ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

DEVELOPING AN ADAPTIVE INTELLIGENT MULTI-AGENT SYSTEM FOR ENHANCED NETWORK PROTECTION

Nkechi Uzoamaka Okoro

Department of Computer Science, Faculty of Physical Sciences, Imo State University, Owerri, Nigeria

Abstract

The aim of this research is to design an adaptive intelligent multi-agent for network protection, the objective is to provide a faster network by application of the multi-agent concept of a distributed artificial intelligence idea, to enhance the network intrusion detection systems (IDS) of existing technology, to provide a system that allows a network element to engage in adaptive behavior by easy communicating and sharing of resources in other to solve a problem faster and to provide an enhance system that could monitor intruders into a network. The motivation towards this study is from the inability to protect the network during request of multiple transactions and network failure due to attack on the network. An object oriented analysis design methodology (OOADM) will be used for the system analysis and design while employing the unifield modeling language (UML) for the development of the multi-agent network protection architecture and the programming language will be PHP, HTML and MySQL as backend and database design. These development tools were chosen because of their simplicity and flexibility in coding, easy integration and deployment. The expected results will be an adaptive intelligent multi-agent network protection system that will solve the current problems witnessed by many organizations network on the issues of network attack, delay on the processing of requested transactions and constant network failure. The proposed system is intended to apply multiple agents architectural model to processes request as they come in by unique communication between the in the system agents. The communication will help speed-up processing speed of the network and hence report any witnessed attack made from any angle for an immediate action

Keywords: Multi-agent system (MAS), Distributed Artificial Intelligence (DAI), Intrusion Detection System (IDS), Denial of Service (DoS), Data Loss Prevention (DLP).

1. INTRODUCTION

BACKGROUND OF THE STUDY

A multi-agent system is a computerized system built of several interacting intelligent agents (Hu *et al.*, 2021). Multi-agent systems can tackle problems that are difficult or impossible for an individual agent or a monolithic system to solve. (Hu *et al.* 2021) Intelligence may include methodic, functional, procedural approaches, algorithmic search or reinforcement learning (Hu *et al.* 2021).

Multi-Agent Systems (MAS) have been employed recently in a variety of fields, including robotics, networking, automation, simulation, and logistics. The success of MAS is mostly attributable to their aptitude for social behavior development and capacity for addressing computationally challenging (or spatially distributed) tasks

(one of the main conditions of agent intelligence). Due to all of these factors, MAS are currently a well-established study area in which numerous intriguing studies relating to tools and design approach have been presented. This study will be focusing on the application of MAS to provide protection of networks. Every day, networks are being used by an exponentially increasing number of individuals, many users attempt to enter private networks as a result they are so worried by attacks that are wicked. Consequently, networks are more protected, it is more important than beneficial, real distributed hosts must be monitored, along with their different interactions and exchanges. This problem's intricacy necessitates the deployment of a multi-agent system.

This study proposes to provide an adaptive intelligent multi-agents for network protection to simulate network security management, in particular network intrusion detection, is its main objective. The current network security management systems are very expensive and sophisticated; a versatile, adaptive, and reasonably priced security system that offers more autonomy is required.

In order to find and address this problem, it is vital to analyze how traditional intrusion detection is implemented and carried out. Multi-agent systems strike a compromise between the need for security and the flexibility and adaptability of the system in this situation.

In fact, the creation of innovative applications for intelligent agent technology is thought to be one of the fastest expanding fields in telecommunication research. A collection of unique named agents with distributed surroundings makes up the DAI (Distributed Artificial Intelligence) idea (Gasser, 2018). Each agent works together and exchanges information with the others, making the optimal (or, in some cases, optimum) judgment is made possible by the agent's knowledge, experience, and data from nearby agents.

In this study, the researcher proposes to integrate DAI approach based on multi-agent computer vision techniques in intrusion prevention systems to enhance network Intrusion Detection Systems (IDS). Multi-agent systems (MAS) have the potential to integrate adaptive features in networks, allowing network elements to engage in adaptive behavior and develop "intelligent" properties. When a network entity exhibits behavior autonomy, adaptation, interaction, communication, and cooperation in order to accomplish a task, it is said to be "intelligent".

STATEMENT OF THE PROBLEM

Security has been one of the vital problems facing many IT organizations worldwide especially when the company solemnly does its business through a web network. But the existing network protection in used by these organizations has been found to weak in protecting their network. This study was able to identify some of the following problems in the existing network protection use by some companies as follows:

1. Inability to protect the network during multiple transactions
2. Because of the delay caused by multiple transaction, the existing network protection could not process some task fast

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

3. The existing system is weak causing more intruders into the network

AIM AND OBJECTIVES OF STUDY

The aim of this study is to design an adaptive intelligent multi-agent for network protection.

