Investigation of a Multi-Agent Intrusion Detection System for Campus Wireless Networks

Femi Elegbeleye,
Omobayo Ayokunle Esan, Ife Elegbeleye
Walter Sisulu University, East London, South Africa

Abstract

Intrusion Detection Systems (IDS) are critical in safeguarding computer networks against unauthorized access, misuse, and abuse. While external threats are significant, internal attacks often present even greater risks within institutional environments. This study examines the development of a multi-agent-based IDS designed to strengthen the security of a university's Wireless Local Area Network (WLAN). A proposed framework integrates intelligent agent technology with intrusion detection techniques to enable proactive analysis and adaptive response to potential threats. Data were collected through an online questionnaire and analyzed using Microsoft Excel to assess vulnerabilities and perceptions of IDS implementation. The findings indicate that IDS adoption enhances network security and substantially benefits students, particularly in supporting learning activities. Nonetheless, specific challenges remain about WLAN infrastructure. The study contributes valuable insights into IDS-based applications in academic settings and offers practical guidance for improving institutional cybersecurity.

Keywords: Intrusion Detection System (IDS), Multi-Agent Systems, Wireless Local Area Network (WLAN), Network Security, Cybersecurity

1. Introduction

This research investigates the risks and vulnerabilities of a suitable multi-agent-based intrusion detection system. There is a need to create awareness within the university community among students using multi-agent-based systems design and to recommend best practices in evaluating multi-agent-based risks and vulnerabilities. The paper is about Walter Sisulu University (WSU), Ibika campus, which understands the importance of intrusion detection. Wireless Local Area Network (WLAN) intrusion prevention or prevention of the system can manage wireless traffic for the WSU Ibika case study WLAN. Prevention systems can manage traffic, while Wireless Intrusion Detection Systems (WIDS) use dedicated wireless integrated network sensors to detect embedded intrusions for WSU, wherever a wireless access point is open on the network. Wireless lunchtime teaching security school compares wireless network Intrusion Detection System (IDS) and explains how WSU enterprise can choose between them.

The current situation of WSU is not bad because its network has a server and a firewall. Although it has a firewall, it must be detected using an IDS security system. The type of current system they use in the WSU Ibika campus case study is an IDS integrator. This study introduces the central issue of the WSU Ibika campus: students need to work efficiently and effectively. It will assist the Ibika Campus IDS technologies and maintain IDS for the WSU, Ibika Campus. It will also provide an overview of complementary technologies, including the tools that analyze. A Multi-Agent System (MAS) is a loosely coupled network of problem solvers that interacts to solve problems beyond the individual capabilities or knowledge of each problem solver (Derfee & Lasser, 1989).

A Wireless Local Area Network (WLAN) is one in which a mobile user can connect to the local area network (LAN) through a wireless (radio) connection (Rouse, 2020). An Intrusion Detection System (IDS) is a type of security software designed to automatically alert administrators when something is trying to compromise an information system through

malicious activities or security policy violations (Jassen, 2018). The WSU Ibika campus has never had the IDS and MAS based on its WLAN, so most IDS activities do not apply to the Ibika Campus. This paper aims to investigate a suitable multi-agent-based intrusion detection system for WSU students and the Wireless Local Area Network to help university community members understand the importance of intrusion detection.

The main problem with the current wireless network at WSU Ibika Campus is that the intruders can easily hack the WLAN because the wireless network of Ibika is not as secure as the wired one (Mr. N Lushaba, Jaza M, 2021). The current WSU network is secure, but not because the brilliant internal hackers can easily hack it. Another challenge is that there is an Advanced Persistent Threat that the intruders use to gain access to the WLAN of the Ibika campus. The researcher had a positive impact by detecting the intrusion on the Ibika campus. WSNs are more vulnerable to security attacks due to their open environment. They had come across some limitations in implementing many approaches. Networks are secured from attacks by managing the IDs in each maintained system. More challenges are proposed to overcome limitations (Ziv Hagba, 2021). To address these challenging issues, this study aims to make the students of Walter Sisulu University (WSU), Ibika campus, understand the importance of intrusion detection so that students can detect intruders who might want to hack their system.

