Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 14 – 24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MODIFIED WOLF SHEEP PREDATION ALGORITHM FOR NETWORK THREAT REDUCTION

Audecious Mugwagwa[1], Colin Chibaya[2], Ernest Bhero[1]

[1]School of Engineering, University of KwaZulu Natal, Howard College, South Africa
[2]Department of Computer Science, and Information Technology, School of Natural and Applied Sciences, Sol Plaatje University, Kimberley, South Africa

ABSTRACT. Because most attacks target computers, intrusion detection has emerged as a key component of network security. This is a result of the widespread expansion of internet connectivity and information system accessibility on a global scale. The Wolf Sheep Predation Algorithm (WSPA), evolved from the Wolf Pack Algorithm. It models how wolves hunt in packs. This paper focused on the Lotka-Volterra predator-prey model. Due to its global convergence and computational strength, it has mostly been applied in a variety of engineering optimization issues. The method, however, has numerous flaws, including slow convergence and a tendency to quickly reach the local optimum. To address the above-mentioned flaws, this research developed the Modified Wolf Sheep Predation Algorithm (MWSPA) to reduce network threats. the algorithm models the wolves and sheep, where the wolves in this study represent the network security agent while the sheep represent network threats. The model suggests a better strategy to address the problem of slow convergence and quickly reach the local optimum by making sure that there is a balanced ecosystem at any point in time. This is achieved by ensuring that the network security agents(wolves) are not outnumbered by threats(sheep) and they do not become extinct when there is no food source. So in the absence of food, the MWSPA ensures the wolves can survive on grass and maintain their strength to hunt their next prey. This idea prevents the algorithm from crashing if the wolves die while the prey grows to infinity and consumes all the available grass. This therefore solves the problem of rapidly failing into a local optimum. This study aimed to identify the most pertinent features employed by wolves (network security agents) while hunting the sheep (network threats). We therefore established that sense of hearing and smell, splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey as the most outstanding attributes used by wolves while hunting. The study further evaluated the MWSPA, and the outcomes demonstrate that the suggested algorithm outperforms its predecessor approach in a variety of search environments. Therefore, this shows that the MWSPA may possess the necessary qualities for creating a solution that will completely eradicate network threats and might provide leads in solving growing cybersecurity concerns globally.

Keywords: cybersecurity, cyberthreats, self-organization, swarm intelligence, algorithms

1.0 INTRODUCTION

One of the most difficult problems resulting from the rapid development of information technology is network security (Yuchong & Qinghui, 2021). As a result, the network's perimeter and the data that traverses across it need to be protected (Eric & Anca, 2022). The primary objective of intrusion detection systems (IDSs) is to identify and differentiate between regular and abnormal network connections, which is regarded as one of the main problems with intrusion detection systems due to the abundance of qualities or features quickly and accurately. Designing intrusion detection systems is significantly hampered by the emergence of malicious software (malware) (Ponnusamy, et al., 2021). The main issue in identifying unknown and obfuscated malware is that the creators of the infection utilize various evasion tactics for information concealment to evade detection by an IDS (Ansam, et al.,

2019). Malicious attacks have become more complex. Additionally, there have been more security risks like zero-day attacks that are aimed at internet users. Consequently, since the usage of information technology has permeated our daily lives (Mugwagwa, et al., 2023), computer security has become crucial (World Economic Forum, 2022).

Every company has a purpose and risk management is essential to protecting an organization's information assets (NIST, 2011). This is achieved by employing (Mugwagwa, et al., 2023)automated information technology systems to detect and eliminate network threats (Sikender & Lakshmisri, 2018). As a result of this trend's expansion of the attack surface, there have been more cyberattacks directed at businesses and organizations (Mugwagwa, et al., 2023). The cybersecurity landscape has changed in terms of the sophistication of attacks, their complexity, and their impact (Government of Canada, 2022). This is due to factors such as an ever-increasing online presence, the conversion of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity, and the exploitation of new features of emerging technologies like Artificial Intelligence (Yuchong & Qinghui, 2021). Notably, the threat to supply chains has taken the top spot among major threats because of the magnitude of their potentially catastrophic cascade effects (CISA, 2022). It is important to note that the impact of cyber threats on different industries has been given special attention with the continuously changing threat landscape (Heloise, 2022). The unique characteristics of each sector with respect to the threat landscape and areas of concern may provide interesting insights. Additionally, there have been some noteworthy actions taken by policymakers and cybersecurity specialist to lessen the impact of network threats (Hans & Marijn, 2017). Ransomware and phishing are the most common threats being reported globally, and the international community has started to realize the need for communication and collaboration in tracing indicators of compromise and cyber attackers (Alok, et al., 2022). Considering the foregoing, this article attempts to contribute to current efforts to eradicate and lessen the effects of network threats on a worldwide scale by assessing the degree to which the implementation of the Modified Wolf Sheep Predation algorithm could aid in the eradication of network risks in enterprises.

