**INTELLIGENT AGENTS DEFENDING FOR AN IOT WORLD: A REVIEW**

**209074206**

**FAKOREDE OLUMIDE DANIEL**

# CHAPTER 1

1.0 INTRODUCTION

The emergence of the Internet of Things (IoT) has brought about a paradigm shift in the way we interact with devices and systems around us. The interconnection of heterogeneous devices, ranging from household appliances to industrial machinery, has opened up a world of possibilities for automation, efficiency, and convenience (Perera et al., 2014; Xu et al., 2014; Zanella et al., 2014). However, this interconnectivity also introduces new security challenges that traditional cybersecurity measures may not be equipped to handle effectively.

The IoT ecosystem is characterized by a vast number of devices with varying computational capabilities, operating systems, and communication protocols. These devices often lack robust security features, making them vulnerable to attacks and exploits (Stankovic, 2014). Additionally, the sheer volume of data generated by IoT devices presents a significant challenge for intrusion detection and prevention systems (IDS/IPS) (Desai et al., 2015; Rivera et al., 2015).

Traditional IDS/IPS solutions, which rely on signature-based detection or anomaly-based detection techniques, may not scale well in the IoT environment (Coulter and Pan, 2018). Signature-based detection can only identify known threats, leaving the system vulnerable to zero-day attacks. Anomaly-based detection, on the other hand, can generate a high number of false positives, leading to increased operational costs and inefficiencies (Sobh, 2006).

1.1 PROBLEM STATEMENT

The inherent complexity and heterogeneity of the IoT ecosystem pose significant challenges for traditional intrusion detection and prevention systems. Existing solutions struggle to cope with the sheer volume of data generated by IoT devices, the diversity of communication protocols, and the varied computational capabilities of these devices (Desai et al., 2015; Rivera et al., 2015). Furthermore, the lack of robust security features in many IoT devices makes them vulnerable to a wide range of attacks, including zero-day attacks, which traditional signature-based detection techniques are ill-equipped to handle (Coulter and Pan, 2018).

The limitations of traditional IDS/IPS solutions in the IoT context have led to a growing interest in the development of intelligent, adaptive, and autonomous intrusion detection agents capable of addressing the unique challenges of this environment (Coulter and Pan, 2018; Zhao and Ge, 2013). These intelligent agents must be able to learn and adapt to new threats, collaborate with other agents in a distributed manner, and take autonomous actions to mitigate or prevent attacks (Igbe et al., 2016; Liu et al., 2012; Sreelaja and Pai, 2014).

1.2 AIMS AND OBJECTIVES

This research aims to investigate how current intrusion detection approaches fulfill the role of intelligent agents, the requirements for autonomous action against compromised intelligent and distributed IoT nodes, and the vulnerabilities, challenges, and applicable methodologies.

Review literature on traditional and distributed intrusion detection approaches, and model them as intelligent agents for an IoT perspective.

Define and Identify various key terms across intrusion detection, AI, and IoT domains, defense cycle requirements for defensive agents, relevant manufacturing and security challenges, and considerations for future development.

1.4 METHODOLOGY

To achieve the stated aims and objectives, this research will employ a combination of theoretical and empirical methods, drawing from the fields of computer science, cybersecurity, artificial intelligence, and multi-agent systems.

* A comprehensive review of existing literature will be conducted to gain a thorough understanding of the current state of intrusion detection and prevention techniques, focusing on their applicability and limitations in the IoT context. This will involve analyzing research papers, technical reports, and industry publications related to IoT security, multi-agent systems, machine learning, and artificial intelligence.
* A discussion of the characteristics and types of intelligent agents, as well as their applications in IDS.
* The review will also include a discussion of the challenges and limitations of using intelligent agents in IoT security.

1.5 CONCLUSION

In conclusion, intelligent agents have the potential to play a significant role in enhancing the security of IoT devices. Their ability to operate autonomously and make decisions based on their environment and goals makes them well-suited to the challenges of IoT security. However, the development and deployment of intelligent agents in IoT security is a complex task that requires careful consideration of the characteristics and types of agents that are relevant to this field. Further research is needed to fully explore the potential of intelligent agents in IoT security.

REFERENCES

Igbe, O., Darwish, I., & Saadawi, T. (2016). Distributed network layer security management using multi-agent system. 2016 IEEE Symposium on Computers and Communication (ISCC), 917-922.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by Internet of Things. Transactions on Emerging Telecommunications Technologies, 25(1), 81-93.

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32. Stankovic, J. A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), 3-9.

Desai, M. M., Desai, M. M., & Desai, M. M. (2015). Internet of things: A survey. International Journal of Computer Science and Engineering (IJCSE), 3(7), 2786-2790.

Rivera, J., & van der Meulen, R. (2015). Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. Gartner Newsroom.

Coulter, R., & Pan, L. (2018). Intelligent agents defending for an IoT world: A review. computers & security, 73, 439-458.

Sobh, T. S. (2006). Efficient signature discovery for intrusion detection systems. The 4th ACS/IEEE International Conference on Computer Systems and Applications, 1-8

Sreelaja, N. K., & Pai, G. V. (2014). Stream-based random wireless sensor network using ant optimization and distributed agents for securing iot enabled environments. International Journal of Communication Networks and Information Security (IJCNIS), 6(2).