The remaining part of the paper follows: Section II is the related work, Section III is the research methodology, Section IV is the data analysis, Section V is the discussion, and Section VI concludes the paper.

2. Related Works

The “Layered Intrusion Detection Framework” was proposed by Komninos N and Douligeris (2018). Delineates a specialized mobile ad-hoc IDS technique in which nodes assume different roles (e.g., alert, detection, and collection). This differs from our approach, in which data collection and processing are done on each host node; IDS instances have no coordinated action (Adrian P, 2019). This allows for greater application independence and allows the host systems to operate independently of information from other systems. It also reduces the possibility of failure and reduces computational needs (Adrian M, 2018). Implement threshold-based IDS (Patwardhan A et al) that works with routing on an ad-hoc network infrastructure using “watchdog” nodes. This is a specialized case of IDS that utilizes nodes serving a specific purpose. Our system implements a general-purpose detection scheme that is not dependent on special-function nodes. Because of its inherent scalability, low resource consumption, and portable code base, our IDS applies to a different set of possible target scenarios than those featured in the related works in this section.

For Intrusion Detection Systems (IDSs) in Vehicular Ad Hoc Networks (VANETs), a single-objective optimization algorithm has inherited limitations for the feature selection problem with multiple objectives (J Liang, 2020) (Elegbeleye & Isong, 2025). Moreover, the imbalanced problem commonly exists in various datasets. Thus, in this paper, a feature selection algorithm based on a many-objective optimization algorithm is proposed for IDSs in VANETs, in which the Adaptive Non-dominant Sorting Genetic Algorithm serves as the many-objective optimization algorithm (QTA Pham, 2019). Two improvements, called Bias and Weighted (B&W) niche-preservation and Information Gain (IG)-Analytic Hierarchy Process (AHP) prioritizing, are further designed in FS-MOEA. The former is used to counterbalance the imbalanced problem in datasets by assigning rare classes to higher priorities. At the same time, the latter is employed to search for the optimal feature subset for FS-MOEA. In IG-AHP prioritizing, a more distinct measurement, average IG, is used as the dominant factor to guide the decision analysis of AHP (J Liang). Experimental results show that the proposed FS-MOEA can improve the performance of IDSs in VANETs and alleviate the negative impact of the imbalanced problem. Vehicular Ad-hoc Networks (VANETs) are vulnerable to various types of network attacks like Blackhole attack, Denial of Service (DoS), Sybil attack, etc. (H Zhang, 2018).

Intrusion Detection Systems (IDSs) have been proposed in the literature to address these security threats. However, high vehicular mobility makes formulating an IDS framework for VANET problematic. Moreover, by (B Subba), VANETs operate in bandwidth-constrained wireless radio spectrum. Therefore, IDS frameworks that introduce a significant volume of IDS traffic are unsuitable for VANETs. In addition, dynamic network topology, communication overhead, and scalability to higher vehicular density are other issues that need to be addressed while developing an IDS framework for VANETs (MS Sheikh). This paper aims to make the students of Walter Sisulu University (WSU), Ibika campus, understand the importance of intrusion detection.

3. Research Methodology

This study adopts a mixed-methods approach, combining both qualitative and quantitative techniques to provide a comprehensive understanding of the research problem. The mixed-methods strategy enables the exploration of both measurable data and subjective insights, ensuring a balanced analysis of the Multi-Agent Intrusion Detection System (IDS) deployment within the university network.

Data was collected using structured online questionnaires, which were carefully designed to be clear, descriptive, and user-friendly to facilitate accurate and meaningful responses from participants. Questionnaires were chosen as the primary data collection tool due to their efficiency in reaching a large and diverse group of respondents, affordability, and ease of administration. This method also allows respondents to provide thoughtful feedback at their convenience, reducing potential biases that can occur during face-to-face interviews. The questionnaire focused on gathering information about participants' awareness of IDS, perceived benefits, potential challenges, and vulnerabilities associated with the university's Wireless Local Area Network (WLAN). Direct engagement through the questionnaire enabled effective communication with respondents, ensuring comprehensive data collection while maintaining anonymity and confidentiality.