The objectives are:

1. To provide a faster network by application of the multi-agent concept of a distributed artificial intelligence idea.
2. To enhance the network intrusion detection systems (IDS) of existing technology
3. To provide a system that allows a network element to engage in adaptive behavior by easy communicating and sharing of resources in other to solve a problem faster.
4. To provide an enhance system that could monitor intruders into a network

2. LITERATURE REVIEW

In this current digital age, most people and organizations have become reliant on the internet for their daily necessities with the rise of the internet activities, cyber threats has also increased substantially (Kong, 2021). The security of network and computer systems becomes increasingly important as the amount of sensitive information being stored and deployed online increases In recent years majority of institutions and large organizations has suffered a substantial increase in cyber-threats, scams, exploits and other malicious contents. Cyber-attacks are targeted towards business and privates firms on a daily basis and the variations in which these attacks are made have also increased. Individual are also subjected to cyber-threats as they store their personal information on their mobile phones and make use of insecure public networks (Snider *et al.* 2021). Cyber attackers can use an individual's or a company's sensitive data to steal information or gain access to their financial accounts, among other potentially damaging actions, which is why it is essential for individuals and organizations alike to adopt or employ the use of cyber security programs or professionals to keep their information secured from the prying eyes of the web (Snider *et al.* 2021).

Cyber Attacks and Their Forms

According to (Bada and Nurse, 2020), a cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors. It is also referred to as the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties. There are various forms and ways in

which individuals or organizations can be subjected to threats and network attacks. Listed below are the most common cyber threats faced by both individuals and organizations alike (Bada, and Nurse, 2020); **Malware:**
This is one of the most common types of cyber-attacks. Malware or malicious software such as spyware, viruses, adware, etc, are intruding software that are developed by cyber attackers or hackers to destroy, damage and steal relevant data and information from a computer.

Phishing:

Phishing is a prominent widespread type of attack carried out by sending out fake mails to the individual, tricking the receiver into providing sensitive information such as; bank and credit card details and passwords. **Denial of Service (DoS) Attack:**

The DoS attack is notably a significant threat most especially to organizations. The organizations networks or computers are being flooded with irrelevant requests from attackers, exhausting their bandwidth and resources preventing them from responding to legitimate or relevant requests.

Password Attack:

This is a form of attack in which a hacker decodes your password with various programs and password cracking tools like Aircrack, Cain, Abel, Hashcat, etc. Or out-rightly guessing or using brute force attacks. With the right password a hacker has access to a wealth of information.

5. Man in the Middle Attack:

This occurs when an attacker comes in between a two-party transaction and hijacks the session between client and host. By doing so the hackers filters, steals and manipulates the information.

Network and Network Security

According to (Sengupta *et al.* 2020) a network is the connection of at least two computer systems, either by a cable or a wireless connection. A simpler form of network is the combination of two computers connected by a cable. This type of network is called a peer-topeer network that does not have any hierarchy, both participants have equal privileges. Each computer has access to the data of the other device and can share resources such as disk space, applications or peripheral devices. As these networks grow and become more complex and as organizations rely more on their network and data to conduct their business, security becomes more important. Network security covers all the various aspect taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber-attacks, like distributed denial of service. This aims at

securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data has a degree of solutions against many cyber threats (Sengupta *et al.*, 2020).

Network Security Protections

There are various methods or measures taken for network security and protection as stated by (Xu *et al.*, 2022).

Firewall:

The firewall is the first and foremost line of defense for any network. Firewall can either be hardware, software or both, it monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewall keep out unfriendly traffic and is a necessary part of daily computing. Network Security relies heavily on Firewalls, and especially Next Generation Firewalls, which focus on blocking malware and application-layer attacks (Xu *et al.*, 2022).

Intrusion Prevention Systems (IPS)

This is a form of network that helps to detect and prevent identified threats and network security attacks. An intrusion prevention system monitors the network continually, trying to identify possible malicious incidents and capture information about them. A vulnerability is a weakness for instance in a software system and an exploit attacks that leverage on that vulnerability to gain control of that system. An Intrusion Prevention System can be used in these cases to quickly block these exploits (Xu *et al.*, 2022).

Anti-malware software

Malware, in the form of viruses, Trojans, worms, key-loggers, spyware, and so on, is designed to spread through computer systems and infect networks. Anti-malware tools are a kind of network security software designed to identify dangerous programs and prevent them from spreading. Anti-malware and antivirus software may also be able to help resolve malware infections, minimizing the damage to the network (Xu *et al.*, 2022).

Email Security

Email Security are the processes, procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks (Xu *et al.*, 2022).

Data Loss Prevention (DLP)

Often times, the weakest link in network security are caused by humans. Data loss prevention (DLP) helps protect staff and other users from misusing and possibly compromising sensitive data or allowing said data out of the network. Data loss prevention (DLP) is a cyber-security methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization.

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

Access Control

This is a security technique that involves identifying a user based on their credentials and then authorizing the appropriate level of access once they are authenticated thereby denying unsanctioned access, and maybe threats. Integrations with Identity and Access Management (IAM) products can strongly identify the user and Role-based Access Control (RBAC) policies ensure the person and devices are authorized access to the asset. Examples are passwords, pins, security token, biometric scans (Xu *et al.*, 2022).

Multi Agent Systems (MAS)

Dorri et *al*. (2018) defined a multi-agent system as a computerized system composed of multiple interacting intelligent agents that can solve problems that are difficult or impossible for an individual agent or a monolithic system to solve. Multi agent systems are applied in the real world to graphical applications such as computer games. Agent systems have been used in films. It is widely advocated for use in networking and mobile technologies, to achieve automatic and dynamic load balancing, high scalability and self-healing networks.

