Innovative Computing Review (ICR)

Volume 1 Issue 2, Fall 2021
ISSN(P): 2791-0024 ISSN(E): 2791-0032
Journal DOI: https://doi.org/10.32350/icr
Issue DOI: https://doi.org/10.32350/icr/0102
Homepage: https://journals.umt.edu.pk/index.php/icr

Article: **Mobile Agent (MA) Based Intrusion Detection Systems (IDS): A Systematic Review**

Author(s): Farzana Kausar Gondal

Affiliation: Deparment of Computer Science, Gold Campus, Superior University, Lahore, Pakistan

Citation: K. G. Farzana, “Mobile Agent (MA) Based Intrusion Detection Systems (IDS): A Systematic Review”, *Innova Comput Rev*, vol. 1, no. 2, pp. 85–102, 2021. https://doi.org/10.32350/icr/0102/05

Journal QR

Article QR

Farzana Kausar

Estd. 1990

A publication of the
School of Systems and Technology
University of Management and Technology, Lahore, Pakistan

Mobile Agent (MA) Based Intrusion Detection Systems (IDS): A Systematic Review

Farzana Kausar Gondal[1]*

ABSTRACT: An Intrusion Detection System (IDS) identifies the attacks by analysing the events, considered undesirable from a security perspective, in systems and networks. It is necessary for organizations to install IDS for the protection of sensitive data due to an increase in the number of incidents related to network security. It is difficult to detect intrusions from a segment that is outside a network as well as an intrusion that originated from inside a distributed network. It should be the responsibility of IDS to analyse a huge amount of data without overloading the networks and monitoring systems. Mobile agents (MA) emerged due to the deficiencies and limitations in centralized IDS. These agents can perform predefined actions by detecting malicious activities. From previously published literature, it was deduced that most of the existing IDS based on MA are not significantly effective due to limited intrusion detection and high detection time. This study categorized existing IDS and available MA-IDS to conduct a strategic review focusing on the classification of each category, that is, data collection modes, architecture, analysis techniques, and security. The limitations and strengths of the discussed IDS are presented/showcased wherever applicable. Additionally, this study suggested ways to improve the efficiency of available MA-IDS in order to secure distributed networks in the future. This overview also includes different implementations of agent based IDS.

INDEX TERMS: data mining, distributed systems, Intrusion Detection System (IDS), Mobile Agents (MA), network security

I. INTRODUCTION

The security of computer systems should be taken into consideration because it has turn out as the stake of companies [1].

[1]Deparment of Computer Science, Gold Campus, Superior University, Lahore, Pakistan
*Corresponding Author: farzana.gondal@gmail.com

Identification mechanism of different activities over a network that may lead to compromise in the policy of security is known as intrusion detection technique [2]. IDS aggregates/collects and analyzes a huge amount of data that is gathered from multiple access points of a network [3]. An intrusion is a group of actions aimed to harm any resource's confidentiality, integrity and availability (CIA triad). An intrusion occurs when a system's CIA guarantees are violated and vulnerabilities in security are exploited by an attacker or a group of attackers. Therefore, it is pertinent to have a system to detect intrusion in form of an auxiliary protection wall [2]. IDS keeps track of all outgoing and incoming network activities. It also detects unknown actions that may indicate a system intrusion or attack trying to intrude into a system [3]. IDS is an authorized mechanism used to detect and identify illegal users, vulnerabilities, and attacks having the potential to affect or damage the functioning of computer systems properly. Some sets of predefined actions are executed when IDS detects an intrusion [4]. Intrusions must be identified immediately to enact quick and effective remedial or corrective actions. Hence, IDS is a crucial part of any security infrastructure since it is used to deal with network attacks [5]. The main objective of IDS is to detect unexpected access patterns and then respond to keep the system secure [6, 7].

Therefore, existing mobile agent intrusion detection systems (MA-IDS) are critically examined in this paper. The organization of the paper as follows: IDS is explained in second section in detail; third section provides an introduction of mobile agents; fourth section provides classification of IDS; fifth section analyses the existing available MA-IDSs; sixth section discusses the proposed architecture by considering the current design's shortcomings; the last section provides the conclusion of the work.