Collected responses were analyzed using Microsoft Excel, employing descriptive statistics to summarize key trends and patterns. This analysis supported the identification of IDS-related risks, benefits, and areas requiring improvement, providing a foundation for validating the proposed Multi-Agent IDS framework. The methodological approach ensures that both technical and user-centered perspectives are incorporated, enhancing the reliability and applicability of the research findings for academic network security improvements.

3.1. Research Sampling and Data Collection

The study sample comprised 40 students enrolled in the Information Technology Systems program, selected based on the assumption that they are frequent users of the Walter Sisulu University (WSU) wireless network. This purposive sampling approach ensured that participants had sufficient exposure to the campus WLAN, providing relevant insights into their awareness, understanding, and experiences regarding intrusion detection systems (IDS).

Data collection was conducted using a structured questionnaire consisting of two sections. Section 1 gathered demographic information such as age, gender, and level of study. Section 2 included 15 Likert-scale questions designed to measure students' knowledge, perceptions, and attitudes toward IDS deployment on the campus network, with responses ranging from 1 (strongly disagree) to 5 (strongly agree).

The questionnaires were administered in person across different locations on the WSU Ibika campus. The researcher provided guidance to participants unfamiliar with technical WLAN concepts, assisting them in completing the questionnaire when needed. Additionally, mobile devices were employed to record responses during informal interviews, enabling accurate documentation of students' perspectives and experiences. This approach allowed the study to capture both quantitative data from the Likert-scale responses and qualitative insights from informal

4. Data Analysis

Data analysis embraces a whole range of activities of both qualitative and quantitative types. It is a usual tendency in behavioral research that much use is made of quantitative analysis, and statistical methods and techniques are employed. Statistical methods and techniques. Data analysis encompasses a wide range of activities, incorporating both qualitative and quantitative approaches. In behavioral research, there is a common emphasis on quantitative analysis, with statistical methods and techniques frequently employed to derive meaningful insights. These methods occupy a central role in research, as they provide systematic solutions to research problems (Wolpe, 1978).

For this study, an online questionnaire was distributed to students at Walter Sisulu University, Ibika campus, and 25 responses were received. The questionnaire responses were compiled in a Microsoft Excel spreadsheet and subsequently analyzed. Selected questions and their corresponding responses are presented in this section, with results illustrated using tables and graphical representations to facilitate interpretation and understanding of the data.

Question 1: What Gender are you?

The gender information of respondents was asked, and the information provided is shown in Figure 1

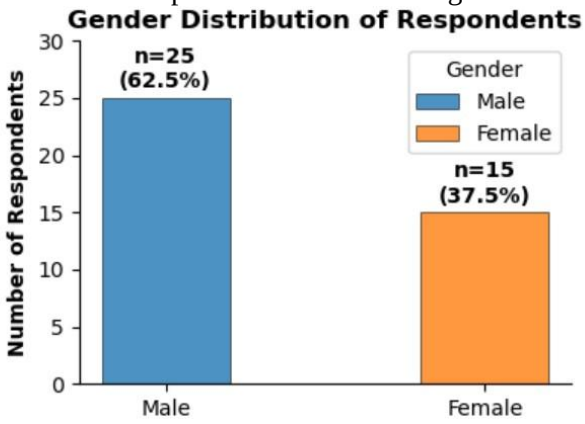

Figure 1. Respondents gender.

Figure 1 captures the gender distribution of the respondents, providing an understanding of the

demographic context. The visualizations indicated the proportion of male and female participants. This is important because demographic characteristics can influence knowledge, perception, and behavior regarding network security and intrusion detection systems (IDS). Ensuring a diverse sample enhances the generalizability of the findings.

Question 2: Do you understand what IDS for WLAN is all about? The second question 2 aims to know whether the students understand what IDS for WLAN is about. The student response is as shown in Figure 2.