1.2 Wolf Sheep Predation Algorithm (WSPA)

The algorithm mimics wolves as they hunt for food. Wolves find prey by using their exceptional sense of smell in conjunction with their superb hearing (Rui, et al., 2012). Although wolves prefer to hunt in packs, lone wolves can also successfully hunt small animals on their own. The WSPA uses a mathematical mapping that mimics the tactics employed by the wolf while hunting, such as splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey (Wu & Zhang, 2014). Wolf predation algorithms can be modeled using a mathematical model that considers various factors such as the number of wolves in a pack, their hunting capabilities, and the abundance of prey in their ecosystem (Xuan, et al., 2021). This paper focuses on the Lotka-Volterra model and assumes that a predator's rate of prey consumption is inversely related to its abundance (Frank, et al., 2021). As a result, the only factor affecting predators' ability to feed is the availability of prey (Thomas, et al., 2021). This mathematical model can be useful in predicting the behaviour of wolf predation patterns and can help inform conservation efforts to ensure the stability of both predator and prey populations (Noah, et al., 2021). The model is based on several key assumptions, including the idea that wolves have a certain hunting efficiency, which is determined by factors such as the size of their pack, their experience level, and the abundance of prey in their habitat. Additionally, the model considers the reproductive rates of both wolves and their prey, as well as the effect of environmental factors such as weather and vegetation on the survival and growth of both populations.

1.2.1 Inspiration of the WSPA

The algorithm was influenced by the studies done on the behaviour of social wolves while hunting for food. To be more precise, we concentrated on colony predation, which is a strategy adopted by wolves to evade predators and boost the likelihood of a successful hunt (Muro, et al., 2021). Predators

frequently acquire more prey through colony predation, which increases the likelihood that each individual will survive (Dipanjan, et al., 2020). Colony predation is a strategy used by wolves and other animals that live in colonies to ensure their survival (Muro, et al., 2021). The wolf sheep predation algorithm is a heuristic optimization algorithm inspired by how wolf packs hunt and search for food. In this algorithm, there are two types of wolves: alpha wolves and beta wolves (Xuan, et al., 2021). The alpha wolves are responsible for exploring the search space and finding potential solutions, while the beta wolves follow the alpha wolves and refine the solutions found by the alpha wolves (Weitzenfeld & Vallesa, 2006).

The algorithm starts with an initial population of solutions, which are randomly generated. The alpha wolves then select the best solutions and share their knowledge with the beta wolves (Xuan, et al., 2021). The beta wolves then use this knowledge to refine the solutions and generate new ones. To catch more prey than they could individually, wolves, communicate and work together through colony predation (Jiaze, et al., 2021). The two most popular strategies for increasing the likelihood of successful hunting are dividing and encircling animals. Another tactic used by wolves when they come into circumstances, such as when consumption outpaces their yield, is selective abandonment (Jiaze, et al., 2021). They will switch to another target in this behaviour, which increases the effectiveness of their predation. This process continues until a stopping criterion is met, such as a maximum number of iterations or a satisfactory solution has been found (Dipanjan, et al., 2020). The main aspects of the algorithm are splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment which all revolve around the communication aspect. The section below discusses the various strategies used by wolves while they hunt for prey.

1.2.1.1 Communication:

Wolves that hunt in packs have a higher success rate for predation due to cooperation and communication. To affect their behavior of looking for food, they convey their positions relative to the position of the pack leader. These positions also help in the event the hunters with the best chances of success need support.

1.2.1.2 Splitting/Dividing:

Another aspect of colony predation by wolves is to drive their prey in separate directions, separating it from the rest of the pack, this predation technique is employed by individual wolves when looking for food.

1.2.1.3 Encirclement:

The other tactic employed by the hunting wolves is to encircle and approach the prey increasing the chances of a successful hunt.

1.2.1.4 Assisting hunter with the best chances of success:

The closest member requests help from the group because they might have trouble hunting prey to increase success chances. This is achieved through communication, which has been identified as one aspect employed by wolves in successful hunting.

1.2.1.5 Selective abandonment:

If no prey is found nearby, or food is located too distant from the prey, the remaining individuals will find another food source.

1.2.2 The Model

The mathematical simulation of the algorithm's position illustrates the search process of individuals and groups in two and three dimensions, with a predator at position (X, Y) updating its position in accordance with the target's location (Xbest, Ybest). The predator leader and other predators in the 2D search space are used to update the search agent's position. The ultimate position will be at random influenced by the positions of the predator leader and the other predators in the search area.