II. INTRUSION DETECTION SYSTEM

In [8], some of the required features for IDS have been defined by authors with a focus on two themes: performance requirements and functional requirements.

Some of the characteristics of these requirements are summarized in [3] and given in the following section.

A. Functional Requirements

- IDS should monitor continuously and report the intrusion immediately [3].
- In IDSs, the false alarm rate must be very low [3, 8].
- IDS must generate sufficient information to repair the system in case an intrusion is detected since IDS only provides alerts to the administrators without any recommendation of corrective actions [8, 9].
- IDS should react and detect coordinated and distributed attacks [9].
- IDS must adapt to the changes made in configuration and the network topology [3].

B. Performance Requirements

- Real-time intrusion detection should be done to reduce network damage [3].
- Scalability should be a part of IDS to handle additional loads of communications and computation [3, 10].

III.1 IDS Limitations

In the initial designs, IDS faced the following shortcomings [2], [3], [10]:

- High rate for false positive alerts.
- *Degradation of efficiency*: In a network, when IDS has to face a large number of events, it will drop the network packets and also slow down the system.
- *Vulnerability for attacks*: Hierarchical structures provide opportunities to attackers to easily harm the IDS.
- Time delay.
- A single point of failure.
- Reduced scalability.
- Mutual communication among different IDSs is difficult.

IV. MOBILE AGENTS

At present, mobile agent technology is implemented to IDS in order to solve the aforementioned shortcomings. It is a specific software type agent that is capable of moving between multiple hosts over the network. MA is a software application that existed autonomously in a certain environment. It achieves its goals by sensing the environment and acting upon the available knowledge base [2].

A. Mobile Agent Advantages

Mobile agents have the advantage of using static components in IDS [3] as specified below.

1) Improved Network Latency: As the agents directly operate on the host, hence they give a response faster as compared to the hierarchical systems, where the central coordinator has to take the actions [2], [3].

***2) Network Load Reduction*:** Network load is reduced by sending only the agent code instead of audit data to central stations from sensors, since audit data may increase to huge amounts [3], [11].

***3) Autonomous and synchronous Execution*:** To prevent the whole network, the agents can execute autonomously even when their parent process doesn't exist anymore [3, 12].

4) Support for Heterogenous Platforms: Agents can run on hosts having any platform and are not platform dependent [11].

5) Dynamic Adaptation: Any feature can be added or removed to the system at run-time due to dynamic behaviour of the agents [3].

6) Static Adaptation: System restart is not required for an update of the agent's algorithm when an attack signature is added to the IDS [3].

7) Scalability: By dividing at different hosts, the computational load can be reduced on the system by using mobile agents [12].

***8) Fault Tolerance/ Robustness*:** Due to the robust nature of mobile agents, fault tolerance is not an issue [11, 12].

Due to these features, mobile agent technology is really effective for solving the intrusion detection in a distributed network [13]. Hence, giving advent to MA based IDS.

B. Mobile Agent Limitations

Some shortcomings faced by MA-IDSs [2] include three limitations.

1) High Time to Detection: There is a compatibility issue between the speed of MA solutions and the needs of IDS. One major challenge for MA-IDS is to improve the speed for the identification of malicious activities [2, 15].

2) Performance: Although the detection performance of the MA paradigm increased extensively, the detection is still not effective for autonomous attacks. Even though agents are often written using scripting languages that support portability for different platforms, still their execution mode is very low comparatively against native codes [2, 16].

3) Security: Another shortcoming is to protect from attacks, the protector i.e. MA-IDS [2, 17].

V. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Proper classification and good taxonomy have significant beneficial effects on the research of any field. Previously, several surveys have been conducted to define taxonomies and the classification of intrusion detection [18]. However, there is still no widely acceptable or applicable taxonomy for intrusion detection. "This may be, because of, it being a young research field and due to inherent complexity" [19].

