Acta Scientific COMPUTER SCIENCES

Volume 3 Issue 10 October 2021

Review Article

Application of Malware Agent Based Datasets to Deep Learning Networks: A Review

Charles O Ugwunna[1]*, Moses O Onyesolu[1] and ChukwuNonso H Nwokoye[2]

[1]Nnamdi Azikiwe University, Awka, Nigeria

[2]Nigerian Correctional Service, Awka, Nigeria

***Corresponding Author:** Charles O Ugwunna, Nnamdi Azikiwe University, Awka, Nigeria.

Received: July 21, 2021

Published: September 14, 2021

Abstract

Implanting malware into servers or endpoints in a network has become a huge possibility in institutions that use the World Wide Web to accomplish tasks. Thanks to the penetration of connectivity due to the Internet and mobile devices into personal life, work, and entertainment, as well as the increasing number of smartphones and diverse IT applications. So is the application of both machine learning (ML) and deep learning (DL) models to a variety of programs used in big data analytics and data mining. On the other hand, the agent-based model (ABM) is a computer model for simulating the activities and interactions of autonomous agents. However, we enumerated some challenges of traditional models that gave rise to the use of ABM. With the observation that both ABM and ML/DL have yet to be applied to epidemics in communication networks, we reviewed the literature surrounding the aforementioned subjects. This is to provide the appropriate background for malware spread forecasts and the development of transitional methods from ABM to DL networks during representations of epidemic theory.

Keywords: Machine Learning; Deep Learning; Malware

Introduction

Lately, developments in the form of several connected devices like smart grids, cyber physical systems, the Internet of Things, the Internet of Vehicles, long-term evolution, and 5G communication have been changing constantly the world as we know it. By 2022, the number of Internet Protocol (IP)-connected devices is anticipated to be triple that of the world's population, generating 4.8 ZB of IP traffic per year. According to Aldweesh, Derhab and Emam [1], this exponential growth raises enormous security threats because large quantities of sensitive information are exchanged through resource-constrained gadgets and over the insecure Internet using non - homogenous technologies and routing algorithms. These malicious threats are mostly from worms, viruses, rootkits, trojan horse and ransomeware. More so, "computer misapplication and nonconformity with regulations in workplaces also aid the malware intrusion into networks [2]. The consequences of malicious code propagation have been catastrophic to companies and organizations, with even more lethal evidences being reported; the dark turn in cyber-attacks, preying on educational institutions, municipal departments, and our other severely undermanned and overstretched public institutions (CrowdStrike [3]).

With the increasing prevalence of malicious code in communication networks, automatic malware identification is required to cope with the increasing level and frequency of malware attacks generated [4]. Malware detection in particular, relates features derived from an inbound file's script to a recognized list of malicious code signatures. Currently, "with the growth of internet, malicious code has advanced quickly in terms of classifications and amounts, and the transmission methods have brought up to date." Unknown malware detection is becoming a big challenge" [5]. Aside from the use of anti-malware software, epidemic approaches (through compartmental models (CM)) were used to fully comprehend the circulating processes of malwares and to reduce the frequency of cyber-attacks on ICT infrastructure [2]. Forecasts using spatio-temporal variables are indeed very plausible for both contagious diseases and malicious code outbreaks, and have remained an active topic in recent years. The trend has been extended to include agent based models (ABM) due to constraints attributed to modeling with equations. The individual level details in an agent-based model can be easily aggregated to obtain epidemic data of any resolution, e.g. number of newly infected people in a county in a specific time frame [6]. Many forecasting methods have been developed based on either CM or ABM in both biological and communication networks. With the advances in artificial intelligence (AI), there is the hypothesis that: results of ABM can be extended to include machine learning (ML) or deep learning (DL) networks in such a manner that predictions are possible. To this end, we aim to present a review of related literature surrounding these mentioned concepts.

Definition of terms

At this point, we present the definition of several keywords to guide this review. They include agent based models, malware, datasets, machine learning and deep learning.

- **Agent Based Models:** Individuals (commonly referred as agents or actors) are described as distinct and autonomous entities that interact with one other and their immediate environment in models where they are characterized as unique and autonomous entities. ABMs are made up of agents, environments, and rules, with various kinds of agents representing different sorts of people in the simulated system [6].