Types of Multi-Agent System (MAS)

In multi-agent systems, there are agents and their surroundings. Normally, software agents are discussed in multi-agent systems research. However, a multi-agent system's agents could just as easily be robots, people, or human teams. Mixed human-agent teams may be present in a multiagent system. The type includes:

1. Passive agents (Kubera *et al.*, 2010) or "agent without goals" (such as obstacle, apple or key in any simple simulation)
2. Active agents (Kubera *et al.*, 2010) with simple goals (like birds in flocking, or wolf–sheep in prey-predator model)
3. Cognitive agents (complex calculations)

Agent environments

Agent environments can also be organized according to properties such as accessibility (whether it is possible to gather complete information about the environment), determinism (whether an action causes a definite effect), dynamics (how many entities influence the environment in the moment), discreteness(whether the number of possible actions in the environment is finite), periodicity (whether agent actions in certain time periods influence other periods), (Russell, 2003) and dimensionality (whether spatial characteristics are important factors of the environment and the agent considers space in its decision making). (Salamon, 2011) Agent actions are typically mediated via an appropriate middleware. This middleware offers a firstclass design abstraction for multi-agent systems, providing means to govern resource access and agent coordination (Weyns *et al.*, 2007).

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

Applications MAS

MAS have not only been applied in academic research, but also in industry (Leitão *et al.*, 2015) MAS are applied in the real world to graphical applications such as computer games. Agent systems have been used in films. (massivesoftware, 2012). It is widely advocated for use in networking and mobile technologies, to achieve automatic and dynamic load balancing, high scalability and self-healing networks. They are being used for coordinated defense systems. Other applications (Leitao *et al.*, 2016) include transportation, (Xiao-Feng *et al.*, 2012) logistics, (Máhr *et al.*, 2010) graphics, manufacturing, power system, (semanticscholar, 2019) smart grids (semanticscholar, (2019) and Geographic Information Systems (GIS). Also, Multi-agent Systems Artificial Intelligence (MAAI) are used for simulating societies, the purpose thereof being helpful in the fields of climate, energy, epidemiology, conflict management, child abuse,

(Hallerbach *et al.*, 2018). Some organization's working on using multi-agent system models include Center for Modeling Social Systems, Centre for Research in Social Simulation, Centre for Policy Modeling, Society for Modeling and Simulation International. (Hallerbach *et al.*, 2018) discussed the application of agent-based approaches for the development and validation of automated driving systems via a digital twin of the vehicle-under-test and microscopic traffic simulation based on independent agents. (Hallerbach *et al.*, 2018) Waymo has created a automated vehicles. People's behavior is imitated by artificial agents based on data of multiagent simulation environment Car craft to test algorithms for self-driving cars (Madrigal *et al.*, 2020) It simulates traffic interactions between human drivers, pedestrians and real human behavior.

3. MATERIALS AND METHODS METHODOLOGY ADOPTED

The object oriented analysis design methodology (OOADM) was adopted for this study because of its popular technical approach for analyzing and designing an application, system, or business by applying object-oriented programming, as well as using visual modeling throughout the development life cycles to foster better stakeholder communication and product quality. In the aspect of producing an advanced model by using unified Modeling Language (UML) which will follow the OOADM object designing approach in providing a detailed design on how the MultiAgent Systems (MAS) technology could help detect protect a network and facilitate transaction on the network. Nevertheless, the proposed adaptive intelligent multi-agents for network protection system modeling will be designed following the OOADM stages /approach: ObjectOriented Analysis, Object-Oriented Design and Object-Oriented Implementation.

Phase 1: Object-Oriented Analysis

In this stage, the problem is formulated, user requirements are identified, and then a model is built based upon real–world objects. The analysis produces models on how the desired system should function and how it must be developed.

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

The requirement looked into includes:

User Functional Input Requirements:

Functional Requirement describes the use cases and actors that are found in the adaptive intelligent multi-agents for network protection system. Each use case is described in details with diagrams achieved by the UML in their respective module section. These use case diagrams model the desired behavior of the system. The Functional requirement is categorized in two (2) main modules:

1. Manager layer 2. Local layer

The manager layer has the responsibility to managing the global security of a network. This network can be local or distributed. In this layer the researcher identified three levels of agents:

1. Security Policy Manager Agent (SPMA)
2. Extranet Manager Agent (EMA)
3. Intranet Manager Agent (IMA)

The Security Policy Manager Agent (SPMA) manages the security policies specified by the security officer.

The Extranet Manager Agent (EMA) manages the security of the entire distributed network. Its role is to manage and control Intranet Manager Agents (IMA). These agents report pertinent analysis to the EMA. The role of the user is then to perform another analysis on suspicious events in order to confirm or not the detection of an attack.

It can also ask for another data processing and delegate then new monitoring tasks to the IMAs. The Extranet Manager Agent communicates with the Security Policy Manager Agent. This user can specify new security policy, new monitoring tasks or new attacks to detect. The EMA is also responsible for distributing the set of Local Agents to each IMA.