This paper aimed to classify IDS based on its basic features. The details of the proposed IDS classification are illustrated in Figure 1. Each element of this classification is discussed below.

A. Framework

The collection points where information is collected are either network-based or host-based and are represented as leaf nodes in a hierarchical framework. The internal nodes receive and aggregate the event information from several leaf nodes [20]. Furthermore, the abstraction, data reduction, and correlation take place at higher nodes and continue until the root node is accessed.

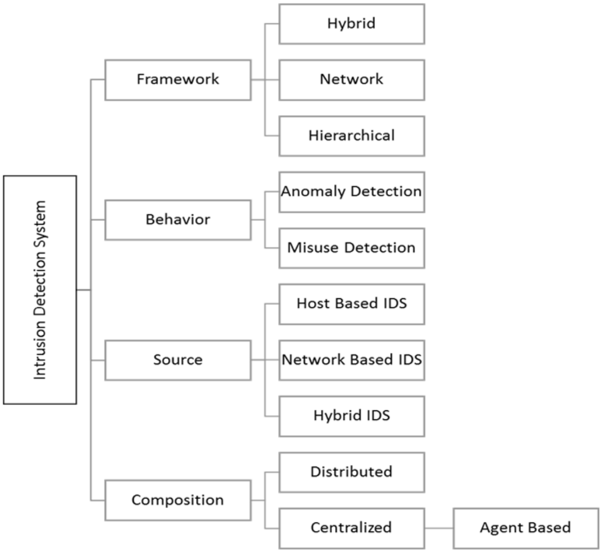

Fig.1. Classification of IDS

The intrusion detection and response generation are the responsibility of the root node, which is not only the command but also the control system. Information can move between any nodes in a network IDS framework. The collection and correlation of data, as well as the command-and-control system are integrated into every monitored system. Hybrid IDS comprises both a hierarchical IDS framework and a network [3, 20].

B. Intrusion Detection Behaviour

There are two types of intrusion detection behaviour: anomaly detection and misuse detection. Anomaly IDS identifies the usage of normal behaviour patterns to detect any intrusions. Any deviation found from the normal constructed behaviour is determined to be an intrusion. Well defined attack patterns are used by the Misuse intrusion that exploits the application software to detect intrusion and vulnerabilities found in the system. These patterns are already defined and are used to compare the behaviour of the user to detect any sign of intrusion [21].

C. Source

Host-based IDS, also known as HIDS [3], derives and utilizes information from a single host of a system, whereas network-based IDS, also known as NIDS, utilizes the information that is derived from a LAN segment. Conversely, hybrid IDS [22] is a term used to describe a system that combines both NIDS and HIDS.

D. Composition

After 1980, when IDS was first introduced, several IDSs were designed and implemented for the centralized system [23]. The data analysis is done in centralized IDS on fixed locations, regardless of the number of hosts that are monitored. Distributed IDS analyzes a huge amount of data without putting additional load on monitored systems and the network. In a computing system, distributed sources are used to obtain data [2]. The distributed information is gathered by mobile agents autonomously and intelligently across the network. The limitations of the centralized system are overcome by the MA based IDS by performing distributed correlation with the use of the mobility feature of agents [3, 24].

VI. Analysis of Available MA-IDSs

The technology of mobile agents has been proposed for intrusion detection due to the reduced cost of communication and new threats adaptability. New detection features can be easily added without restarting or rebuilding the IDS due to the independent execution of the agents. The following research in the domain of MA-based IDS was conducted focusing on the framework, data collection modes, security, their strengths and weaknesses.

A. Autonomous Agents for Intrusion Detection (AAFID) [25]

1) Framework: AAFID implements a hierarchical design based on the host to overcome the centralized system's limitations. There are three layers in the system. The upper layer is called the procedure of the lower layer. Information is collected by the agent at the base level, after which suspicious data is searched. Subsequently, the collected information is sent to the transceiver in the top layer, as well as the one in each host. At a higher level, one or more transceivers send data to the monitors, which they subsequently evaluate.