- **Malware:** Malicious software, commonly termed "malware", continuously presents one of the top security concerns for organizations. Typical malware includes viruses, worms, Trojan horses, spyware, adware, and others [7]. Due to their self-replicating disposition, rapid propagation speed, and potentially severe damaging effects, viruses and worms, the two most frequently encountered kinds of malware, have attracted more industry and academic interest than other malicious software.

- **Datasets:** Is an assemblage of raw facts and figures. Examples of classical datasets include; Iris flower data set, Modified National Institute of Standards and Technology database, Categorical data analysis, Robust statistics and Time series.

- **Intrusion Detection Systems (IDS):** Which may be either host-based or network-based, is primarily designed to detect dangerous assaults in real time and notify network administrators [8]. This may encourage operators to take the steps required to mitigate the harmful attack's impact. Davis further divided IDS into two kinds: misuse-based and anomaly-based; the former rely on domain experts' principles, while the latter works by "first modeling all sorts of normal or acceptable behavior." An oddity is reported when observed behavior differs from the model".

- **Machine Learning (ML):** Applies to any computer software that can "learn" without being expressly designed by a person [9]. The term (and its fundamental concept may be traced back to Alan Turing's pioneering 1950 article "Computing Machinery and Intelligence," which included a segment on his renowned "Learning Machine," which could deceive a person into thinking it was genuine. Note that both

- **Deep Learning (DL):** Deep learning is a kind of machine learning that may use supervised, unsupervised, or both methods. While not quite new, deep learning has lately gained prominence as a means of speeding up the solution of some kinds of complex computer problems, particularly in the areas of computer vision and natural language processing (NLP). Deep learning models provide faster results than conventional machine learning methods because they extract high-level, complex abstractions as data representations via a hierarchical learning process [9]. In the light of our aims, we aim to check the use of some DL networks such as the Long Short Term Memory Recurrent Neural Network (LSTM RNN) and some metrics such as Root Mean Square Error (RMSE) and Pearson's Correlation Coefficient (CORR).

Deficiencies of mathematical models

Traditional analytical models have been used to model epidemics over time [10,11], but their use has been adjudged limited. The little prediction done with these models are so limited because parametric values are small and inadequate to impact decision making in malware epidemics. On the other hand, these models also included mathematical stability analyses at the equilibrium points i.e. disease-free and endemic. The stability analyses filled with the rigors of mathematical theorem hardly contributes to prediction using ML, hence the need for the agent based model. Other shortcomings of these kind of models includes; "homogenous mixing and distribution, inability to represent individual dynamical behavior and the inability to account for local infections between nodes in a network". Put another way, "models based on differential equations fail to capture the local characteristics of spreading processes, nor do they include interaction behaviors among individuals" [11].

Pellis., *et al*. [12] identified the following challenges of network epidemic models: "understanding the effect of heterogeneity on parameter estimation and epidemic outcome, developing analytical methods to generate and study epidemics on static unweighted complex networks, developing analytical methods to model weighted and dynamic networks and epidemics theorem, incorporating waning immunity in network epidemic models, clarifying the impact of network properties on epidemic outcome, strengthening the link between network modelling and epidemiologically relevant data and designing network-based interventions".

Cunniffe., *et al*. [13] identified the following challenges of epidemic models: "linking epidemiological models to crop yield and ecosystem services, temporal changes in host availability, from plant organs to populations, effects of vector preference on transmission, capturing host spatial structure, even when data are limited, beyond a single species: multiple and alternate hosts, spillover and community ecology, realistic dispersal models, including meteorological and anthropomorphic drivers, accounting for time-varying infectivity, effects of vector preference on transmission, beyond a single species: multiple strains, multiple pathogens and evolution, using models to optimise detection, optimising dynamic controls in heterogeneous systems, accounting for economics: moving optimal control theory to realistic landscapes and use of models by policy makers and stakeholders". Roberts., *et al*. [14] identified the following challenges of epidemic models: "understanding the endemic equilibrium, defining the stability of the endemic equilibrium, modelling multi-strain systems, modelling time-varying infectivity, modelling superinfection, modelling superinfection, exploring the interaction with non-communicable diseases, defining the limitations of deterministic models, and developing robust deterministic approximations of stochastic models".

Researchers suggested the use of Individual based models (IBMs) in order to salvage the above shortcomings. IBMs attempts to highlight the real-world autonomy of interacting individuals/hosts. Studies involving IBMs simulate local interactions between cells/agents in discrete time and space so as to produce emergent outcomes. Examples of IBM are cellular automata and ABM, such as the one proposed by this study. Few of these models exist for malware propagation, perhaps due to the complexity of representing individual level mechanisms of a particular phenomenon.

