Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 351047, 6 pages
http://dx.doi.org/10.1155/2013/351047

Review Article

Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks

Nabil Ali Alrajeh[1] and J. Lloret[2]

[1] *Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia*
[2] *Department of Communications, Universidad Politecnica de Valencia, Camino de Vera, 46022 Valencia, Spain*

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 13 September 2013; Accepted 21 September 2013

Academic Editor: S. Khan

Intrusion detection system (IDS) is regarded as the second line of defense against network anomalies and threats. IDS plays an important role in network security. There are many techniques which are used to design IDSs for specific scenario and applications. Artificial intelligence techniques are widely used for threats detection. This paper presents a critical study on genetic algorithm, artificial immune, and artificial neural network (ANN) based IDSs techniques used in wireless sensor network (WSN).

1. Introduction

Wireless sensor networks (WSNs) are distributed in nature where sensor nodes operate independently without any centralized authority. Furthermore, sensor nodes have many design and functional limitations in terms of storage, processing, and communication. WSN applications have evolved at very fast pace and are consistently growing in many fields of everyday life [1]. The fast growth of WSN applications demands more ubiquitous and service oriented computing. The fast growing applications, distributed nature, and design limitations of WSNs have resulted in the increase of network related vulnerabilities and threats. There is a need of proper security mechanisms for protecting sensor networks against potential security threats and attacks [2, 3].

The majority of security mechanisms designed so far for WSNs are capable of packet encryption or require authentication to restrict malicious user's access. Furthermore, many other security related solutions for WSNs have been proposed such as authentication, key exchange, and secure routing to prevent some specific attack. However, such security measurements cannot provide a wide range of protection against variety of security attacks and threats against WSNs. An IDS is one possible solution to address a wide range of security attacks in WSNs [4]. IDSs are passive in nature; that is, they are capable of detecting intrusion; however, they cannot prevent or defuse security attacks.

Research community is working on developing new methodologies for intrusion detection in WSNs [5]. Artificial intelligence provides many important and comparatively low cost techniques for designing IDSs while taking care of the energy consumption [6]. Few important intelligent techniques are artificial immune system, artificial neural network, and genetic algorithms.

IDSs based on artificial immune systems are inspired from human immune system. Human immune system is a complex defense system which has the capability to protect human body from foreign germs and other microorganisms. ANN based IDSs are inspired from human neuron system. An ANN is composed of number of neurons (basic processing elements) that are interconnected with each other through weighted connections. Genetic algorithm based IDSs utilize biological concepts of natural selection.

This paper presents short review of the existing intrusion detection mechanisms which are based on artificial intelligence techniques such as artificial immune system, artificial neural network, and genetic algorithm.

The paper is organized as follows. Section 2 analyzes IDSs based on artificial immune system. Section 3 shows the artificial neural network based IDSs. Genetic algorithm based

Table 1: Comparison of immune based IDSs.

IDS	Immune base mechanism	Accuracy	Lightweight	Attack types
[8]	DCA	N/A	No	ICP
[9]	DCA	Below 70%	No	ICP
[10]	Coevolutionary	Moderate	Yes	DoS, R2L, U2R
[11]	Adaptive immune	Above 75%	No	Network layer anomalies

IDSs are studied in Section 4. In Section 5, we conclude the paper.

2. Artificial Immune Based IDSs

This section investigates the applications of artificial immune based IDSs in WSNs. Artificial immune technique provides anomaly based detection of security threats against WSN. Human immune system is a complicated security system which safeguards the human body against many invisible organisms. Human immune system is very complex and consists of dendritic cells (D cells), T cells, and B cells [7].

D cells move in blood and collect information about antigens and dead cells. These cells basically activate response system. T cells are manufactured in bone marrow and are used to destroy infectious cells present in blood. B cells are white blood cells which are responsible for production of antibodies. Nowadays, artificial immune based systems have many applications in computing such as systems optimization, data classification, and intrusion detection.

The general architecture of IDS using artificial immune system is present in Figure 1.

Many works have been done in intrusion detection using artificial immune system.