2) Data Collection: Audit router delivers the audit information to the agents, which enables them to communicate with each other. Audit router contains the database of agents that are running. Agents after registering to this database get a handle that helps them communicate with other agents.

3) Security: The AAFID architecture faces the problem of security as traditionally in the field of research of distributed systems.

4) Technique: The higher-level elements in the AAFID architecture are Transceivers and Monitors. They are involved in the central analysis of the data based on the host as well as the network. The feasibility of the AAFID architecture is described and experimented by implementing the working prototypes using Perl and C language, having the advantage of easy portability for different platforms.

5) Strength: Transceivers and monitors use system scalability to detect distributed attacks.

6) Problem: One of the major drawbacks of AAFID architectures is the delay in detecting the intrusion between monitor and agents caused by layers. Furthermore, the monitors constitute a single point of failure.

B. Intelligent Mobile Agents for Intrusion Detection System (IMA-IDS) [26]

1) Framework: IMA-IDS framework is based on four kinds of agents.

a) *Collector agent:* This agent is distributed over the network and is responsible for collecting the events which occurred in the host.

b) *Correlator agent:* It gathers critical information and forwards it to the appropriate analyser agent. The predefined set of rules, specifying crucial events, are used by the correlator agents.

c) *Analyzer agent:* Several analysis operations are performed by this agent, such as signature detection, protocol analysis, and anomaly detection.

d) *Manager agent*: They generate alarms if they identify any anomaly in the results reported by the analyzer agents.

Communication agents can get information from other agents by requesting the manager agent.

2) Data Collection: Data collection is based on both the network as well as the host.

3) Technique: IDS is based on the centralized IDS model. The results, generated by the collector agents, inform the manager agent. who then passes them on to the analyzer agents. A higher level of correlation and analysis (anomaly and policy detection) is performed by the analyzers. Subsequently, the results of the analyzer agents are sent to the manager, and if any anomaly is found, they activate the alarms.

4) Security: The security mechanism uses asymmetric cryptography to exchange keys between different hosts. This mechanism is based on Aglet Framework.

5) Strength: Its agents can not only gather data but also respond to situations. They have increased efficiency, scalability, and flexibility when operating in a heterogeneous environment. Java is used to write the whole system, which makes this agent very portable. It is able to run on any platform supporting Java.

6) Problem: One of the major disadvantages of the IMA-IDS architecture is the security. If an attacker has deep knowledge and expertise of Aglet, then mobile agents can be modified to harm the host, due to which the host can cause damage to the mobile agents.

C. A Mobile Agent-based Programmable Hybrid Intrusion Detection System (APHIDS) [27]

1) Framework: APHIDS uses a network-based framework and places an agent engine in the network at each site. Its implemented in the form of a distributed layer on top of the engines of the distributed agent. By designing a system that can distribute tasks efficiently and flexibly for analysis and monitoring, this framework takes advantage of mobile agent technology. It is also capable of existing detection technologies integration.

2) Data Collection: Data collection and detection activities are distributed by this architecture to the host and the network, both of which are the existing monitoring systems.

3) Security: In this framework, the security for the agents is not considered.

4) Technique: Anomalous activity on the network is defined as trigger. For detection action, the trigger agent has to be programmed.

A set of Distributed Correlation Script (DCS) is provided as input to the system. It correlates a trigger event with a set of analytical activities to be executed when an event is detected. MA are implemented for a distributed analysis and search.

5) Strengths: The use of lightweight analysis agents reduce the bandwidth usage during log data transfer. Expert knowledge regarding administrator of security is gathered by DCS and automating standard processes of investigation that are carried out in response to an occurrence.

6) Problem: Agent's security is not taken into account.

D. Mobile Agent for Network Intrusion Resistance [28]

1) Framework: The following components are contained in the designed framework of IDS.

a) *Manager*: It controls and adjusts other parts of the system. It also maintains configuration information of other components. It receives alarms in response to intrusions from the host MA monitor. Subsequently, an intrusion response is executed by it.

b) *Host monitor MA*: Over the network, this is maintained on every host. In response to the intrusion, an appeal is sent to the manager by the monitor of the host MA to directly report the anomaly activity. Once the appeal is received, the manager distributes a data gathering MA patrolling to collect the information. Upon detecting the distributed intrusion, an intrusion response MA is activated by the manager to respond to each host being monitored intelligently.

