robust non-linear mapping capabilities. However, in their network model, layers are fully connected, but nodes within each layer lack interconnections. This structure lacks time sequence information. Consequently, traditional neural networks struggle to predict time sequences effectively. The Grey Prediction model necessitates that the function derived from the original discrete data be a smooth discrete function. Yet, when the network is under attack, the function formed by the situational sequence isn't sufficiently smooth. Despite considering the nonlinearity and timing of the situational sequence, the Grey Prediction model faces challenges in predicting time series with significant fluctuations.

Support Vector Machines are more suitable for handling small samples and are less adept at managing large-scale data. Moreover, they don't account for the timing of the situational sequence. While improvements can enhance the prediction accuracy of the mentioned methods, this article seeks a comprehensive approach that accommodates the characteristics of the situational sequence. In this pursuit, Recurrent Neural Networks (RNN) within deep learning emerge as a promising solution. RNNs can effectively address both nonlinearity and timing in the data. Moreover, RNNs suffer from the issue of gradient disappearance, prompting the development of Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN) to mitigate this challenge.

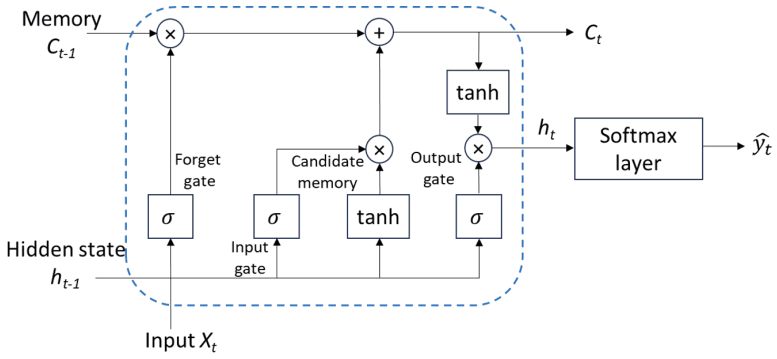

Fig. 3.1: Framework of situation awareness model

This article introduces the mathematical model of LSTM-RNN and the variant Gated Recurrent Unit (GRU) within the LSTM framework. Both LSTM-RNN and GRU are subsequently applied in predicting network security situations.

Long Short-Term Memory Recurrent Neural Networks, abbreviated as LSTM-RNN or simply LSTM, belong to a class of recurrent neural networks designed to enhance long-term and short-term memory capabilities. They excel in retaining knowledge over extended periods and have the capacity for sustained long-term learning. LSTM effectively addresses the gradient disappearance inherent in conventional RNNs, making it a deep learning technique with significant developmental potential. Its applications span various domains, including stock prediction, disease forecasting, language translation, image analysis, and more. LSTM enhances its structure by incorporating gates that regulate the flow of information. When a gate is open, the current neuron receives input from the preceding neuron, whereas a closed gate prevents this interaction. It's through these gates that LSTM achieves its exceptional long and short-term memory capabilities.

The network architecture of LSTM has introduced notable enhancements within the hidden layer of traditional RNNs. Instead of using hidden neurons, LSTM employs memory units. Each memory unit comprises one or more memory cells and incorporates three fundamental "gates", essentially non-linear summation components. These three "gates" are the Input, Output, and Forget gates. The mathematical model of LSTM is systematically introduced in this article, offering a step-by-step breakdown.

Breaking down the LSTM structure can make it appear less intricate. The primary objective of LSTM is to regulate information flow to enable long-term information retention. One straightforward approach to understanding LSTM is realizing the dot product of two matrices of equal dimensions. If the matrix values fall within the range of [0, 1], it can be interpreted as '0' indicating suppression and '1' indicating activation. With this design goal in mind, it becomes evident that the information within the Memory Cell corresponds to the horizontal line in Figure 3.1.

The following are the various gates of the LSTM RNN security awareness system [11].

(1) Forget gate

The forgetting gate controls the influence of the Memory Cell information of the previous moment on the Memory Cell information of the current moment. The oblivion gate is determined jointly by the output h_{t-1} of the previous moment and the input x_t of the current moment. The function formula of the gate f_t is as follows:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right) \tag{3.1}$$

σ is the sigmoid function, which is mapped to $[0, 1]$, h_{t-1} represents the output of memory cells at the previous time, x_t represents the input at the current time, W_* is the coefficient matrix, b_* is the bias matrix.