In the model, we can consider the cyber security threats as the prey, and the security measures as the wolves. We can then define the fitness function that represents the effectiveness of the security measures in protecting the system from the threats. The wolf pack can be modelled as a group of security measures that work together to detect, prevent, and mitigate cyber security threats. The wolf agents can communicate with each other and coordinate their actions to optimize their fitness function. Through iterations of the algorithm, the wolves can adapt their strategy to improve the overall security of the system. The Wolf Sheep Predation model works as follows:

1. *Initialization: Generate an initial population of wolves and prey.*
2. *Fitness evaluation: Evaluate the fitness of each wolf in the population based on the objective function to be optimized.*
3. *Leader selection: Identify the best wolf (alpha) and the second-best wolf (beta) in the population.*
4. *Prey search: Each wolf in the population performs a prey search to explore the search space and improve its position. This is done by randomizing the position of the wolf and evaluating its fitness.*
5. *Pack hunting: Wolves then move towards the position of the alpha and beta wolves in the population. They adjust their positions based on the position of the leaders and evaluate their fitness at the new positions.*
6. *Updating the population: The population is updated with the new positions of the wolves.*
7. *Termination: The algorithm terminates when a stopping criterion is met (e.g., a maximum number of iterations or a certain level of fitness is achieved).*

4. RESEARCH AND METHODOLOGY

We created a simulator to test how well the Modified Wolf Sheep Predator Algorithm is for eliminating network threats. One simulator was run to determine how well the WSPA algorithm can individually address the network threat issue. The objective was to determine if the main attributes of the algorithm can be used to address the problem defined problem. Wolf agents would scout for food targets which are represented as sheep. The wolf will represent the hunting agent and the sheep will resemble threats. Once the simulations begin, both agents and threats get generated in the simulator's deployment environment, being created at random. The simulations used 100 sheep and 50 wolf agents which were randomly generated and deployed into the environment. Using the outstanding characteristics namely, splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey, the deployed set of wolf agents searches for and identifies potential dangers(prey) in the environment or ecosystem. Separate simulations were run for the same algorithm varying the number of agents, the results were noted, and conclusions were drawn on how the algorithm can address the network threat problems.

4.1 Experiment

The modified wolf sheep predation algorithm's potential for eliminating network threats was tested through an experiment. Using the Netlogo simulators, the experiment was run using an Intel® CoreTM i5 10th generation PC running Windows 11Pro with a 2.40GHz processor and 8GB of RAM. The environments randomly generated wolf, sheep, and grass agents where the wolf agent will hunt for threats(sheep), in the environment. The wolf should ensure that there is no or minimal prey in the environment. While the threat(sheep) feeds on vulnerabilities(grass) to keep alive. Since the sheep can become extinct, the algorithm has been modified so that the wolf can feed on grass for a short period of time if the sheep become extinct. While the simulation is being executed, the agents communicated until they reached the optimal position determined by the instructions given. The key aspects of the algorithm were noted and discussed on how they can be adopted in eliminating network threats.

4.2 Environment setup

The environment in this research refers to two-dimensional square like surface designed in Netlogo. The environment is made up of threat sources and agents which are randomly generated across the two-dimensional square. Once the simulations begin to run, agents scout around the area looking for threat sources. The agent's position keeps changing and being communicated through various techniques until they converge at the best location. While hunting for prey, wolves, communicate and work together through colony predation. They use the four most popular strategies for increasing the likelihood of successful hunting namely dividing, encircling the prey, assisting the hunter with the best chances, and selective abandonment. With selective abandonment, they will switch to another target in this behaviour, which increases the effectiveness of their predation. This process continues until a stopping criterion is met, such as a maximum number of iterations or a satisfactory solution has been found. The main aspects of the algorithm are splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment. The afore mentioned, are the main aspects employed by the WSPA in eliminating network threats.

5. FINDINGS

This section articulates the findings of the experiments as well as the results obtained. The results discuss the number of deployed agents, noting the convergency times as the number of deployed agents varies. Finally, the section analyses these findings and gives recommendations for improving the Wolf Predation Algorithm's detection and elimination of network threats.

5.2 WSPA Simulation

Separate simulations were run for the same algorithm varying the number of agents, the results were noted, and conclusions were drawn on how the algorithm can address the network threat problems. Figure 1 depicts the ecosystem with fifty (50) hunting or search agents looking for prey and one hundred (100) threats represented by sheep as prey. The hunting agents are seen scouting for prey in Figure 2 below, which demonstrates that the predator population has grown greatly relative to that of the prey. Figure 5 demonstrates how predators or hunting agents that resemble wolves are initialized with various strengths depending on the prey they have consumed. As they hunt, their energy reserves go smaller, thus they would prefer to spend as little energy as possible before catching the next prey.