An immune based mechanism for WSN is present in [8]. The authors claim that WSN is an area where immune based mechanisms can be applied easily. It is based on dendritic cell algorithm (DCA). Furthermore a new security threat called interest cache poisoning (ICP) attack is introduced. ICP is a network layer attack which is capable of disrupting routing packets. Both the DCA and directed diffusion are implemented on every sensor node to perform two tasks, that is, detection of misbehaving nodes and detection of antigens. The direct diffusion mechanisms are as follows:

(i) maintain two tables, that is, interest cache and data cache;

(ii) handle two types of packets, that is, interest packets and data packets.

The DCA monitors different types of signals such as danger signals and safe signals to detect ICP attack. This mechanism was evaluated and tested later on [9] to detect ICP attack; however, the detection rate was below 70%.

Another intrusion prediction technique based on coevolutionary immune system is present in [10]. This mechanism combines both coevolutionary immune system and grid computing features. The proposed system is compared and evaluated with pure immune system. The results show that the proposed system has better learning and understanding capabilities as compared to pure immune system. Furthermore, the proposed mechanism has better detection rate of variety of security attacks such DoS, R2L, U2R, and probing.

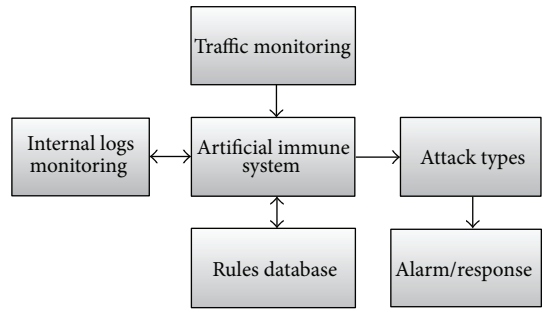

Figure 1: General architecture of IDS using artificial immune system.

Another proposal is present in [11] which is based on adaptive threat detection using immune system. In this work, a MAC layer gene is identified which is helpful in intrusion detection. Every node is equipped with natural selection algorithm to monitor the traffic behavior of surrounding neighbors. This mechanism is capable of detecting network layer anomalies such as packet drop. The detection accuracy of the system is below 85%.

Table 1 presents brief comparison of few immune based IDS.

As we know, WSNs are resource constraints such as memory, processing, and energy. Such constraints demand lightweight IDSs for such networks. In our opinion, the detection mechanisms present in [8, 9, 11] are not suitable for WSNs as they are involved in many processes and computations. The detection mechanism [8, 9] maintains two tables and handles two types of packets. Furthermore different types of signals are monitored for the detection of only ICP attack. Such kind of complex computations for the detection of one attack is not feasible for resource constraint WSNs.

The detection mechanism [11] is involved in identification of MAC layer gene and routing layer security attacks. The exchange of parameters between two different layers needs more resources in terms of memory, computation and energy.

3. Artificial Neural Network Based IDSs

Artificial neural network (ANN) is inspired from human nervous system, which is connected through neurons. Neural networks have the capability to understand and learn by training and can be used to identify complex trends. There

Table 2: Comparison of ANN based IDSs.

IDS	ANN based mechanism	Accuracy	Lightweight	Attack types
[12]	Backpropagation	Above 90% (in many cases)	No	Flooding
[13]	Unsupervised ANN	Above 80%	No	Time related changes
[14]	Feedforward	High	Yes	Malicious nodes

are two types of ANN architectures, that is, feedforward ANN and feedback ANN.

In feedforward ANN, the signals move in only one direction from input to output. In feedback ANN, the signals move in both directions.

ANN concepts are helpful in many areas such as pattern recognition and intrusion detection. ANN based intrusion detection can be helpful to eliminate the shortcomings of rule based IDSs. However, ANN based IDSs can be more effective if properly trained with both normal and abnormal data sets.

The general architecture of artificial neuron is given in Figure 2.

Many intrusion detection mechanisms based on ANN have been proposed for WSNs. In [12], ANN based mechanism for detection of energy exhaustion attack is proposed. The system is for cluster based WSN in which all the sensor nodes are capable of energy harvesting. It consists of three layers, that is, input layer, hidden layer, and output layer. It is trained to discriminate normal and abnormal events. The detection rate for routing attacks is above 95%; however, low detection rate is observed in case of channel access attack.