The Intranet Manager Agent (IMA) manages the security of a local network. It controls the Local Agents and analyzes the monitored events reported by these agents. The manager layer use case diagram is shown in figure 3.1 below:

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

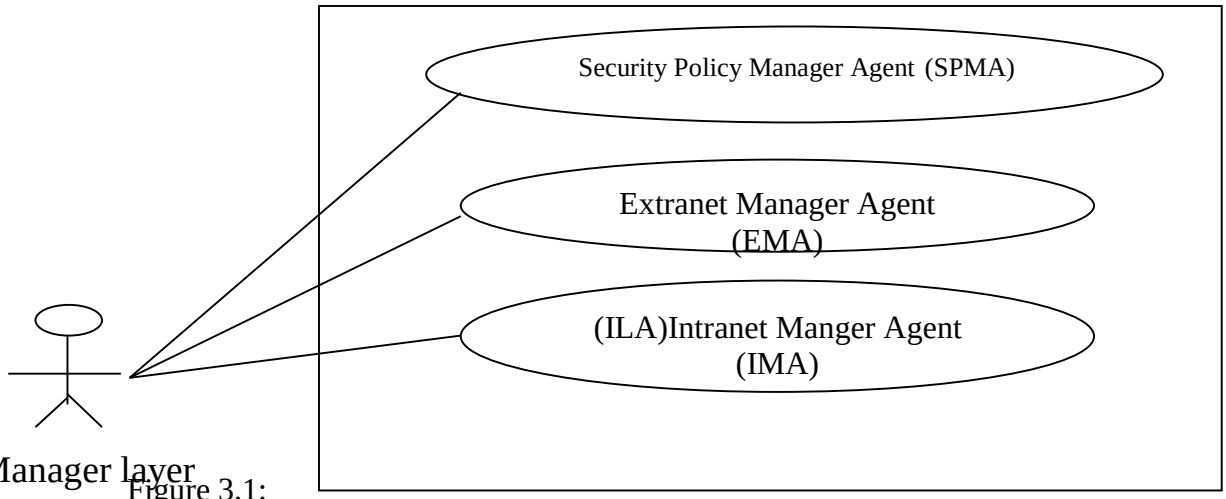


Figure 3.1: Use Case Diagram of Manager layer User Module

Local layer User Module

The Local Layer manages the security of a domain, which is constituted by a set of hosts. This layer is composed of a group of Local agents, which have specific functions. In fact, the Manager Layer specifies to the Local Layer the activities that must be monitored. These activities can be classified in Extranet, Intranet and Local activities. According to this classification, the study distinguishes three kinds of Local Agents: The use case diagram below illustrates various activities required by the local agents on the platform shown in figure 3.2.

i. Extranet Local Agent (ELA) ii. Intranet Local Agent (ILA) iii. Internal Local Agent (ILA)

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

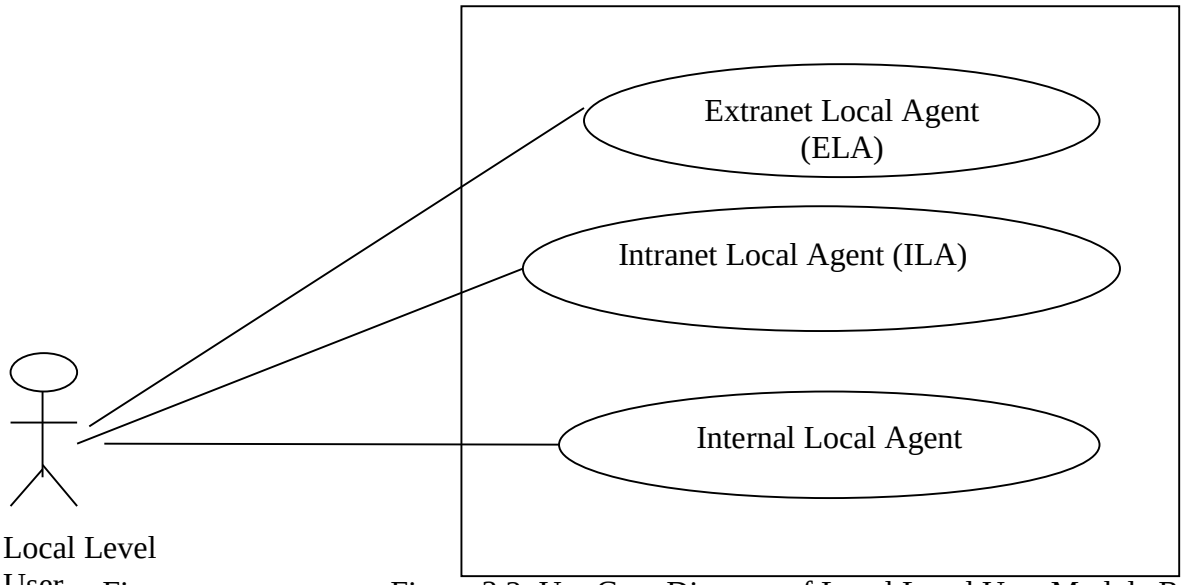


Figure Figure 3.2: Use Case Diagram of Local Level User Module Requirement

SYSTEM ANALYSIS

System study aims at establishing requests for the system to be acquired, developed and installed. Analyzing the problem thoroughly forms the vital part of the system study. In system analysis, prevailing situation of problem is carefully examined by breaking them into subproblems. Problematic areas are identified and information is collected. Data gathering is essential to any analysis of requests. It is necessary that this analysis familiarizes the designer with objectives, activities and the function of the organization in which the system is to be implemented.