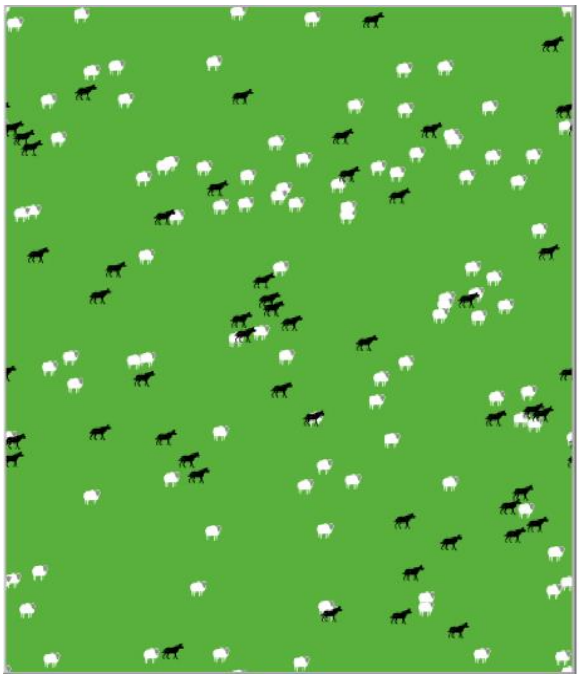

Fig.1 - Wolf Sheep Predation simulation environment

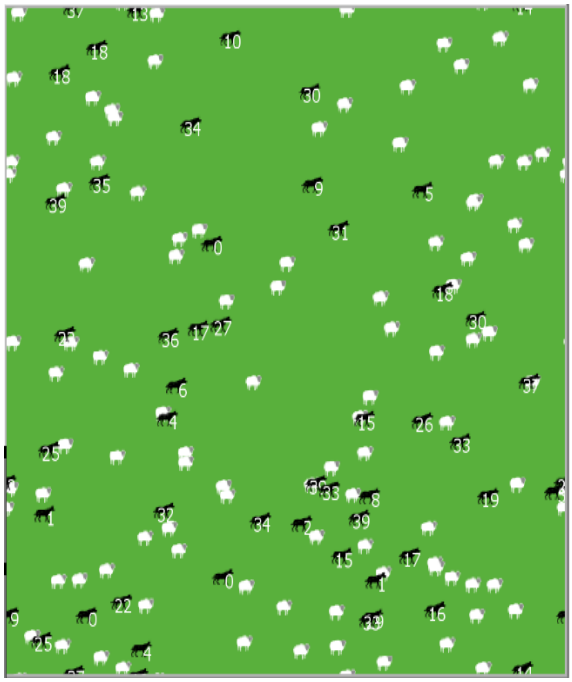

Fig. 2 - Searching and elimination of threats

As the algorithm continues to run, as seen in Figure 3, the predator agent population continues to decline. This is because there will be less food available (prey), which will result in loss of energy. This illustrates how the energy of the predator decreases until it is zero, at which point the wolf agent perishes which gives a situation depicted in figure 4.