Intruder detection in WSN with an intelligent mobile robot response system is present in [13]. This mechanism uses an unsupervised neural network for intrusion detection. It detects time related changes using Markov model. Once an intruder is detected, a robot travels to the infected site for investigation. The results show that the detection rate is approximately 85%. As WSN nodes are deployed in harsh and unattended environment where the attacker can manage to compromise few of the nodes, few of the sensor nodes that are compromised may result in wrong data forwarding to the sink. Malicious node detection mechanism using ANN for WSN is proposed in [14]. This mechanism is designed for hierarchical WSN, where nodes sense and share information with neighbor nodes. This mechanism is based on feedforward technique of ANN. The authors claim that the proposed mechanism successfully identified malicious nodes even if 25% of sensor nodes are compromised.

Table 2 presents comparison of few ANN based IDSs.

Any mechanism which is designed for WSN should take care of limited resources of sensor nodes. In our opinion, the detection mechanisms which are present in [12–14] are not suitable for WSNs.

Although the mechanism [12] has high accuracy and the detection rate is above 90%, it has many requirements such as clustering in WSN, energy harvesting, backpropagation algorithm, and training of proposed mechanism.

The mechanism present in [13] is a costly approach as it involves a specialized robot to investigate the infected location.

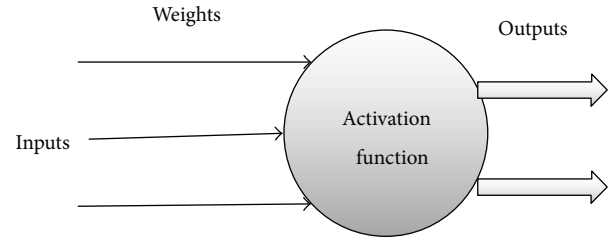

Figure 2: General architecture of artificial neuron.

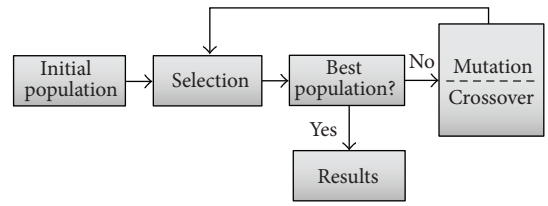

Figure 3: General architecture of genetic algorithm.

The proposal present in [14] seems to be lightweight; however, the claim about the accuracy of the system even in case of 25% malicious nodes needs further investigation.

4. Genetic Algorithm Based IDSs

Genetic algorithms are widely used in many areas of computing to solve a complex problem. It provides robust, adaptive, and optimal solutions for many computing related problems. Genetic algorithms in computing are inspired from biological processes such as natural selection, evolution, theory of mutation, and genetic inheritance.

The general architecture of genetic algorithm used in computing is present in Figure 3.

In genetic algorithm, the selection module derives most suitable answer or solution for some specific problem.

In crossover module, different parameters are exchanged out of different solutions in order to get new solutions.

Mutation module changes one or two parameters to get optimality in genetic algorithm.

Genetic algorithm is widely used technique in network security especially in designing and proposing IDSs. In IDSs, genetic algorithm can be used for classification of security attacks and for generating specific rules for different security attacks [15].

A lightweight IDS with reduced complexity using genetic algorithm for WSN is proposed in [16]. This work deals with measurement of sensor node suitability and attributes to