ANALYSIS OF THE EXISTING SYSTEM

Securing a network involves protecting it against all possible attacks. But, in practice it is not possible to have a completely secure network. So, the problem is how to detect in real time security violations. The existing network security and detecting systems have been doing their best in the reduction of signal failure and delay but are achieve that through a single channel. The channel receives a signal, service every transaction no matter the number of transactions which causes network failure and poor signal. The existing system do not have a stronger protection devices that could identify a poor signal or when there is an attack on the network causing a network break down and malfunctioning of the entire system operation.

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

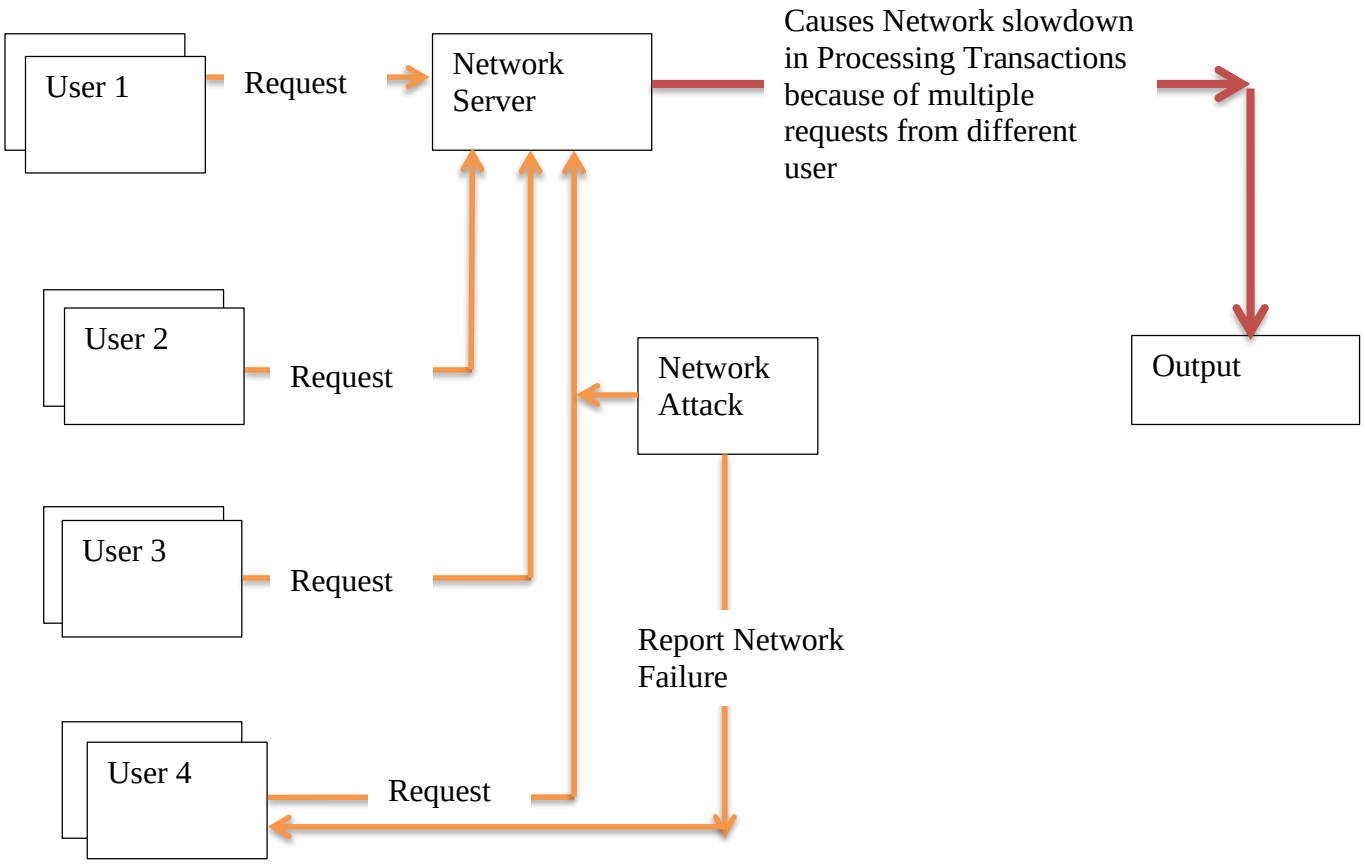


Figure 3.3: Diagram showing analysis of existing system

WEAKNESSES OF THE PRESENT SYSTEM

The present network protections systems are found with the following weaknesses are follows:

1. Constant attack on users transactions causing queue and process failures on the server because there is no intelligent device that can detect and report if such occurs without allowing it to affect other activities on the network.
2. Limited network server are used to attend to request from multiple users from different location
3. There is no immediate response to attack if occurs on the network
4. There is no circle communication between the devices which also makes it possible for intruders to easily have access to the network and once they do causes heavy damage on the entire network

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

ANALYSIS OF THE PROPOSED SYSTEM

The analysis of the proposed system is categorized in two different ways: the function of the manger layer and the local layer shown in figure 3.4.