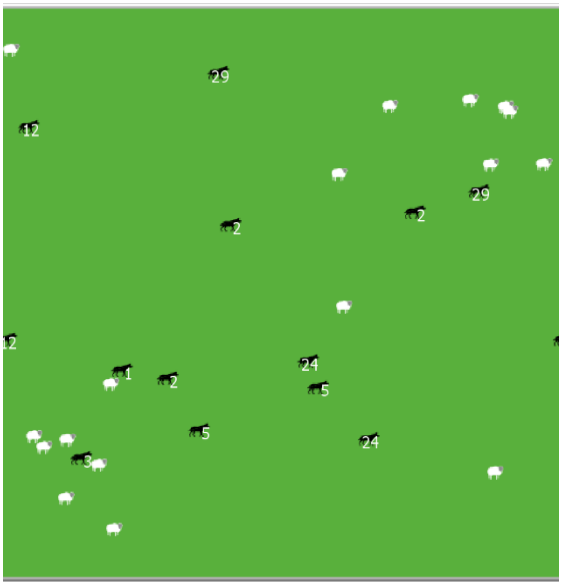

Fig. 3 - Predator energy reduced

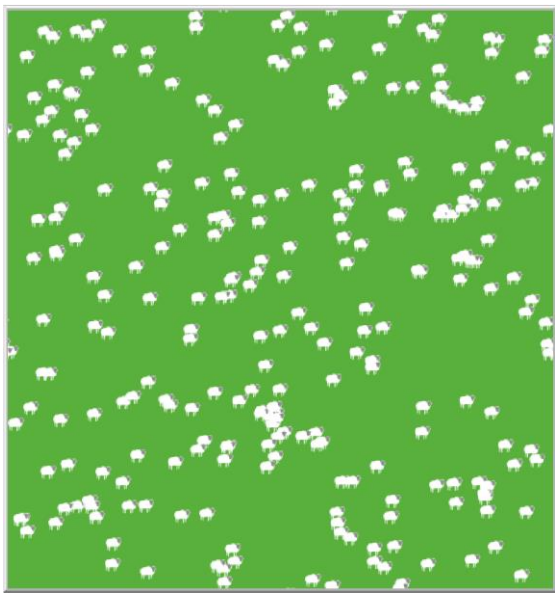

Fig. 4 - Predator Agents extinct

Due to a lack of food when the number of preys decreased (see figure 4), predators or hunting agents all become extinct. This suggests that the environment becomes vulnerable as the hunting agents reach a point where they fail, and the network becomes overrun with threats. There is need to enhance or refill

the predator energy is thus suggested to prevent their extinction, to keep them actively securing the network.

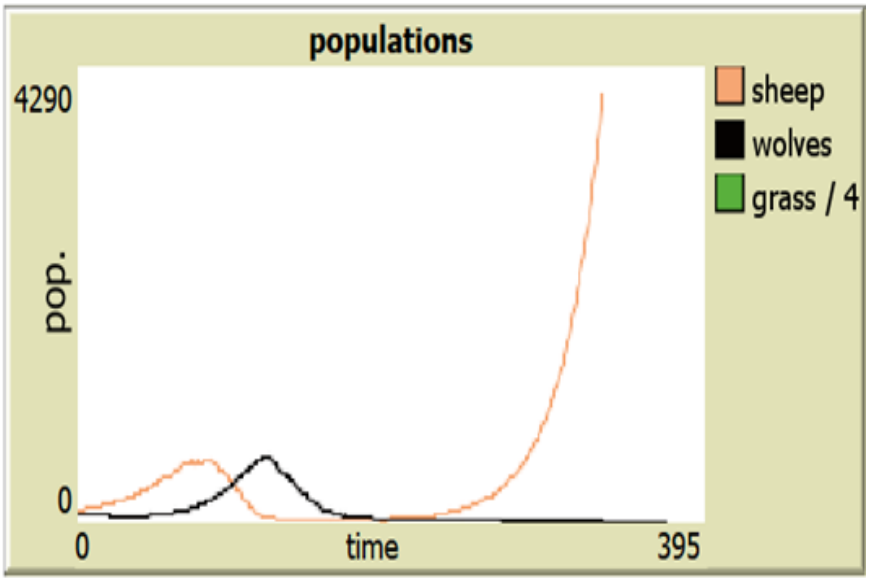

Fig. 5 - Predator agents failed to neutralise threats.

The agents' failure to converge is shown in Figure 5. This is substantiated by the fact that the predators were unable to get rid of the prey, and that this will have a significant impact on network security. This suggests that the WSPA may need to be enhanced to replenish the energy of the predators and guarantee that agents are constantly actively hunting and eliminate threats within a network.

5.3 MWSPA Simulation

To solve the issue, the WSPA must be improved by including a new feature that permits predators to eat grass if there is no prey present. By including these elements, the MWSPA is created, and while the predators feed on grass, they may not gain the same amount of energy as when they eat their prey but will instead keep them alive till they catch their next prey. With these components incorporated it gave the following results.