(2) Input gate

The input gate controls the input information's contents that can affect the current memory cell. The input information includes the output h_{t-1} of the previous time and the input x_t of the current time. The function

formula of the input gate i_t is given by

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right) \tag{3.2}$$

Equation (3.3) of $\widetilde{C_t}$ can be obtained from the standard of RNN:

$$\widetilde{C_t} = \tanh\left(W_C \cdot [h_{t-1}, x_t] + b_C\right) \tag{3.3}$$

After passing the above two gates, the state of memory cells at this time is as follows:

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C}_t \tag{3.4}$$

where * represents the multiplication of matrix elements.

(3) Output gate

The output gate determines the output content in memory cells and the function of the output gate. o_t is expressed as

$$o_t = \sigma\left(W_o \cdot [h_{t-1}, x_t] + b_o\right) \tag{3.5}$$

The output information h_t at the current time is given by:

$$h_t = o_t * \tanh\left(C_t\right) \tag{3.6}$$

The description above pertains to the conventional LSTM, but numerous LSTM variants exist. One widely adopted variant is the Gated Recurrent Unit (GRU). GRU combines the memory cell state and hidden state similar to LSTM but with fewer gates, maintaining the effectiveness of LSTM. Additionally, GRU boasts a more straightforward structure and requires less computation time than LSTM. In GRU, the forgetting and input gates are consolidated into a single update gate, responsible for governing the influence of the previous moment's state information on the current moment's state.

The mathematical model of GRU is shown in Equation (3.7):

$$\begin{aligned} z_t &= \sigma\left(W_z \cdot [h_{t-1}, x_t]\right) \\ r_t &= \sigma\left(W_r \cdot [h_{t-1}, x_t]\right) \\ \tilde{h}_t &= \tanh\left(W \cdot [r_t * h_{t-1}, x_t]\right) \\ h_t &= (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \end{aligned} \tag{3.7}$$

where the update gate is z_t and the reset gate is r_t.

3.2. Network security prediction experiment based on LSTM. LSTM represents a neural network model well-suited for mining non-linear temporal data. In this article, LSTM is harnessed for predicting network security situations. The process commences by delineating the precise task requirements for situation prediction. This involves an analysis of the experiment-supported scenarios and the intrinsic characteristics of the situational data. Subsequently, the article provides an overview of the initial construction process for the LSTM prediction model, encompassing aspects like model architecture and strategic parameters. Lastly, the constructed LSTM model is employed in prediction experiments, and the results are subjected to comparative analysis against other models.

3.2.1. Experimental subjects and requirements. This article employs an attack simulation scenario to enhance its research methodology and practical applicability. To simulate a real-world cybersecurity incident, the researchers utilize IDS informer software to arrange a Denial of Service (DoS) attack scenario, a commonly encountered threat in information security. The attack is designed to mimic malicious performers' strategies and techniques to disrupt network services. To gather relevant data and comprehensively capture the evolving security situation, we have collected the data in discrete sets at 10-minute intervals, resulting in 1000 distinct data points over a specified period.

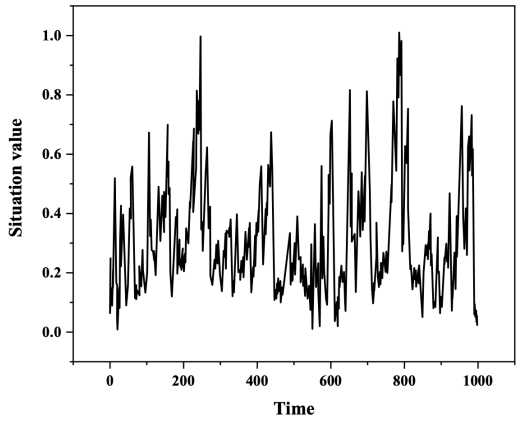

Fig. 3.2: Dynamic visualization of normalized network security systems

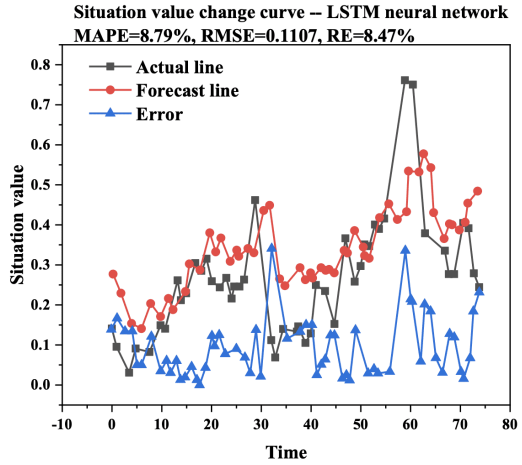

Fig. 3.3: Situation prediction results of LSTM

The situational value, a crucial metric for understanding the evolving security landscape, is meticulously computed using the established network security situational index. This index is based on a well-defined framework considering various critical factors and parameters contributing to the overall security posture. Subsequently, the calculated situational values are employed to construct a chronological change curve, visually depicting the temporal evolution of the security situation. As illustrated in Figure 3.2, the resulting curve provides a dynamic representation of how the security situation unfolds over time. This empirical approach and visualization technique give valuable insights into the nature of the attack, its impact on the network, and the effectiveness of the proposed security measures.