Methodology for the Review

Initially, we looked for relevant literature by searching for words such as agent based models, malware, datasets, machine learning, deep learning, RNN, LSTM and intrusion detection. Then, we found publications that contained all of the abovementioned specific keywords and included them in the investigation. The papers used were published in reputable publishers. Specifically, most of these models are published in journals of Information Processing and Management, Computer Science and Information Technology, Theoretical Biology and Medical Modelling, and other reputable conferences. Aside from categorizing the review based on malware types, we intended to generate the associated pros and cons of each reviewed model. As the transition here is from ABMs to AI-based models, note that the review did not involve mathematical models for malware spread. Table 1 contains agent based models for networks while table 2 lists studies that applied machine/deep learning, intrusion detection and malware spread prediction.

	Authors	Problem	Strengths	Weaknesses
1.	Kotenko [15]	Distributed Denial of Service (DDoS) attacks	Modeled agents' team structures and action plans.	It does not include agent, ML or DL analyses.
2.	Kotenko [16]	Network cyber-attacks (DDoS, network worms, botnets)	Combined discrete-event, multi-agent approach and packet-level simulation of network protocols	It does not include agent, ML or DL analyses.
3.	Niazi and Hussain [18]	Self-organization	Modeled self-organization in peer to peer (P2P) network	It does not include agent, ML or DL analyses.

4.	Pan and Fung [17]	Malware outbreak	Modeled coordinated and non-coordinated containment plan	It does not include agent, ML or DL analyses.
5.	Bose and Shin [34]	Malware spread in networks	Modeled using an epidemic model	It does not include agent, ML or DL analyses.
6.	Wasti [19]	Issues radio channel environment, resource allocation, routing, medium access control and cognitive radio	Workload of the network operator while maintaining the QoS level	It does not include agent, ML or DL analyses.
7.	Mojahedi and Azgomi [20]	Infection time of topology-aware P2P worms	Modeled time lag and network topology for P2P worms	It does not include agent, ML or DL analyses.
8.	Hosseini, Azgomi and Torkaman [35]	Malware spread in scale-free networks	Modeled using an epidemic SEIR model	It does not include agent, ML or DL analyses.
9.	Nwokoye., *et al*. [10]	Malware spread in wireless sensor networks	Modeled the SEIR-V mathematical model	It does not include agent, ML or DL analyses.
10.	Batista [33]	Malware spread in wireless sensor networks	Modeled the SEIR-D mathematical model	It does not include agent, ML or DL analyses.
11.	Mwangi, Masupe and Mandu [36]	Malware spread in IoT	Modeled using an epidemic SIRR model	Evaluations didn't involve RMSE and CORR.

Table 1: Agent Based Models for Networks.

	Authors	Problem	Strengths	Weaknesses
1.	Shone, Ngoc, Phai, and Shi [21]	Levels of human interaction detection accuracy	Used the benchmark KDD Cup '99 and NSL-KDD datasets	It was not based on epidemic theory and is not a time series issue that allows LSTM RNN use.
2.	Chawla [22]	Security anomalies in IoT networks	Evaluated using real network traces and scalability.	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR
3.	Rhode, Burnap and Jones [4]	Static detection of malicious codes	Perform behavior analyses	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.
4.	Xiaofeng, Xiao, Fangshuoa, Shengwei, and Jing [5]	Malicious code detection	The combination architecture is 99.3%	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.
5.	Hijazi, Safadi, and Flaus [23]	Security of industrial networks	Enhanced identification of new attacks	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.
6.	Kang, Jang, Li, Jeong, and Sung [24]	Estimation by analyzing the opcodes in its executable files	Analyze opcodes and API function names	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.
7.	Fang., *et al*. [25]	Used LSTM RNN for the prediction cyber-attack rates	Better than ARIMA approaches and involved RMSE, MSE, PMAD and MAPE	It was not based on epidemic theory and datasets are not based on agent based models. CORR wasn't considered.
8.	Thamilarasu and Chawla [26]	Security anomalies in IoT networks	Evaluated using real network traces and scalability.	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.
9.	Ren, Guo, Qian, Yuan, Hao and Jingjing [27]	Detecting anomalies with fewer records	The UNSW-NB15 dataset was used	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR

10.	Boukhalfa, Abdellaoui, Hmina and Chaoui [28]	Malware intrusions	Found a two-class means of blocking intrusions	It was not based on epidemic theory. Evaluations didn't involve RMSE and CORR
11.	Almseidin, Alzubi, Kovacs and Alkasassbeh [29]	False negative and false positive performance metrics	Decision table classifier had the highest accuracy	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR
12.	Wuke, Guangluan and Xiaoxiao [30]	Failure to extract representative and abstract features	Compared with support vector machine approach	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR
13.	Kim [31]	Performance evaluation for detection rate	Combined stacked feature extraction and weighted feature selection	It was not based on epidemic theory or LSTM RNN. Evaluations didn't involve RMSE and CORR.