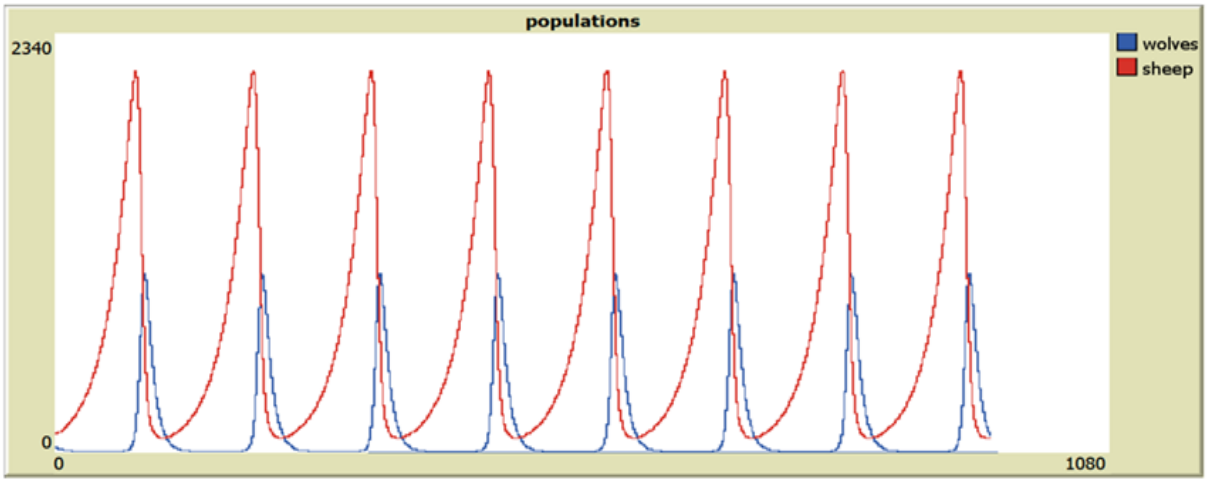

Fig. 6 - MWSPA convergence Graph

The shortfalls of the WSPA of slow convergence and reaching the local optimum have addressed by the MWSPA through the introduction of other variables which includes increasing the grass growth rates and making wolves to feed on grass to boost their energy in case there is no prey. These concepts will help to eliminate predators becoming extinct and therefore ensure that there are no vulnerabilities posed in the network environment as we have seen with the results presented earlier.

5.4 Discussion

The purpose of this section is to give suggestions regarding how the adoption of the WSPA may help eliminate network threats influenced by the results of the simulations done. The research established that the WSPA employees splitting/diving, encircling, assisting the hunter with the best chance of success, communication, and selective abandonment as the main aspects of the algorithm. The results of the experiments conducted further revealed that the predator agent population continues to decline when they fail to find prey as they keep losing energy while hunting. This further suggested that predator agents needed to use the least energy to hunt to ensure that it keeps surviving. As evidenced by the results due to the decreasing number of preys, predators or hunting agents all become extinct at some point in time. This suggests that the environment becomes vulnerable as the hunting agents reach a point where they fail, and the network becomes overrun with threats. There is a need to enhance or refill the predator energy to prevent their extinction and to keep them actively securing the network. This paper, therefore, suggested additional elements to the model that modifies the approach based on success rates and simulates the selective abandonment behavior of hunting wolves through the Modified Wolf Sheep Predation Algorithm (MWSPA). The MWSPA seeks to enhance Lotka-Volterra predator-prey model and make it more suitable for eliminating network threats by dealing with the slow convergence and reaching the local optimum issues. These issues have been addressed by introducing the concept that the sheep/prey agent do not lose energy and the wolf agent can gain limited energy by feeding on grass if there is no prey so that they don't die. Each wolf or sheep agent has a fixed probability of reproducing at each time step in order to maintain the population. In this form, we don't directly represent the eating or growing of grass; instead, we treat the grass as infinite so that sheep always have plenty to eat. As a result, eating and moving do not cause sheep to gain or lose energy. This allows for a stable ecosystem. With these elements incorporated with the development of the MWSPA, the convergence graph will be as shown below. This represents a balanced ecosystem where the problem of slow convergence and reaching local optimum are addressed and the population of the predators wont get zero as with the WSPA.