Figure 3.2 clearly illustrates that the ship system's normalized network security situation curve exhibits significant volatility and nonlinearity. To achieve precise situation value prediction, it's imperative to thoroughly extract timing information from existing data and comprehend its underlying mechanism via a model. In this context, the initial 925 situation values are designated as the training set, while the remaining 75 situation values constitute the test set. The input comprises historical situation values, and the output consists of the predicted situation values.

3.2.2. LSTM modeling. A three-layer LSTM with a unidirectional loop is designed to accomplish the prediction task. To optimize the applicability of the constructed LSTM, it is crucial to scrutinize its parameter configuration and the strategies implemented for learning and training. The subsequent section offers a concise exploration of these critical aspects. The LSTM-RNN represents a typical Many to One model, wherein the input consists of data from the previous moment, and the output comprises the predicted value for the subsequent moment's data. Given the enduring nature of information security threats, security situation data often exhibits prolonged temporal correlations. Hence, it is advisable to set a relatively large input dimension.

Since LSTM inherently excels at depicting long-term dependencies, increasing this value does not negatively impact model effectiveness; instead, it enhances the breadth of information extraction. Here, we set the initialization value to be equal to 30. To mitigate issues like gradient explosion or vanishing gradients and improve the efficiency of training a multi-layer model, we employ the Xavier initialization strategy for initializing the parameters of the recurrent network (LSTM-RNN) and the output nested feedforward multi-layer network (MLP) [15]. Given the limited training data, we have introduced the Dropout strategy to aid training and prevent overfitting. Additionally, we employ the Adam optimization algorithm in this experiment to ensure the efficiency of neural network training. The mean square error (MSE) is the optimization objective during training.

4. Simulation Results and Discussion. The Keras development framework is utilized efficiently to implement the designed LSTM model. Through a rigorous and exhaustive training process, the LSTM-RNN model is unlocked to generate predictions for situational data. Figure 3.3 is the culmination of the activities, providing a striking visual representation of the proposed predictive model's outcomes. This graphical representation illustrates the ability of the proposed model, as it investigates network security situations and offers valuable insights into potential threats. These predictions are a valuable asset, supporting information security and situational awareness within the context of our study.

The LSTM model has demonstrated remarkable predictive accuracy on the test dataset by its impressive performance metrics: a mean absolute percentage error (MAPE) as low as 8.79%, an exceptionally minimal root mean square error (RMSE) of 0.1107, and a mere 8.47% relative error (RE). This article conducted a comprehensive series of comparative experiments to ensure a thorough evaluation of the current model's performance. These experiments encompassed the utilization of several well-established prediction methods, including linear regression (LR), support vector regression (SVR), backpropagation (BP) neural networks, and GRU, among others. The findings and invaluable insights from these comparative experiments have been presented and visually explained in Figures 4.1 to 4.5. The comprehensiveness of these experiments offers valuable insights into the respective strengths and weaknesses of different prediction methods, ultimately reinforcing the LSTM model's resilience and effectiveness within the domain of information security situational awareness.

The discussed results indicate that LSTM and GRU exhibit higher prediction accuracy than other methods. This superiority starts from the fact that these two models account for data nonlinearity and consider data autocorrelation and timing. In contrast, other methods are constrained by data stationarity, data correlation, model parameter selection, noise levels, and the choice of prediction step size. LSTM and GRU perform exceptionally well, and their prediction accuracy is on par. GRU, in particular, benefits from its more straightforward structure and fewer training parameters, resulting in a slightly faster training time than LSTM. Specifically, the training time for LSTM is 18.9 seconds, while GRU takes 18.5 seconds. Moreover, both LSTM and GRU demonstrate rapid prediction time consumption at the millisecond level.