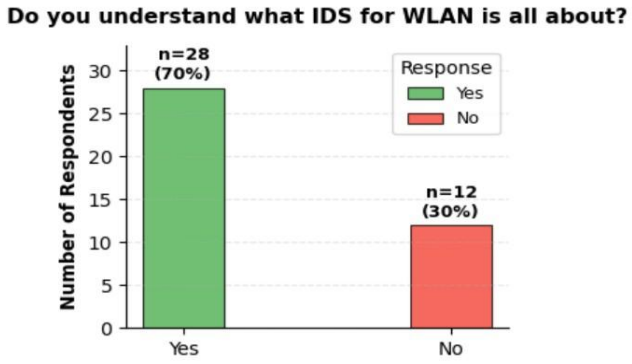

Figure 2. Level of respondents' understanding of IDS for WLAN.

Question 2 examined whether students understand what IDS for WLAN entails. The majority of respondents demonstrated limited understanding, with a significant portion responding negatively or indicating uncertainty. This suggests that awareness and knowledge of wireless network security measures are not uniformly distributed among the student population. The findings highlight the need for educational interventions and awareness campaigns to improve knowledge about IDS technologies and their benefits in securing wireless networks.

Question 3: Do you know the benefits of using IDS for WLAN? From the respondents' responses, some people said they know the benefits of IDS for WLAN, while others disagreed with the benefits of IDS for WLAN. Figure 3 shows the number of respondents who agree, disagree, strongly agree, and strongly disagree.

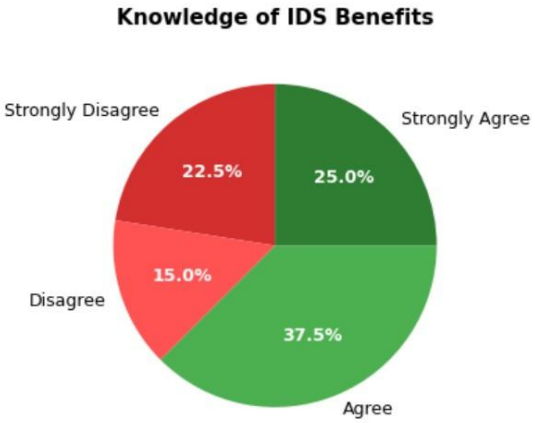

Figure 3. Benefits of IDS for WLAN.

The survey investigated whether respondents had practical experience using IDS. The results showed that most participants had not used IDS, while a smaller portion had some experience. This gap between knowledge and practical exposure is consistent with the findings from Question 2 and emphasizes that awareness alone does not equate to hands-on competence. Limited practical experience may affect students' ability to respond effectively to network intrusions, highlighting the importance of laboratory exercises and simulated IDS environments for skill development.

Question 4: What is your attitude as a student towards using IDS on WLAN on the Ibika Campus? From the respondent's response, some students agreed on having a positive response towards using IDS on the WLAN campus, while some disagreed on its usage on campus. The pictorial representation of the respondent's response is illustrated in Figure 4.

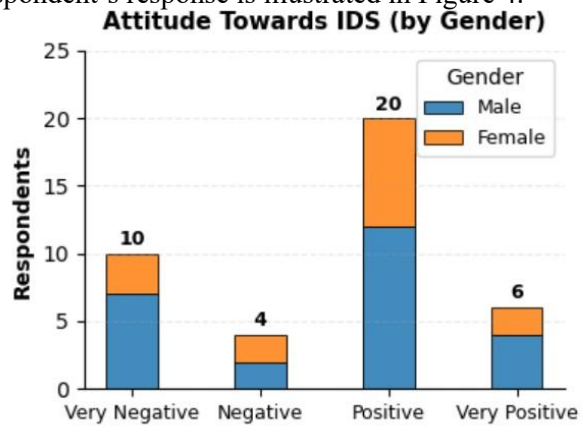

Figure 4. Positive attitude in using IDS for the student WLAN.

From Figure 4, one can observe that 20 students agreed with a positive attitude towards using IDS on the WLAN at the Ibika campus, 10 students strongly disagreed with the use of IDS on the Ibika campus, four students disagreed, and only four strongly disagreed with its usage on the campus. This response shows that most of the students have a positive

attitude towards the use of the IDS for WLAN on campus.

Question 5: Have you ever used IDS to secure a wireless network against intruders? The questionnaire response shows that some students have used IDS to secure the wireless network against intruders, some did not even know what IDS is all about, and some said they have not used it before in securing the wireless network against intruders. The statistics of the respondents' responses are shown in Figure 5.