2) Data Collection: In this framework, the source of data is both networks as well host based. There are different types of data collection, such as audit records and system logs.

3) Technique*s*: The log files of the monitored host system are analysed by the mobile agent, which are then compared with the predefined signatures of the attacks to detect abnormal actions or intrusions.

4) Security: Aglet response is the security mechanism base of this framework.

5) Strengths: This system changed the traditional hierarchical structure of a distributed IDS.

6) Problem: A significant part of the IDS is carried out by the control centre. The system can collapse if the location is discovered by this centre.

E. Intrusion Detection Agent System (IDA) [29]

1) Framework: It is an intrusion detection technique based on the implementation of the mobile agent. It is based on a basic framework that includes several types of agents, sensors, and a central manager for each network segment. The collection and analysis of the information is the responsibility of the central manager.

The network traffic is monitored by the sensors. The first type of agent examines the logs in detail and is known as Information Gathering Agent (IGA). The second type of agent is named the tracing agent. It is responsible for tracing the attack source. These agents work by coordinating with IDAs. The communication board must facilitate agents to communicate with the manager and each other as well.

2) Data Collection: Agents collect the information on the intruder and the intrusion. The central manager collects and analyses the information using sensors.

3) Security: The agent's security is managed from a central location.

4) Technique:The main goal of IDA is to detect intrusions by scanning MLSI or to detect any marks left by an intruder who is currently in the stage of mark.

5) Strength: The agent distribution and communication protocol are fully described.

6) Problem: One of the main drawbacks of the IDA architecture is scalability since only a few sensors and agents are dealt with by the central managers.A comparison of the classification features of the reviewed MA-IDS is illustrated in Table 1. It is observed that some of these IDS are still facing drawbacks while some are strong in comparison.

TABLE 1

COMPARISON OF REVIEWED MA-IDS

Sr. No.	Paper	Framework	Behavior	Data Collection	Security	Technique	Strength	Problem
1	[25]	Hierarchical	Anomaly Detection	Network based	Not Considered	Central Analysis	Scalability	Delay in detection
2	[26]	Network	Hybrid	Hybrid	Asymmetric Cryptography based on Aglet Framework	Statistical Analysis	Scalability & Portability	Security
3	[27]	Network	Anomaly Detection	Hybrid	Not Considered	Correlation Scripts	Lightweight Analysis Agents	Agent Security Not Considered
4	[28]	Hierarchical	Hybrid	Hybrid	Aglet Framework	Analysis Based on Rules	Improved Hierarchical Structure	Central Control
5	[29]	Hybrid	Misuse Detection	Host Based	Centrally managed	MLSI (Marks Left by Suspected Intruder)	Communication Protocol	Scalability

VII. Suggested Features for MA-IDS Improvements

In [30, 31] authors suggested that the research on use of mobile agents in IDS should be considered in these three categories as follows

A. New Detection Paradigm

The intrusion detection techniques must be improved.

B. New Architecture Paradigm

New Architecture Paradigm should decide upon the architecture of the IDS according to the requirements of the systems by answering these questions. Does it follow network IDS architecture, Hybrid IDS architecture, or hierarchical architecture of IDS?

C. Amendments

Amendments should be made to the design that exists already. For example, the rate of false alarm can be reduced.

To address the limitations of the available IDS based on MA and enhance the MA-IDS, this article presents some suggestions based on the features given below:

1) Framework: The nature of hierarchical architecture is inflexible because of the lines of communication and exact functioning that tend to become connected with their components as discussed in the section on IDS categorization. Due to the unconstrained flow of communication, the network framework faces an issue related to the inefficiency in communications [2]. A hybrid model enabling free communication is recommended as the method of merging the best features of network and hierarchical systems.

2) Behaviour: As in the case of anomaly-based IDS, a hybrid approach is proposed based on the combination of both misuse and anomaly in order to solve the problem of high false positive.