5. Conclusion. This article explores a method for predicting network security situations, analyzing their predictability with a focus on nonlinearity and time series characteristics. Experimental comparisons between LSTM-RNN, GRU, and existing methods reveal that LSTM exhibited robust prediction accuracy on the test data, with MAPE at 8.79%, RMSE at 0.1107, and RE at 8.47%. Both LSTM and GRU exceeded other methods, offering similar prediction accuracy. With its more straightforward structure and fewer training parameters, GRU is slightly faster training times (18.5 seconds compared to LSTM's 18.9 seconds). Notably, both LSTM and GRU achieved millisecond-level speed in predictions, satisfying real-time demands. These findings underscore the potential for improved modeling of complex network systems by addressing practical challenges and enhancing each stage. Furthermore, comprehensively representing knowledge is vital in network environments with limited local knowledge. Extending the confidence rule-based identification framework to

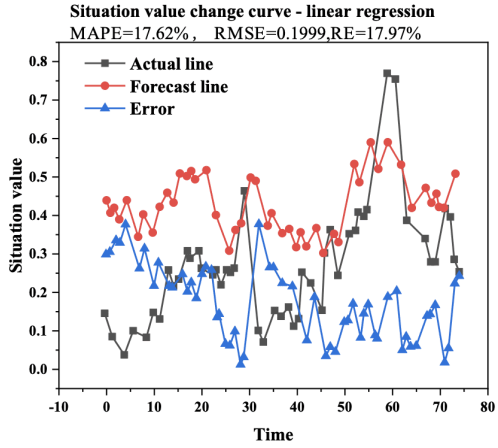

Fig. 4.1: Prediction results of linear regression method

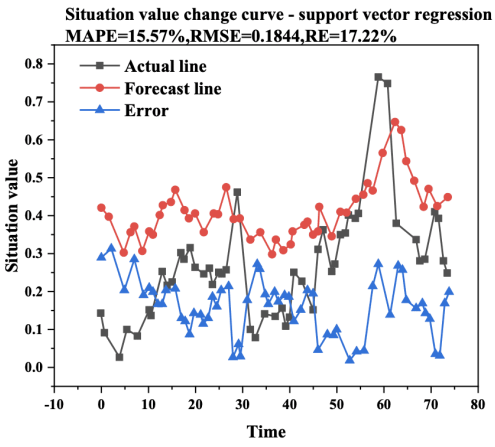

Fig. 4.2: Prediction results of support vector regression

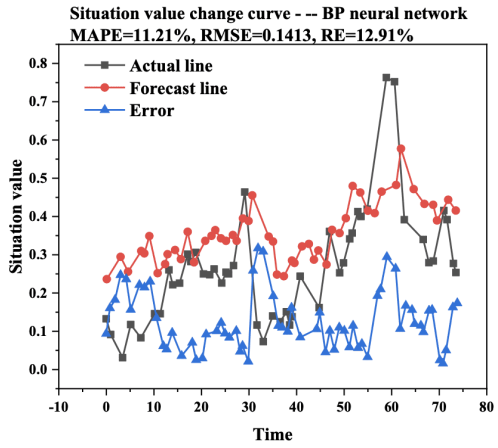

Fig. 4.3: Prediction results of back propagation (BP) neural networks

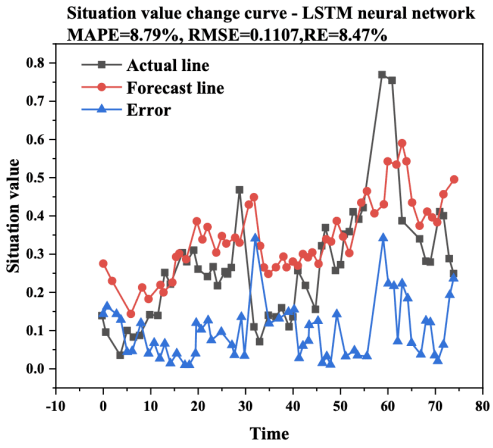

Fig. 4.4: Outcomes of the LSTM neural network's predictions

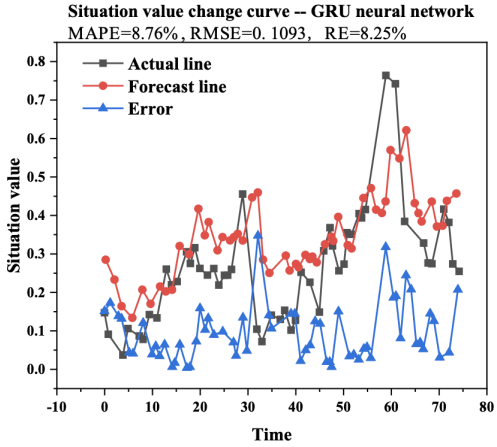

Fig. 4.5: Prediction results of gated recurrent unit

include the power set promises enhanced prediction outcomes. Future research will focus on refining observable value selection and further developing theories underpinning the implicit confidence rule base model within the power set identification framework, advancing network security situational awareness and prediction.