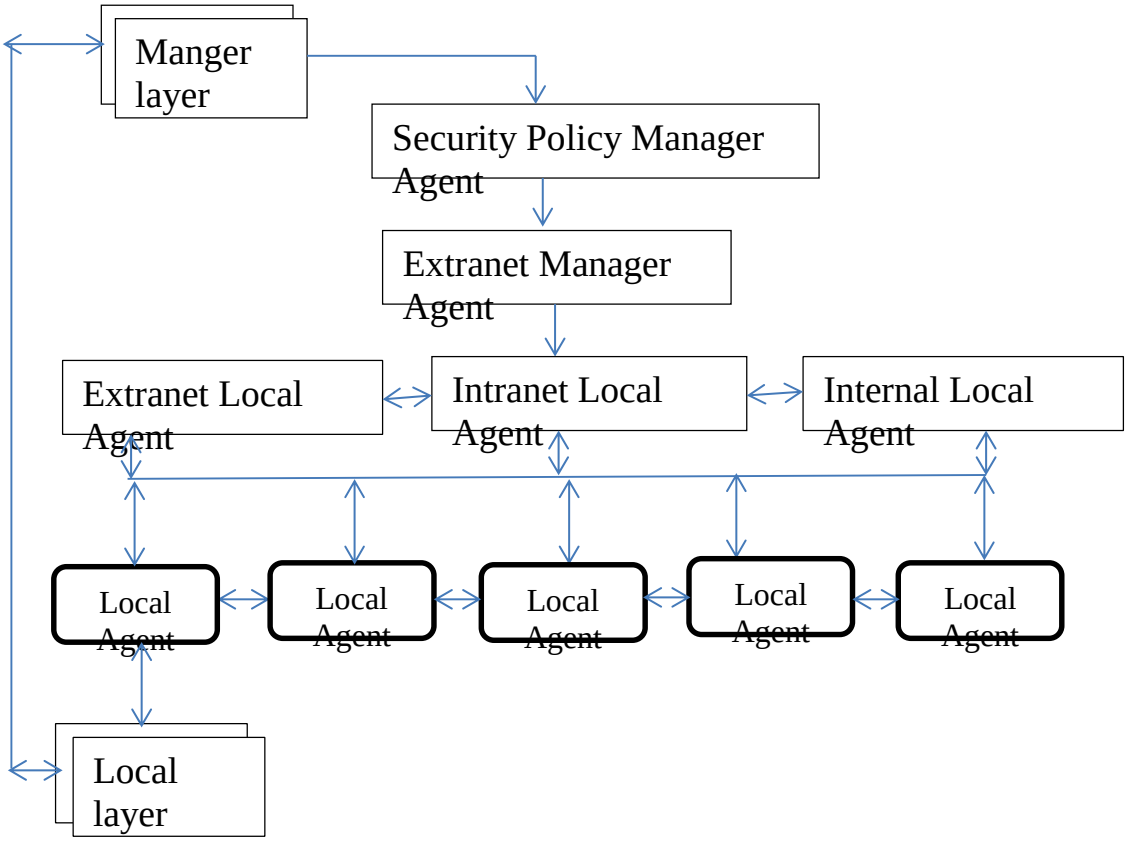
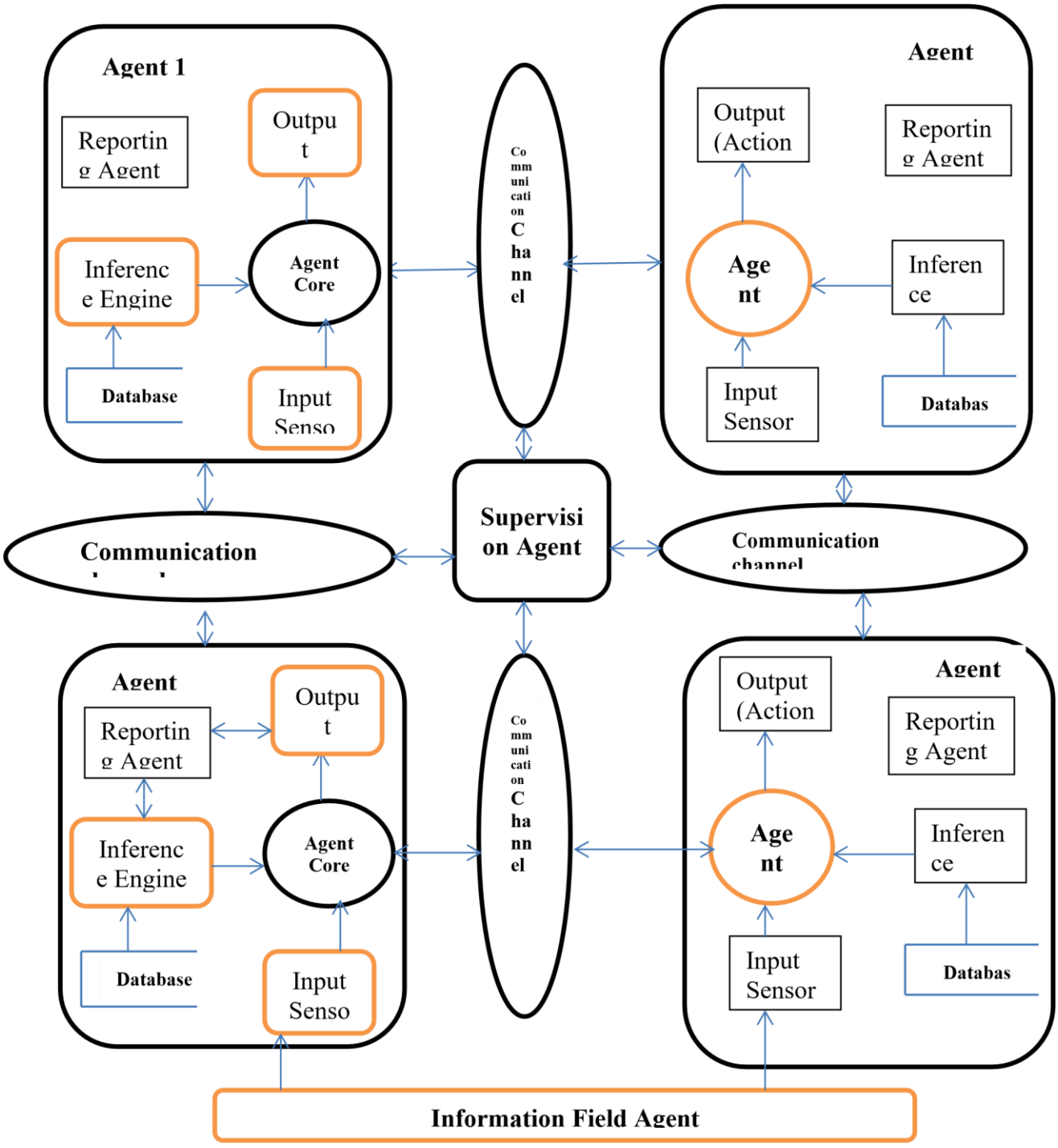