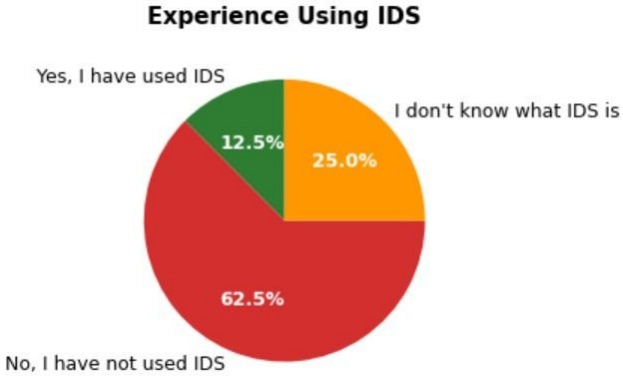

Figure 5. Positive attitude in using IDS for the students' WLAN.

The graph in Figure 5 shows responses from the questionnaires. Out of forty, only five used IDS to secure the network against intruders, 10 out of forty students did not know what IDS was for securing the network, and 25 respondents indicated they had not used IDS against network intruders.

Question 6: Do you feel safe when unauthorized people intrude into your system?

From the response obtained from the questionnaire, a small number of people who used e-commerce before are atleast feel safe, some students did not know whether they are safe (this implies they do not do not have experience in IDS, so they are no sure about the IDS for WLAN), and some say they are not safe when unauthorized person get access into their system. The respondent's response is illustrated in Figure 6.

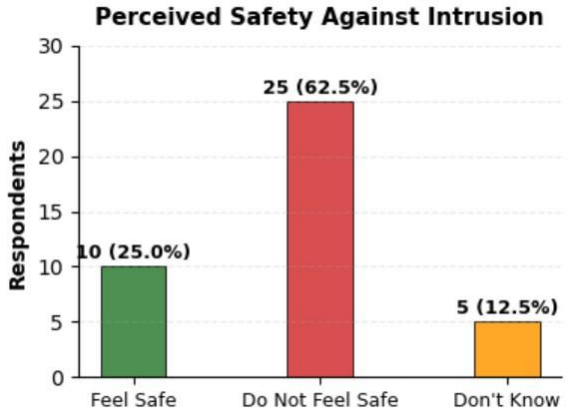

Figure 6. Use of IDS for WLAN.

Question 6 addressed whether students feel safe when unauthorized individuals access their system. The majority of respondents indicated that they do not feel safe, while only a quarter felt secure. This perception aligns with their limited experience using IDS (Question 5) and lack of in-depth understanding (Question 2). It underscores the importance of practical exposure to security tools and the integration of security awareness training to enhance users' confidence in protecting their systems.

5. Political Trust

Investigating the Multi-Agent IDS for WSU WLAN can be a serious problem if proper planning and management are not done. The researcher used a qualitative and quantitative approach, using questionnaires, which mainly had closed-ended questions, and the subjects filled in the answers because the questions were written in English. The entire department should be informed about the IDS security plans for the WLAN. Ibika Campus identifies all the resources that should be made available for WLAN. The researcher was very diligent when dealing with the challenges of this Multi-Agent IDS for the wireless network.

The charts in Section A indicate that Ibika Campus students are interested in using the IDS for WLAN, even though a few students do not know about it. The first section has four student choices: agree, disagree, strongly agree, and strongly disagree. Agree and strongly agree that the longest bars are according to the first section. It is important to state the major problems experienced through the study. The main problem during the data collection was that the students were not interested in giving any information, as this research targeted the Ibika Campus. The purpose of the research was explicitly explained to them. However, since they have little knowledge of the required information, they became shy, which tended to affect the quality of data collection.