3) Source: Network as well as Host based.

4) Security: “Because an agent's code cannot be altered by an attacker to make it harmful, security risks can be significantly reduced if processing is restricted by MA-IDS system to just those agents who are signed digitally by a security administrator” [2].

Signing the code or any other object with a digital signature is a fundamental mechanism required to protect an agent. A digital signature can be defined as an electronic equivalent of any hand-written signature, which may be used to verify an object's integrity, validity, and origin. In light of these efficient and secure features, Digital Signature Algorithm (DSA) is suggested to secure the mobile agents.

5) Technique: Data mining techniques, focusing on the extraction of closed frequent patterns, are used for detecting intrusions.

VIII. CONCLUSION

This study showcased an unconventional classification of a typical IDS. Furthermore, the selected features of the existing MA-IDS, such as framework, data collection, technique of detection, security and strength measures along with the weaknesses, were critically reviewed in this study. It is explored that these existing systems are facing yet some drawbacks and strengths as well. Subsequently, suggestions were outlined based on the identified limitations to enhance the MA-IDS. IDS are critical for ensuring the survival and security of information systems against intrusions. Many network resources are used by centralised IDS and is the only failure point. The shortcomings of centralised IDS were addressed by using MA platforms. These platforms operate the system effectively and dynamically. Moreover, they respond to the rules of an event and changes of network. MA-IDS are better than centralised IDS in terms of performance and can report intrusions instantaneously. A general definition of IDS architecture, requirements, and limitations is provided in this paper. It also provides a comprehensive comparison of several IDS. In future more work will be done for detecting attacks in large data which are even more complex.

REFERENCES

[1] X. Sun, Y. Zhang, and R. Liu, "Design of security integrated monitoring system based on Internet of things," in *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, 2021, pp. 429-432. https://doi.org/10.1109/ICISCAE52414.2021.9590670

[2] S. A. Onashoga, A. D. Akinde, and A. S. Sodiya, "A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems," *Issues in*

Informing Science & Information Technology, vol. 6, 2009.

[3] N. Patil, C. Das, S. Patankar, and K. Pol, "Analysis of distributed intrusion detection systems using mobile agents," in *2008 First International Conference on Emerging Trends in Engineering and Technology*, 2008, pp. 1255-1260.

[4] D. Gurven Vaseer and P. S. Patheja, "Intrusion Detection a Challenge: SNORT the savior", *International Journal of Computer Trends and Technology*, Vol 45, 2017

[5] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Procedia Computer Science*, vol. 167, pp. 636-645, 2020.

[6] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. M. Chaabani, and A. Taleb-Ahmed, "Network intrusion detection system using neural network and condensed nearest neighbors with selection of NSL-KDD influencing features," in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, 2021, pp. 23-29. https://doi.org/10.1109/IoTaIS50849.2021.9359689

[7] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, pp. 1-27, 2021. https://doi.org/10.1186/s42400-021-00077-7

[8] W. Jansen, W. Jansen, T. Karygiannis, and D. Marks, *Applying mobile agents to intrusion detection and response*: US Department of Commerce, National Institute of Standards and Technology, 1999.

[9] Z. Mu, H. Liu and C. Liu, “Design and implementation of network intrusion detection system,” In *2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, IEEE, 2020, 494-497, 2020.

[10] A. Thakkar and R. Lohiya, "A survey on intrusion

detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review*, pp. 1-111, 2021. https://doi.org/10.1007/s10462-021-10037-9

[11] O. M. Okonor, "*Improving Energy Efficiency in Cloud Computing Data Centres Using Intelligent Mobile Agents*," University of Portsmouth, 2021.

[12] G. Tsochev, R. Trifonov, S. Manolov, and G. Pavlova, "Investigation Of Secure Mobile Agents As A Tool In Intrusion Detection Systems," in *2020 International Conference on Mathematics and Computers in Science and Engineering (MACISE)*, 2020, pp. 114-118.