Figure 3.4 Functional analysis diagrams between the manager layer and the local Layer of the proposed System

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article



ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

Figure 3.5 Analysis of the proposed multi agent system

The propose multi-agent based architecture is shown in figure 3.5, this diagram illustrate how the system handles request from different user, if a request is made to the Agent 1, and immediately another request comes in, the request could be handled by the second agent 2 etc. From the diagram, one could see that there is a circle communication between the four agents trying to ensure that all request made are treated and delivered on time. In other for an attack to be identified, there is a reporting agent that detects an attack an automatically takes an action while other transactions are being processed by other agents.

NOTE: The supervision module coordinates interactions between the different modules using a finite state automaton while the communication module manages the interactions between the agent and the other agents of its group(s), no matter what machine they are running on. It defines the mailbox of the agent and the way the messages are received and enquired for later interpretation. An agent may need some others information to refine its analysis. In this case, it asks other agents to give it the necessary information.

ADVANTAGES OF THE PRESENT SYSTEM

The present system of network protection has its own advantages base on the fact that the present system could permit the network administrator block a preferred network or transaction without automatically initiating the request and also the present system does not require random communication between other servers before taking an action which the proposed system does.

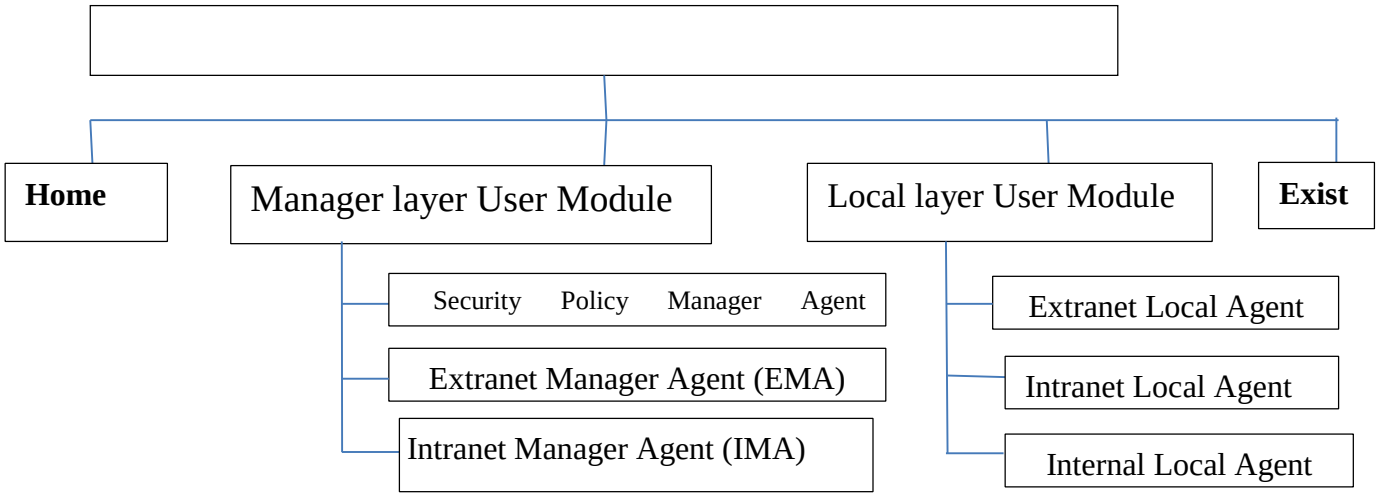


Figure 3.6 High Level Model of proposed system

HIGH LEVEL MODEL OF PROPOSED SYSTEM Adaptive intelligent multi-**agent network protection system**

ISSN: 3064-8270

Artificial Intelligence, Machine Learning, and Data Science Journal

Research Article

4. RESULT AND DISCUSSION

In this study, the researcher underlined the network intrusion detection requirements. The study presented some existing systems and illustrated their limitations. Mainly, the flexibility, autonomy, adaptability and distribution were the principal features to be addressed to build a suitable architecture that fulfills these requirements. Thus, the introduction of a multi-agent system was proposed as a mean of modeling and implementing adaptive decision. The multiagent system makes intrusion detection more flexible. In fact, the autonomy given to the agents reduces considerably the implication of the security officer in security management (Supervision module agent) and makes its administration tasks easier and faster.