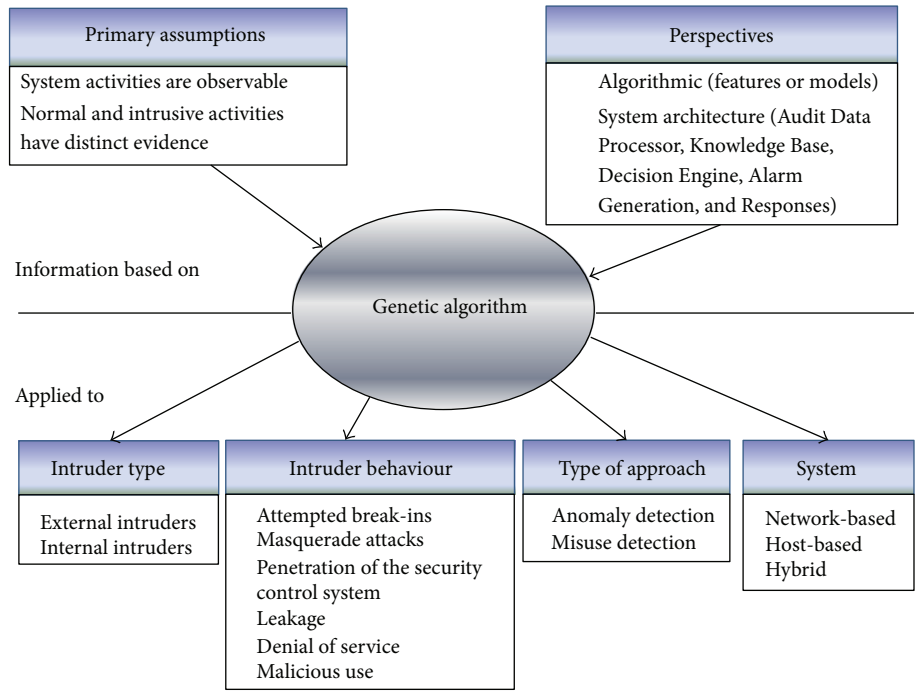

Figure 4: Intrusion detection systems and element types where genetic algorithms can be applied.

the perceived threat. A local monitoring node is introduced that acts like a proxy agent for the sink and is capable of monitoring neighbors. A Genetic algorithm based network IDS (GA-NIDS) is present in [17]. The proposed system considers many parameters such as protocol type, network services, and status of the connection to generate rules. The detection mechanism is trained on specific dataset, so that it can accurately identify and classify security attacks. In this mechanism, six rules are designed to detect six different types of denial of service (DoS) and probing attacks. The authors claim that the detection rate of DoS attacks is 100%.

Many IDSs are rule based where new and innovative attacks are not detected. An anomaly based IDS using concept of genetic algorithm is discussed in [18]. This framework uses set of classification rules which are derived from network audit data. It uses fitness function to monitor quality and stability of each rule.

Another evolutionary approach to intrusion detection is proposed in [19]. The proposed system is connected with a firewall, and it starts by capturing firewall entries. The data is then forwarded to genetic algorithm based system. The output of genetic algorithm is connected to an IDS. This mechanism is capable of detecting malicious connections and the detection rate is above 95%.

Table 3 presents comparison of few genetic algorithm based IDSs.

In our opinion, the detection mechanisms present in [17, 19] are not suitable for WSNs, as they demand more resources. The GA-NIDS considers many parameters such as protocol type, network services, and connection status for detection of an anomaly. Furthermore, different rules are designed for it which may consume more memory and energy due to computations involved in it.

Table 3: Comparison of genetic algorithm based IDSs.

IDS	Accuracy	Lightweight	Attack types
[16]	N/A	Yes	N/A
[17]	100%	No	DoS
[18]	N/A	Yes	Network layer
[19]	Above 95%	No	Malicious connections

The mechanism present in [19] takes input entries from firewall and forwards output entries to another IDS. Sensor nodes have limited processing capabilities, so they cannot operate with such complex mechanism for longer time.

When the genetic algorithm is applied to an IDS, several issues must be taken into account. The first one is the type of intrusion detection system purpose, and the second one is the element where it will be applied. Taking into account the classification provided in [20], we can draw Figure 4.

A general flow chart of a genetic algorithm for intrusion detection system will start using a randomly selected population of chromosomes. These chromosomes are encoded, on one hand, as observable system activities and evidence of normal and intrusive activities and, on the other hand, as the perspectives selected by the security administrator (Audit Data Processor, Knowledge Base, Decision Engine, Alarm Generation, and Responses). Figure 5 shows the general flow chart of a genetic algorithm for intrusion detection system.