[13] P. C. Chan and V. K. Wei, "Preemptive distributed intrusion detection using mobile agents," in *Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2002, pp. 103-108.

[14] R. Leszczyna, "A Review of Traffic Analysis Attacks and Countermeasures in Mobile Agents' Networks," *Moving technology ethics at the forefront of society, organisations and governments*, pp. 439-452, 2021.

[15] J. Ernst, T. Hamed, and S. Kremer, "A survey and comparison of performance evaluation in intrusion detection systems," in *Computer and network security essentials*, ed: Springer, 2018, pp. 555-568.

[16] H. Wang, Z. Wang, Q. Zhao, G. Wang, R. Zheng, and D. Liu, "Mobile agents for network intrusion resistance," in *Asia-Pacific Web Conference*, 2006, pp. 965-970.

[17] N. Patil, C. Das, S. Patankar, and K. Pol, "Analysis of distributed intrusion detection systems using mobile agents," In *2008 First International Conference on Emerging Trends in Engineering and Technology*, IEEE, 1255-1260.

[18] T. Hamed, J. B. Ernst, and S. C. Kremer, "A survey and

taxonomy of classifiers of intrusion detection systems," in *Computer and network security essentials*, ed: Springer, 2018, pp. 21-39.

[19] M. Almgren, E. Lundin, and B. E. Jonsson, "Consolidation and evaluation of IDS taxonomies," in *In Proceedings of the eighth Nordic Workshop on Secure IT systems (NordSec 2003*, 2003.

[20] R. Sharma and V. A. Athavale, "Survey of intrusion detection techniques and architectures in wireless sensor networks," *International Journal of Advanced Networking and Applications*, vol. 10, pp. 3925-3937, 2019.

[21] R. Lips and N. El-Kadhi, "Intelligent Mobile Agent for Intrusion Detection System (IMAIDS)," *European Institute of Technology. rue Pasteur-94270, Le Kremlin-France*, 2008.

[22] M. A. Hatef, V. Shaker, M. R. Jabbarpour, J. Jung, and H. Zarrabi, "HIDCC: A hybrid intrusion detection approach in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 30, p. e4171, 2018.

[23] J. P. Anderson, "Computer security threat monitoring and surveillance," *Technical Report, James P. Anderson Company*, 1980.

[24] M. Özalp, C. Karakuzu, and A. Zengin, "Distributed intrusion detection systems: A survey," *Academic Perspective Procedia*, vol. 2, pp. 400-407, 2019. https://doi.org/10.33793/acperpro.02.03.18

[25] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An architecture for intrusion detection using autonomous agents," in *Proceedings 14th annual computer security applications conference (Cat. No. 98EX217)*, 1998, pp. 13-24.

[26] R. Lips and N. El-Kadhi, "Intelligent Mobile Agent for Intrusion Detection System (IMAIDS)," *European Institute of Technology. rue Pasteur-94270, Le Kremlin-France*, 2008.

[27] K. Deeter, K. Singh, S. Wilson, L. Filipozzi, and S.

Vuong, "APHIDS: A mobile agent-based programmable hybrid intrusion detection system," in *International Workshop on Mobile Agents for Telecommunication Applications*, 2004, pp. 244-253.

[28] H. Wang, Z. Wang, Q. Zhao, G. Wang, R. Zheng, and D. Liu, "Mobile agents for network intrusion resistance," in *Asia-Pacific Web Conference*, 2006, pp. 965-970.

[29] M. Asaka, A. Taguchi, and S. Goto, "The implementation of IDA: An intrusion detection agent system," in *Proceedings of the 11th FIRST Conference*, 1999.

[30] M. Eid, H. Artail, A. Kayssi, and A. Chehab, "Trends in mobile agent applications," *Journal of Research and Practice in Information Technology*, vol. 37, pp. 323-351, 2005.

[31] M. El Fissaoui, A. Beni-hssane, S. Ouhmad, and K. El Makkaoui, "A survey on mobile agent itinerary planning for information fusion in wireless sensor networks," *Archives of Computational Methods in Engineering*, vol. 28, pp. 1323-1334, 2021.