6. Conclusions

This research showed that the investigation of IDS in the Ibika Campus can succeed. The research also discovered that the investigation of IDS in the Ibika Campus can be effective and efficient if properly implemented. The researcher noted this when conducting the IDS investigation. There are other problems experienced by students in the investigation of the Multi-Agent IDS in Ibika Campus, for example, there were places where the Multi-Agent IDS was implemented, but people were not using it. The results of this study were positive, which means that the data were precisely what was collected by the research. For the researcher to get quality data, the questionnaires'

questions were direct, to the point, and understandable. The question was in one language (English) so that respondents could understand what was asked and give clear responses or understanding. The "strongly agree, agree, and yes" options are dominated, as reflected in the charts in this study. Those responses directly supported the positive view of the collected data.

The Students of the Ibika campus will benefit from this study in such a way that the system and WLAN will be in good condition. The student will be able to perform their IDS for WLAN. The most fascinating challenge about multi-agent-based IDS in the network of WSU Ibika Campus (e.g., files, directories, records, programs) is that they move across the network. For example, the intruder may need several accounts to hack the system. To solve this unique problem that has never been dealt with before is vital and very interesting. The rationale and motivating work in the IDS is to identify unauthorized use, misuse, and abuse of the computer system. Another interesting work is when the researcher identifies the set of general IDS performance objectives, the basis for the WSU Ibika campus case study methodology.

Author Contributions: Femi Elegbeleye; writing, conceptualization, and data analysis, Omobayo Esan, proofreading and performing data analysis, and Ife Elegbeleye; data collection and proofreading.

Funding: This research was funded by the Department of Information Technology Systems, Walter Sisulu University, South Africa.

Institutional Review Board Statement: The study was conducted under the Declaration of approval by the Institutional Review Board.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data used in this research is available upon request.

Acknowledgements: In this section, the authors acknowledge the support and financial support provided by the Department of Information Technology Systems, Walter Sisulu University, South Africa.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the study's design; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

REFERENCES

1. A. Richard, multi-sensor agent-based Intrusion Detection System. Proceedings of the 2nd annual conference on Information security curriculum development. Pp.100-103, 2018.
2. C. Janssen, C. Intrusion Detection System. Canada: Carol Backcom. 2020.
3. Wang, H. 2014. Multi-agent-based Intrusion Detection System on a wireless network. Canada: Kunming.
4. R. Heady, G. Luger, A. Maccabe. The architecture of the network-level Intrusion Detection System. Technical report, Computer Science Department, University of New Mexico, 2008.
5. W. Haung, Yan AN, Wei DU. 2015. A multi-agent-based Distributed Intrusion Detection System. China: Handan.
6. L. Brendan. ITS integrator: Enterprise server and storage at WSU, 2014.
7. P. Adrian, A. Lauf. Richard. Distributed Intrusion Detection System-Constrained Devices in Ad Hoc Networks. SI, 2018
8. CippMan, Richard. Intrusion Detection System evaluation. Dirpa offline, 2011
9. N Lushaba, M, Jaza. State about the Existing Wireless Local Area Network, 2021
10. P. Rawat, K. Singh, H. Chaouchi, and J. Bonnin. Wireless Sensor Network, 2019
11. C. Robert. Newman. Survey on Secure Network: Intrusion Detection & Prevention Approaches, 2016.
12. P. Rawat, K. Singh, H. Chaouchi, and J. Bonnin. Study on Intrusion Detection System in Wireless Sensor Networks, 2019.
13. H. Wang. (20016) Multi-agent based Intrusion Detection System on a wireless network. Canada: Kunming.
14. R. Heady. G. Luger, A. Maccabe, A. The architecture of the network-level Intrusion Detection System. Technical report, Computer Science Department, University of New Mexico, 2016.
15. W. Haung, Yan AN, Wei DU. A multi-agent-based Distributed Intrusion Detection System. China: Handan, 2013.
16. W. Samantha. ITS integrator. Butare: National University of Rwanda, 2019.

17. P. Adrian, Lauf. Richard A. Distributed Intrusion Detection System-Constrained Devices in Ad hoc Networks. SI

18. CippMan, Richard et al. (2015) Intrusion Detection System evaluation. Dirpa offline, 2015.

19. James P. Anderson. Computer Security Technology Planning Study, Volume 1999.

20. Yurong XU, F. James, and M. Filia. Literature survey on IDS. SI Taminee S (n.d) Improving intrusion detection system. SI, 2010.