Therefore the expected result of the adaptive intelligent multi-agent network protection system is to solve the current problems witnessed by many organizations network on the issues of network attack, delay on the processing of requested transactions and constant network failure. The proposed system is intended to apply multiple agents to processes request as they come in by unique communication between the four agents. The communication will help speed-up processing speed of the network and hence report any witnessed attack made from any angle for an immediate action.

DISCUSSION

Having reviewed some related studies on this research, the researcher was able to identify some research gap which the current study tends to fill, which includes: The network protection techniques could not grant access to multiple request and processing leading to failure and delay to request made by users, also not all organization understands the architecture of the multi-agent technology approach in network protection which there is need to introduce a lecture to government owned organizations to adopt the technique for adequate security of their network and improved service delivery.

5. CONCLUSION

The work proposed to design a multi-agent intelligent system which is a system that can handle multiple transaction/data despite the request from various users. Ensuring that all the request made by the various users are handled timely and also have the ability to detect an attack on the system and report the attack for adequate action to avoid the system from braking down. The study employed the object oriented analysis design methodology (OOADM) to enable a more clear and detailed analysis and design of the new system by using the object oriented concept. Both the existing system and new system was explained in details capturing the users and drawn by the use case and data flow diagram on the flow of the transactions and where they are stored. The system has input agent that collects data from various users, inference engine agent that analysis and provide the intelligent base on the inference rule that checks from knowledge and passes it to the reporting agent that sends

the signal base of the status of the transactions to the output agent that now displays the result on the screen for the user. Once there is an attack, it will be detected by the attack agent depending where the attack is coming from, the transaction will not still stop rather the duty of the attack agent is to detect the attack on time, report it through the reporting agent while the inference engine agent will indicate if the agent is free or not which if it does, will push the transaction to the next available agent to continue with processing of the transaction. Therefore, all the mechanisms thoroughly discussed in this study proved to work well together and provide the needed security in any professional setting and hence processes received data by application of intelligence.

REFERENCES

Abutair, H. Y., & Belghith, A. (2017). A multi-agent case-based reasoning architecture for phishing detection. *Procedia Computer Science*, *110*, 492-497.

Achbarou, O., El Kiram, M. A., Bourkoukou, O., & Elbouanani, S. (2018). A new distributed intrusion detection system based on multi-agent system for cloud environment. *International Journal of Communication Networks and Information Security*, *10*(3), 526.

Alruwaili, F. F. (2020). Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. *PeerJ Computer Science*, *6*, e323.

Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2017). Real-time multi-agent system for an adaptive intrusion detection system. *Pattern Recognition Letters*, *85*, 56-64.

Grzonka, D., Jakóbik, A., Kołodziej, J., & Pllana, S. (2018). Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security. *Future generation computer systems*, *86*, 1106-1117.

Guo, X., Zhang, D., Wang, J., & Ahn, C. K. (2021). Adaptive memory event-triggered observerbased control for nonlinear multi-agent systems under dos attacks. *IEEE/CAA Journal of Automatica Sinica*, *8*(10), 1644-1656.

Louati, F., & Ktata, F. B. (2020). A deep learning-based multi-agent system for intrusion detection. *SN Applied Sciences*, *2*(4), 1-13.

Rahman, M. S., Orchi, T. F., Saha, S., & Haque, M. E. (2019, August). Multi-agent approach for overcurrent protection coordination in low voltage microgrids. In *2019 IEEE Power & Energy Society General Meeting (PESGM)* (pp. 1-5). IEEE.

Sampaio, F. C., Leao, R. P., Sampaio, R. F., Melo, L. S., & Barroso, G. C. (2020). A multiagent-based integrated self-healing and adaptive protection system for power distribution systems with distributed generation. *Electric Power Systems Research*, *188*, 106525.

Sethi, K., Madhav, Y. V., Kumar, R., & Bera, P. (2021). Attention based multi-agent intrusion detection systems using reinforcement learning. *Journal of Information Security and Applications*, *61*, 102923.

Trifonov, R., Tsochev, G., Pavlova, G., Yoshinov, R., & Manolov, S. (2017, August). Adaptive Optimization Techniques for Inteligent Network Security. In *2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)* (pp. 219223). IEEE.

Uzair, M., Li, L., Zhu, J. G., & Eskandari, M. (2019, November). A protection scheme for AC microgrids based on multi-agent system combined with machine learning. In *2019 29th Australasian Universities Power Engineering Conference (AUPEC)* (pp. 1-6). IEEE.

Wang, P., & Govindarasu, M. (2020). Multi-agent based attack-resilient system integrity protection for smart grid. *IEEE Transactions on Smart Grid*, *11*(4), 3447-3456.

Zhang, D., Feng, G., Shi, Y., & Srinivasan, D. (2021). Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. *IEEE/CAA Journal of Automatica Sinica*, *8*(2), 319-333.