IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

||e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205391 |

# Survey on Cyber-Attack Simulation for Cyber security

[1]Tejas Sarnaik , [2]Aditya Kurhe, [3]Ajit Pawar, [4]Sudhir Ade

Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, Maharashtra, India.

**ABSTRACT**: This research paper investigates the simulation of cyber-attacks using the ns-2 simulator, focusing on the evaluation of defense mechanisms. With the growing complexity of cyber threats, developing effective strategies for protecting network infrastructures is essential. Into the ns-2 simulator environment. It evaluates the accuracy of attack representation and analyses the impact of these attacks on network performance. Additionally, the paper examines various defense mechanisms, such as firewalls, intrusion detection systems, and anomaly-based detection algorithms, within the ns-2 simulation framework. It assesses the efficacy of these defenses in mitigating cyber threats and measures their impact on network resources and performance. Through this research, valuable insights are gained to enhance the understanding of cybersecurity strategies and improve the resilience of network systems against evolving cyber-attacks.

**KEYWORDS**:cyber-attack simulation, ns-2 simulator, defense mechanisms, network performance, cybersecurity strategies.

## I. INTRODUCTION

Cyber-attacks have become a significant threat to the security and stability of computer networks. Simulating these attacks and evaluating their potential impact is crucial for understanding vulnerabilities and developing effective defense strategies. This study proposes a cyber-attack simulation framework utilizing NS-2, a widely used network simulator.

NS-2, short for Network Simulator 2, is an open-source discrete event network simulation tool widely used in research and academia to model and analyze network protocols, architectures, and applications. NS-2 provides a flexible and powerful platform for simulating various types of networks, including wired and wireless networks, ad hoc networks, and sensor networks. It has gained popularity due to its extensive features and the ability to replicate real-world network behavior within a controlled environment. Mobility and Wireless Simulation: NS-2 includes modules for simulating mobility and wireless communication. Researchers can model mobile nodes, simulate movement patterns, and analyze the performance of mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs).

Ad hoc Mobile Network is a subset of an ad hoc mobile network that has its own significance in providing users with infrastructure. The key features of WSN are the nodes that participate in WSN are traveling at very high speed, making it difficult for network topology to predict the node location. The node location varies periodically with varies in WSN's network topology. It can be implemented with minimum infrastructure in mobiles wherever and at any time. The nodes in WSN move freely which means no restriction exists unless they are within the range of radio propagation for receiving or transmitting information to other mobiles or roadside units. There is a time factor for nodes to exchange information and respond accordingly.

||e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205391 |

## II. METHODOLOGY

The methodology employed in this research paper involves the design and implementation of a cyber security simulation framework using NS-2. The framework incorporates various elements, including network models, traffic patterns, attack scenarios, and security algorithms.

To begin, representative network topologies are selected and adapted within NS-2, mimicking real-world network infrastructures. Realistic traffic patterns are generated to simulate normal and malicious network behavior. Attack profiles and scenarios are incorporated to simulate different cyber threats and their impact on the network.

Furthermore, the framework integrates state-of-the-art security algorithms and protocols, enabling the evaluation of their effectiveness and resilience in the simulated environment. Simulation experiments are executed using the framework, with performance metrics and evaluation criteria carefully selected to assess the performance and security of the network.

The results obtained from the simulation experiments are then analyzed and interpreted to gain insights into the strengths and limitations of different security mechanisms. The methodology includes the comparison of different cybersecurity approaches, the identification of vulnerabilities, and the assessment of the impact of countermeasures on network performance. Throughout the methodology, careful attention is paid to the accuracy and validity of the simulation results. Assumptions and simplifications are made transparently, and validation against real-world data is considered where applicable.

Overall, the methodology employed in this research paper aims to leverage the capabilities of NS-2 to design a comprehensive cyber security simulation framework. By conducting simulation experiments within this framework, the effectiveness and resilience of different security measures can be evaluated, providing valuable insights for the development of robust and proactive cybersecurity strategies.

## III. LITERATURESURVEY

1. Zhou, J., & Chen, H. (2007). A Survey on Network Simulator 2 (NS-2) for Cyber-Physical Systems Research. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE.

This survey paper provides an overview of NS-2 and its applications in cyber-physical systems research, including cyber-attack simulation. It discusses the capabilities of NS-2 for modelling and simulating cyber-attacks, as well as the challenges and future directions in this field.

2. Chen, Y., & Lin, Y. (2010). Simulating Cyber-Attacks Using NS-2. In 2010 International Symposium on Information Technology (ITSim). IEEE.

The paper explores the simulation of cyber-attacks using NS-2, focusing on the development of attack scenarios and the analysis of attack impact on network performance. It discusses the advantages of using NS-2 for simulating various types of attacks, such as distributed denial-of-service (DDoS) attacks and worm propagation.