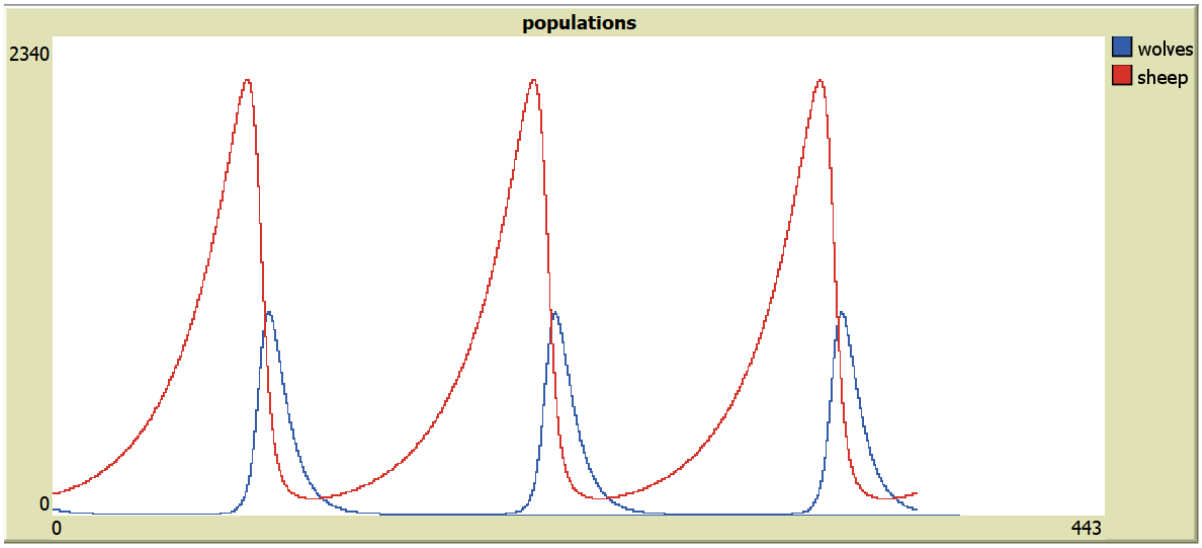

Fig. 7 - MWSPA graph

Figure 7, suggests that the predators and prey agents population have a fixed probability of reproducing. As the predator fail to find prey, they will feed on grass to have the energy needed until the find the next prey. Though they get the energy from grass, their energy continues to deplete but the rate of death is reduced hence ensuring that predator agents wont get extinct. This helps stabiles the ecosystem and ensures that there are predator agents available to eliminates network threats at any point in time.

7. CONCLUSIONS

The Wolf Sheep Predation Algorithm is a bio-inspired algorithm that simulates the hunting behavior of wolves in nature. This algorithm has been found to have useful applications in cyber security.

In cyber security, the Wolf Sheep Predation Algorithm can be used for intrusion detection and prevention. The algorithm can be trained to analyze data patterns and identify anomalies and threats in a network. It works by creating a model of normal network behavior, then comparing the actual behavior with the expected behavior. If the algorithm detects any deviations, it triggers an alert to the security team for further investigation. Overall, the Wolf Sheep Predation Algorithm is an innovative approach to cyber security that has the potential to improve the detection and prevention of cyber threats.

The wolf predation algorithm is a relatively new optimization technique inspired by the hunting behaviour of wolves. However, like any other algorithm, it also has some limitations and shortcomings. One of the main issues is that it can get trapped in local optima, which means that it may not necessarily find the global optimal solution. Additionally, the algorithm can be computationally expensive, especially when dealing with complex optimization problems. Finally, the wolf sheep predation algorithm may require some tuning of the parameters to work effectively, which can be time-consuming and difficult for some users. Despite these limitations, the wolf sheep predation algorithm has shown promise in solving a variety of optimization problems and is still being studied and improved upon by researchers. As a result, this research suggested combining the Wolf Sheep Predation algorithm with other algorithms or existing security solutions to improve its ability to detect and eliminate network threats.

8. KEY OBSERVATIONS

The MWSPA has shown promise in enhancing the capabilities of cyber security systems and improving the detection and response to cyber threats. However, like any other security solution, it is not foolproof and should be used in combination with other security measures for maximum protection. Some possible areas for enhancement could include improving accuracy, increasing efficiency, reducing errors, improving scalability, and optimizing resources. Additionally, main issues which causes it to get trapped in local optima , which means that it may not necessarily find the global optimal solution has been addressed by introducing the concept that the sheep/prey agent do not lose energy and the wolf agent can gain limited energy by feeding on grass if there is no prey so that they don’t die. Each wolf or sheep agent has a fixed probability of reproducing at each time step in order to maintain the population. In this form, we don't directly represent the eating or growing of grass; instead, we treat the grass as infinite so that sheep always have plenty to eat and stabilize the ecosystem.

9. CONTRIBUTIONS

The paper made contributions by providing a review of the Wolf Sheep Predation algorithms' inspirations, the model and the features that constitute the model, how it may be utilized in network threat detection and elimination, and its effects in eliminating network threats.

The paper identified communication, splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment as the outstanding aspects of the algorithm which can be

adopted for network threats detection and elimination. These aspects can be adopted in developing a network threat detection and elimination solution integrated into existing solutions for enhancement.

One of the main contributions in intrusion detection is that by using the Modified Wolf Sheep Predation Algorithm, it is possible to identify and classify malicious activity more accurately, thereby improving the overall security posture of a system. Overall, the use of the Modified Wolf Sheep Predation Algorithm in the network can contribute significantly to the development of more effective and efficient security solutions. Even though the algorithm has these robust features, it also has some shortfalls which may be enhanced by combining it with other algorithms or integrating it with existing network threat detection and elimination solutions to bring better results.