REFERENCES

[1] M. Abbasi, A. Shahraki, and A. Taherkordi, *Deep learning for network traffic monitoring and analysis (ntma): A survey*, Computer Communications, 170 (2021), pp. 19–41.
[2] Y. S. Afridi, K. Ahmad, and L. Hassan, *Artificial intelligence based prognostic maintenance of renewable energy systems: A review of techniques, challenges, and future research directions*, International Journal of Energy Research, 46 (2022), pp. 21619–21642.
[3] M. Alshehri, *Blockchain-assisted cyber security in medical things using artificial intelligence*, Electronic Research Archive, 31 (2023), pp. 708–728.
[4] G. K. Bharathy and B. Silverman, *Applications of social systems modeling to political risk management*, Handbook on Decision Making: Vol 2: Risk Management in Decision Making, (2012), pp. 331–371.
[5] Z. Cui, L. Du, P. Wang, X. Cai, and W. Zhang, *Malicious code detection based on cnns and multi-objective algorithm*, Journal of Parallel and Distributed Computing, 129 (2019), pp. 50–58.
[6] L. Franchina, G. Inzerilli, E. Scatto, A. Calabrese, A. Lucariello, G. Brutti, and P. Roscioli, *Passive and active training approaches for critical infrastructure protection*, International Journal of Disaster Risk Reduction, 63 (2021), p. 102461.
[7] R. Fu, Z. Zhang, and L. Li, *Using lstm and gru neural network methods for traffic flow prediction*, in Proceedings of the 31st Youth academic annual conference of Chinese Association of Automation, Wuhan, China, 2016, IEEE, pp. 324–328.
[8] Y. Gao, *Research on the application of artificial intelligence technology in the development of computer vision*, Highlights in Science, Engineering and Technology, 9 (2022), pp. 80–84.
[9] P. L. Goethals and M. E. Hunt, *A review of scientific research in defensive cyberspace operation tools and technologies*, Journal of Cyber Security Technology, 3 (2019), pp. 1–46.
[10] I. Kamwa, *Dynamic wide area situational awareness: Propelling future decentralized, decarbonized, digitized, and democratized electricity grids*, IEEE Power and Energy Magazine, 21 (2023), pp. 44–58.
[11] P. R. Kshirsagar, R. K. Yadav, N. N. Patil, et al., *Intrusion detection system attack detection and classification model with feed-forward lstm gate in conventional dataset*, Machine Learning Applications in Engineering Education and Management, 2 (2022), pp. 20–29.
[12] B. Roy and H. Cheung, *A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network*, in Proceedings of the 28th international telecommunication networks and applications conference, IEEE, 2018, pp. 1–6.
[13] M. Saratchandra and A. Shrestha, *The role of cloud computing in knowledge management for small and medium enterprises: a systematic literature review*, Journal of Knowledge Management, 26 (2022), pp. 2668–2698.
[14] C. Wang, Z. Li, R. Outbib, M. Dou, and D. Zhao, *A novel long short-term memory networks-based data-driven prognostic strategy for proton exchange membrane fuel cells*, International Journal of Hydrogen Energy, 47 (2022), pp. 10395–10408.
[15] W. Wang, Y. Lei, T. Yan, N. Li, and A. Nandi, *Residual convolution long short-term memory network for machines remaining useful life prediction and uncertainty quantification*, Journal of Dynamics, Monitoring and Diagnostics, 1 (2022), pp. 2–8.
[16] D. Wu, *A network security posture assessment model based on binary semantic analysis*, Soft Computing, 26 (2022), pp. 10599–10606.
[17] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, *Blockchain for healthcare data management: opportunities, challenges, and future recommendations*, Neural Computing and Applications, (2021), pp. 1–16.
[18] E. Zio, *Challenges in the vulnerability and risk analysis of critical infrastructures*, Reliability Engineering & System Safety, 152 (2016), pp. 137–150.

Edited by: Venkatesan C
Special issue on: Next Generation Pervasive Reconfigurable Computing for High Performance Real Time Applications
Received: May 13, 2023
Accepted: Sep 17, 2023