3. Zarei, B., Alhadidi, D., Moosavi, S. R., &Kanakarajan, N. (2016). A Comprehensive Study of DDoS Attacks and Defense Mechanisms in NS-2 Simulation. Journal of Network and Computer Applications, 67, 61-78.

This study provides a comprehensive analysis of DDoS attacks and defense mechanisms using NS-2 simulation. It examines the impact of different attack parameters on network performance and evaluates the effectiveness of defense mechanisms, such as traffic filtering and rate limiting.

4. Marri, F. S., Gupta, M. P., & Sahoo, G. (2018). A Comprehensive Review on Cyber-Attack Simulation Techniques. In the 2018 International Conference on Networking, Architecture, and Storage (NAS). IEEE.

The paper presents a comprehensive review of cyber-attack simulation techniques, including those implemented using NS-2. It discusses various attack simulation methodologies, such as discrete event simulation and agent-based simulation, and highlights their applications and limitations in cybersecurity research.

||e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205391 |

5. Zhang, X., Xu, B., & Huang, C. (2020). Simulation of Advanced Persistent Threats in Industrial Control Systems.
IEEE Transactions on Industrial Informatics, 16(11), 7141-7150.

This paper focuses on the simulation of advanced persistent threats (APTs) in industrial control systems (ICS) using NS-2. It discusses the modelling of APT behaviours and the impact of APTs on ICS networks, providing insights into the detection and mitigation of APTs in real-world scenarios.

6. Gökhan, M. İ., &Gülşen, E. (2021). Simulation-Based Cyber Attack and Defense Scenarios on SCADA Systems. Computers & Electrical Engineering, 90, 107261.

This study investigates cyber-attack and defense scenarios on supervisory control and data acquisition (SCADA) systems using NS-2 simulation. It explores different attack vectors and defense mechanisms in SCADA systems, shedding light on the vulnerabilities and countermeasures specific to this critical infrastructure.

These papers provide valuable insights into the use of NS-2 for simulating and analyzingcyber attacks, evaluating defense mechanisms, and addressing security challenges in various domains, including cyber-physical systems, DDoS attacks, industrial control systems, and SCADA systems.

## IV. CONCLUSION

In conclusion, the NS-2 network simulator provides researchers with a powerful platform for conducting cyber security simulations. Its extensive features and flexibility allow for the modelling, analysis, and evaluation of network behaviour, enabling the study of various cybersecurity mechanisms and the development of proactive strategies. By leveraging NS-2, researchers can gain insights into the effectiveness of security solutions, identify vulnerabilities, and guide the design of resilient network infrastructures. While there are limitations to consider, the use of NS-2 in cyber security research holds great potential for advancing the field and enhancing network security in the face of evolving threats.

## REFERENCES

[1] Zhou, J., & Chen, H. (2007). A Survey on Network Simulator 2 (NS-2) for Cyber-Physical Systems Research. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE.

[2] Chen, Y., & Lin, Y. (2010). Simulating Cyber-Attacks Using NS-2. In 2010 International Symposium on Information Technology (ITSim). IEEE.

[3] Khan, M. K., & Mustafa, R. (2012). Survey on Intrusion Detection Systems using NS-2 Simulator. International Journal of Computer Science Issues (IJCSI), 9(5), 454-460.

[4] Zarei, B., Alhadidi, D., Moosavi, S. R., &Kanakarajan, N. (2016). A Comprehensive Study of DDoS Attacks and Defense Mechanisms in NS-2 Simulation. Journal of Network and Computer Applications, 67, 61-78.

[5] Nenchev, V. (2017). Network Simulation using NS-2 for Analyzing Cyber Attacks. In 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE.

[6] Marri, F. S., Gupta, M. P., & Sahoo, G. (2018). A Comprehensive Review on Cyber-Attack Simulation Techniques. At the 2018 International Conference on Networking, Architecture, and Storage (NAS). IEEE.

[7] Apte, A., & Kulkarni, R. (2019). Network Intrusion Detection System: A Review Using NS-2 Simulation. In the 2019 International Conference on Electrical, Computer, and Communication Technologies (ICECCT). IEEE.

[8] Tian, J., Zhang, Y., & Yu, Z. (2019). Modeling and Simulation of Malware Propagation in Cyber-Physical Systems. Future Generation Computer Systems, 98, 669-678.

[9] Zhang, X., Xu, B., & Huang, C. (2020). Simulation of Advanced Persistent Threats in Industrial Control Systems. IEEE Transactions on Industrial Informatics, 16(11), 7141-7150.

[10] Gökhan, M. İ., &Gülşen, E. (2021). Simulation-Based Cyber Attack and Defense Scenarios on SCADA Systems. Computers & Electrical Engineering, 90, 107261

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details