21. Aamad, Litsa, and CLdixon (n.d), a misuse-based network IDS using temporal logic and stream processing. United Kingdom: Liverpool.

22. L. Phifer. WLAN Security: Best practices for wireless network security. Premium Editorial, 2014.

23. Systematic Cooperation. Wireless local area network security. SI.Sharma M, Jindal K, B.K. Sharma. Analysis of IDS. Ghaza, Uttar Pradesh, India. P 35, 2008.

24. Z. Zhi-yhu, L. Wei. Analysis of the intrusion detection system. China: Hernan University of science and technology, 2019.

25. N. Boyd. What is external validity in research? Educational portal Bricki, N., & Green, J. A Guide to Using Qualitative Research Methodology, 2007.

26. J.W. Creswell. Research design: Qualitative, quantitative, and mixed methods approach. Sage Publications, 2014.

27. J.M. Eakin. Educating critical qualitative health researchers in the land of the randomized controlled trial. Qualitative Inquiry, 22, 2016.

28. Aamad, Litsa, and CLdixon (n.d), a misuse-based network IDS using temporal logic and stream processing. United Kingdom: Liverpool.

29. L. Phifer. WLAN Security: Best practices for wireless network security. Premium Editorial, 2014.

30. Systematic Cooperation. Wireless local area network security. SI, 2018.

31. Sharma M, Jindal K, B.K. Sharma. Analysis of IDS. Ghaza, Uttar Pradesh, India. P 35. 2008.

32. Z. Zhi-yhu, L. Wei. Analysis of the intrusion detection system. China: Hernan University of science and technology, 2019.

33. N. Komninos and C. Douligeris. LIDF: Layered intrusion detection framework for Ad hoc networks. In press, Accepted Manuscripts.

34. N. Komninos, Vergados. And Douligerius. Detecting unauthorized and compromised nodes in mobile ad hoc networks. Ad Hoc Networks: p 289-298, 2007.

35. M. E. Mkiramweni, C. Yang, J. Li, and W. Zhang, “A survey of game theory in unmanned aerial vehicles communications,” IEEE Communications Surveys & Tutorials, 2019.

36. 36. J. Moura and D. Hutchison, “Survey of game theory and future trends with application to emerging wireless data communication networks,” Research Gate. Net/publication, vol. 315764798, 2017.

37. 37. H. Sedjelmaci, M. Hadji, and N. Ansari, “Cyber security game for intelligent transportation systems,” IEEE Network, 2019.

38. 38. J. Pawlick, E. Colbert, and Q. Zhu, “A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy,” ACM Computing Surveys (CSUR), vol. 52, no. 4, pp. 1–28, 2019.

39. 39. C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch,S. Ren, N. Pissinou, and S. S. Iyengar, “Game theory for cyber security

40. and privacy,” ACM Computing Surveys (CSUR), vol. 50, no. 2, pp. 1–37, 2017.

41. 40. S. Bahamou, E. Ouadghiri, M. Driss, and J.-M. Bonnin, “When game theory meets VANET’s security and privacy,” in Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi-Media. ACM, pp. 292–29, 2016.

42. 41. T. Verwoed and Hunt R Department of computer science. Intrusion detection techniques and approaches. New Zealand: university of canter burg.

43. 42. J. Marcus and Ranum.Intrusion detection challenges and myth. Available at: http//:www.infr.net/forum/punlications/id-mynths.htmlhi-yhu Z, Wei L. Analysis of the

intrusion detection system. China: Hernan University of science and technology.

44. 43. S. Ramgovind, E. Mm, and E. Smith. 'The management of security in Cloud computing The Management of Security in Cloud Computing', 2014.

45. 44. S. Saidhbi. 'A Cloud Computing Framework for Ethiopian Higher Education Institutions', IOSR Journal of Computer Engineering, 6(6), pp. 01–09, 2012. doi: 10.9790/0661-0660109.

46. 45. F. Elegbeleye and B. Isong, "A Systematic Review of Challenges in Teaching and Learning Computer Programming Modules," The Indonesian Journal of Computer Science, vol. 14, no. 1, 2025.