10. FUTURE WORKS

The wolf predation algorithm has had several developments and improvements and some possible future developments to enhance its adoption in cybersecurity include:

1. Hybridization with other algorithms: Exploring the possibility of combining the wolf predation algorithm with other optimization algorithms to create hybrid algorithms that can perform better on certain types of problems.
2. Multi-objective optimization: Currently, the wolf predation algorithm is mostly used for single-objective optimization problems. However, there is potential for using it in multi-objective optimization problems, where the algorithm tries to optimize several objectives at once.
3. Dynamic adaptation: In nature, wolves adapt their hunting behaviour based on changing environmental conditions. Similarly, there is potential for the wolf predation algorithm to be extended with dynamic adaptation mechanisms to improve its performance in dynamic optimization problems.
4. Parallelization: As with most optimization algorithms, the wolf predation algorithm can benefit from parallelization techniques that allow it to exploit modern computing architectures more efficiently.
5. Applications in machine learning: The wolf predation algorithm has shown promising results in various optimization problems, and there is potential for using it in the context of machine learning tasks such as feature selection, dimensionality reduction, and model optimization.

11. FUNDING

This research was funded by the University of Kwazulu Natal (UKZN).

REFERENCES

1. Alok, M., Yehia, I. A., Memoona, J. A. & Asif, Q. G., 2022. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Elsevier, Computers & Security.*

2. Ansam, K., Iqbal, G., Peter, V. & Joarder, K., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Springer, cybersecurity.*

3. CISA, C. A. I. S. A., 2022. *Building more resilient ICT Supply Chain: Lessons learned during the COVID-19 Pandemic,* s.l.: CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

4. Dipanjan, C., Sanchayan, B. & De, R., 2020. Survival chances of a prey swarm: how the cooperative interaction range affects the outcome. *PubMed Central, Scientific Reports.*

5. Eric, G. & Anca, J., 2022. Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. *National Library of Medical Science.*

6. Frank, A., Subbey, S., Kobras, M. & Gjøsæter, H., 2021. Population dynamic regulators in an empirical predator-prey system. *Science Direct, Journal of Theoretical Biology,* Volume 527.

7. Government of Canada, 2022. *An introduction to the cyber threat environment,* ottawa: Canadan Centre for Cybersecurity.

8. Hans, d. B. & Marijn, J., 2017. Cybersecurity Awareness: The need for evidence-based framing strategies. *Elsevier, Government Information Quarterly.*

9. Heloise, P., 2022. The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication.*

10. Jiaze, T., Huiling, C., Mingjing, W. & Amir, H. G., 2021. The Colony Predation Algorithm. *Journal of Bionic Engineering.*

11. Mugwagwa, A., Chibaya, C. & Bhero, E., 2023. A survey of inspiring swarm intelligence models for the design of a swarm-based ontology for addressing the cyber security problem. *INTERNATIONAL JOURNAL OF RESEARCH IN BUSINESS AND SOCIAL SCIENCE,* 12(4), pp. 483-494.

12. Muro, C., Escobedo, R., Specto, L. & Coppinger, R., 2021. Wolf-pack (Canis lupus) hunting strategies emerge from simple rules in computational simulations. *Elsevier, Behavioural Processes,* Volume 88, pp. 192-197.

13. NIST, N. I. o. S. a. T., 2011. *Managing Information Security Risk,* s.l.: nist.

14. Noah, B., Victor, L. & Frithjof, L., 2021. Seasonal dynamics of a generalist and a specialist predator on a single prey. *Mathematics in Applied Sciences and Engineering* .

15. Ponnusamy, V. et al., 2021. Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks. *Tech Scoence Press, Computer Systems Science & Engineering,* .

16. Rui, T., Simon, F., Xin-She, Y. & Deb, S., 2012. Wolf search algorithm with ephemeral memory. *2012 Seventh International Conference on Digital Information Management (ICDIM).*

17. Sikender, M. M. & Lakshmisri, S., 2018. Security Automation in Information Technology. *SSRN Electronic Journal,* pp. 901-905.

18. Thomas, J. H., Kevin, D. & Murray, L., 2021. Increasing availability of palatable prey induces predator-dependence and increases predation on unpalatable prey. *PubMed Central, Scientific Reports* .

19. Weitzenfeld, A. & Vallesa, A., 2006. A Biologically-Inspired Wolf Pack Multiple Robot Hunting Model. *IEEE Latin American Robotics Symposium, LARS.*

20. World Economic Forum, 2022. *Global Cybersecurity Outlook 2022, Insights Report January 2022,* s.l.: s.n.

21. Wu, H. & Zhang, F., 2014. Wolf pack algorithm for unconstrained global optimization.. *Mathematical Problems in Engineering.*

22. Xuan, C. et al., 2021. An improved Wolf pack algorithm for optimization problems: Design and evaluation. *PLOS ONE.*

23. Xuan, C. et al., 2021. An improved Wolf pack algorithm for optimization problems: Design and evaluation. *PLos One.*

24. Yuchong, L. & Qinghui, L., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Elsevier,* pp. 8176-8186.