5. Conclusion

Confidentiality, integrity, and availability of any network are of high importance. Network security is gaining importance

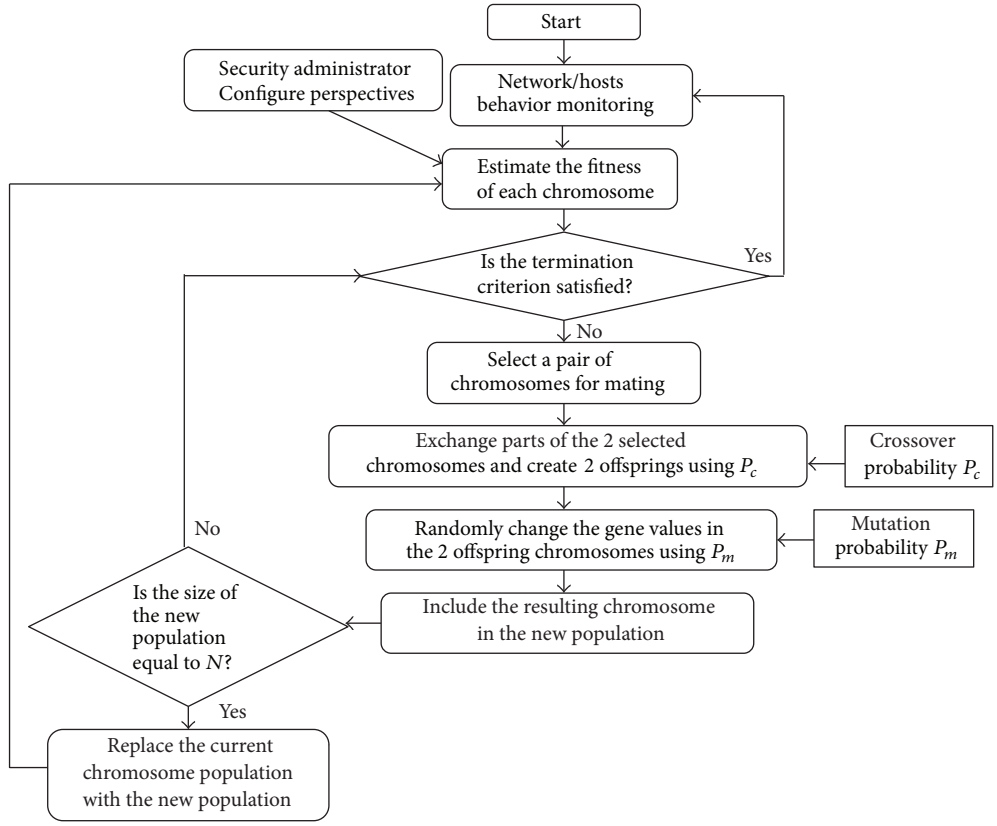

Figure 5: Flow chart of a genetic algorithm for intrusion detection systems.

as the attackers introduce new threats and security vulnerabilities to compromise the normal operations of network [21–23]. WSNs are more vulnerable to different security attacks as they are deployed mostly in unattended environments. IDSs are capable of detecting intrusions and informing the professionals well in time. There are many methodologies and techniques which are used to design IDSs.

Research community is exploring biological concepts to design different mechansisms to solve computing related problems. Similarly, many biological concepts such as artificial immune system, artificial neural network, and genetic algorithm are used in IDSs.

This paper provides brief discription of bioinspired IDSs and their suitability for WSNs.

Acknowledgment

The authors extend their appreciation to the Distinguished Scientist Fellowship Program (DSFP) at King Saud University for funding this research.

References

[1] D. Bri, M. Garcia, J. Lloret, and P. Dini, "Real deployments of wireless sensor networks," in *Proceedings of the 3rd International Conference on Sensor Technologies and Applications (SENSORCOMM '09)*, pp. 415–423, Athens, Greece, June 2009.

[2] A. Radhika, D. Kavitha, and D. Haritha, "Mobile agent based routing in MANETS—attacks & defences," *Network Protocols and Algorithms*, vol. 3, no. 4, pp. 108–121, 2011.