Table 2: Machine/Deep Learning, Intrusion Detection and Malware Spread Prediction.

From these reviews, it is evident that the reviewed papers started from 2005 for ABMs and 2017 for ML/DL models for intrusion detection and malware control (Figure 1). While the former includes 11 models, the latter involved 13 studies. Actually, several gaps were discovered and they are as follows: Although ABMs can aid the development of hypothetical epidemic cases, no study has thought of exploiting the features of the NetLogo agent-oriented language for creating epidemic datasets of communication networks, which will serve as inputs into ML/DL models. Note also that neither have evaluation metrics such as root mean squared error (RMSE), Pearson's correlation coefficient (CORR), mean absolute error (MAE) and mean absolute percentage error (MAPE) been applied to such datasets. Researchers are yet to explore the implementation of epidemic theory using this conception, i.e. the progression from analytical modeling, agent modeling, and recurrent neural network modeling for hypothetical communication epidemic cases. With the reviewed works above, it is clear that DL models are yet to be thought of in terms of susceptibility, recovery, infectiousness, and measuring the impact of virtual vaccination using anti-malware i.e. epidemic theory. Since authors have yet to direct attention to epidemic theory, it is safe to assume that there is no formalized methodology for such progression. In fact, after a thorough literature search, to the best of our knowledge, there exists no approach for merging the salient phases of malware modeling using equations and agent-based representations alongside deep learning models such as the LSTM RNN. Fang., *et al*. [25] was done with LSTM RNN but not with epidemic theory in mind. Note that in principle, RNNs may be thought of as having a memory that can store an infinite history of earlier processed items. As a result, this recorded history is utilized to forecast the process's future output at any given moment. The gradient vanishing/exploding issue may occur during the training phase of RNNs, which can be mitigated by another RNN structure known as the LSTM [25]. As Fang [25] puts it "LSTM is composed of units called memory blocks, each of which contains some memory cells with self-connections, which store (or remember) the temporal state of the network, and some special multiplicative units called gates. Each memory block contains an input gate, which controls the flow of input activations into the memory cell; an output gate, which controls the output flow of cell activations into the rest of the network; and a forget gate.

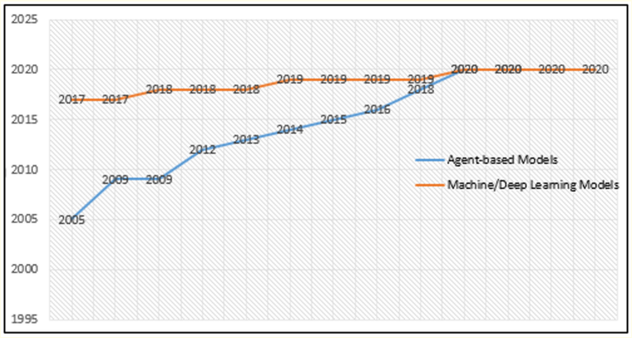

Figure 1: Relationships between corpus tables.

Potential methodologies for merging ABM to deep learning models

Since the review involves modeling and simulation approaches, we suggest that agent-based and deep learning methodologies should be employed for the prediction of malware in communication networks. Firstly, a recent methodology called the analytic-agent cyber dynamical systems analysis and design methodology (A^2CDSADM) [10], has formalized a way to achieve the characterization of agent-based models alongside an analytical model. This methodology merges the strength of the traditional Modeling and Analysis of Dynamical Systems (or Cyber Defense Systems) as well as the Agent Oriented Software Engineering approach, which applies Agent Oriented Programming (AOP). From A2CDSADM, epidemic data sets are generated which will be used as inputs to the AI model training and testing process. Analyzing this method shows that two modeling methods are featured and described, namely; Modeling and Analysis of Cyber Defense Systems (where networks are treated as dynamical systems) and the Agent-Based Modeling approach. While the former allows the development of traditional analytical (equation-based) models, the latter would enable the building of agent simulators with more capabilities. The simulators would go beyond representing some characteristics of our proposed models to characterizing spatial and visual factors. Figure 2 shows the diagrammatic representation of A2CDSADM.