[3] K. Sahadevaiah and P. V. G. D. Prasad Reddy, "Impact of security attacks on a new security protocol for mobile ad hoc networks," *Network Protocols and Algorithms*, vol. 3, no. 4, pp. 122–140, 2011.

[4] N. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[5] M. S. Sisodia and V. Raghuwanshi, "Anomaly base network intrusion detection by using random decision tree and random projection a fast network intrusion detection technique," *Network Protocols and Algorithms*, vol. 3, no. 4, pp. 93–107, 2011.

[6] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting," *Ad Hoc & Sensor Wireless Networks*, vol. 2013, pp. 1–25, 2013.

[7] T. H. Lim, *Detecting anomalies in wireless sensor networks [Qualifying dissertation]*, Department of Computer Science, University of York, 2010.

[8] J. Kim, P. Bentley, C. Wallenta, M. Ahmed, and S. Hailes, "Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm," in *Artificial Immune Systems*, vol. 4163 of *Lecture Notes in Computer Science*, pp. 390–403, Springer, Berlin, Germany, 2006.

[9] C. Wallenta, J. Kim, P. J. Bentley, and S. Hailes, "Detecting interest cache poisoning in sensor networks using an artificial

immune algorithm," *Applied Intelligence*, vol. 32, no. 1, pp. 1–26, 2010.

[10] M. R. Ahmadi, "An intrusion prediction technique based on co-evolutionary im-mune system for network security (CoCo-IDP)," *International Journal of Network Security*, vol. 9, no. 3, pp. 290–300, 2009.

[11] M. Drozda, S. Schaust, and H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: performance and design principles," in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC '07)*, pp. 3719–3726, September 2007.

[12] N. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting," *Journal of Ad Hoc & Sensor Wireless Networks*, vol. 2013, pp. 1–25, 2013.

[13] Y. Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in *Proceedings of the IEEE Southeast Conference*, pp. 37–42, April 2008.

[14] P. Mukherjee and S. Sen, "Using learned data patterns to detect malicious nodes in sensor networks," in *Distributed Computing and Networking*, vol. 4904 of *Lecture Notes in Computer Science*, pp. 339–344, Springer, Berlin, Germany, 2008.

[15] B. Abdullah, I. Abd-alghafar, G. I. Salama, and A. Abd-alhafez, "Performance evaluation of a genetic algorithm based approach to network intrusion detection system," in *Proceedings of the International Conference on Aerospace Sciences and Aviation Technology*, Military Technical College, Cairo, Egypt, 2009.

[16] R. Khanna, H. Liu, and H.-H. Chen, "Reduced complexity intrusion detection in sensor networks using genetic algorithm," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–5, June 2009.

[17] A. Goyal and C. Kumar, "GA-NIDS: a genetic algorithm based network intrusion detection system," 2008, http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf.

[18] A. A. Ojugo, A. O. Eboka, O. E. Okonta, R. E. Yoro, and F. O. Aghware, "Genetic algorithm rule-based intrusion detection system (GAIDS)," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 3, no. 8, pp. 1182–1194, 2012.

[19] B. S. Dhak and S. Lade, "An evolutionary approach to intrusion detection system using genetic algorithm," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 2, pp. 632–637, 2012.

[20] T. S. Sobh, "Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art," *Computer Standards and Interfaces*, vol. 28, no. 6, pp. 670–694, 2006.

[21] A. Triviño-Cabrera and S. Cañadas-Hurtado, "Survey on opportunistic routing in multihop wireless networks," *International Journal of Communication Networks and Information Security*, vol. 3, no. 2, pp. 170–177, 2011.

[22] D. P. Franco, F. D. Barboza, and N. M. Cardoso, "A secure method for authenticity verification of handwritten signatures through digital image processing and artificial neural networks," *International Journal of Communication Networks and Information Security*, vol. 5, no. 2, pp. 120–126, 2013.

[23] N. Jeyanthi, N. Ch. S. Iyengar, P. Kumar, and A. Kannammal, "An enhanced entropy approach to detect and prevent DDoS in cloud environment," *International Journal of Communication Networks and Information Security*, vol. 5, no. 2, pp. 110–129, 2013.