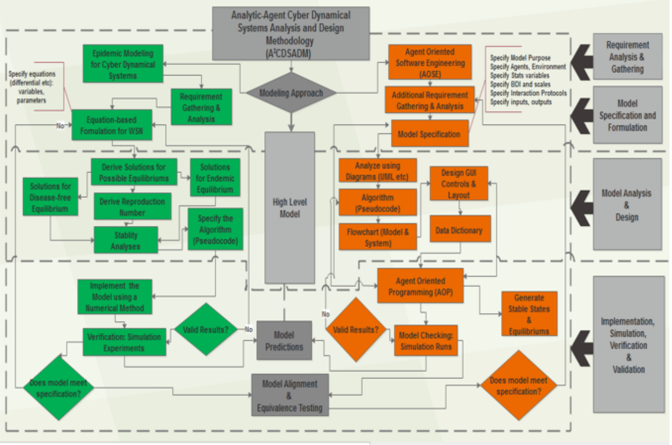
Analytic-Agent Cyber Dynamical Systems Analysis and Design Methodology (A^2CDSADM)
Epidemic Modeling for Cyber Dynamical Systems
Specify equations (differential etc): variables, parameters
Requirement Gathering & Analysis
Modeling Approach
Equation-based Fomulation for WSN
No
Derive Solutions for Possible Equilibriums
Solutions for Endemic Equilibrium
Solutions for Disease-free Equilibrium
Derive Reproduction Number
Specify the Algorithm (Pseudocode)
Stablity Analyses
High Level Model
Implement the Model using a Numerical Method
Verification: Simulation Experiments
Valid Results?
No
Model Predictions
Does model meet specification?
Model Alignment & Equivalence Testing
Agent Oriented Software Engineering (AOSE)
Additional Requirement Gathering & Analysis
Specify Model Purpose
Specify Agents, Environment
Specify Stats variables
Specify BDI and scales
Specify Interaction Protocols
Specify inputs, outputs
Model Specification
Analyze using Diagrams (UML etc)
Algorithm (Pseudocode)
Flowchart (Model & System)
Design GUI Controls & Layout
Data Dictionary
Agent Oriented Programming (AOP)
Generate Stable States & Equilibriums
No
Valid Results?
Model Checking: Simulation Runs
Does model meet specification?
Requirement Analysis & Gathering
Model Specification and Formulation
Model Analysis & Design
Implementation, Simulation, Verification & Validation

Figure 2: Diagrammatic representation of the A2CDSADM (Nwokoye and Umeh [10]).

Secondly, using LSTM RNN involves the method depicted in figure 3. This method was gleaned from the study by Bediako [32]. Therein, the data collection was by downloading the NSL-KDD dataset from the University of New Brunswick Lab, but in our case, data from agent-based models was used. The process started with data collection, data cleaning and segmentation, preprocessing, training of the data set, model training, and testing of the data set. Note that in the diagram, the method ends with classification. However, in this study, predictions would end the process.

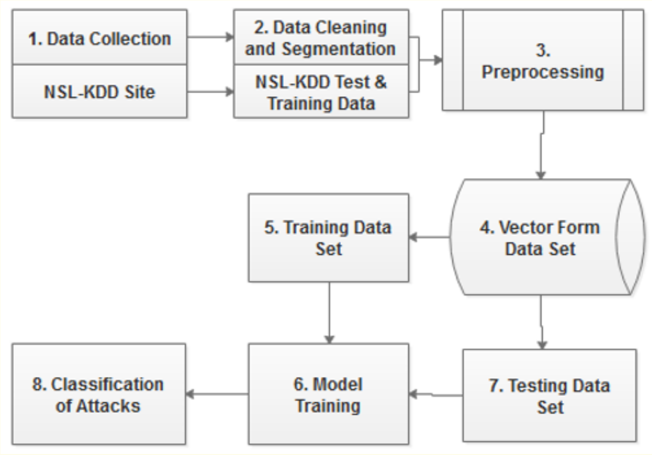

Figure 3: AI model training and Testing Process (Bediako, 2017).

Conclusion and Future Directions

The permeation of connectivity owing to the Internet and social media into private life, work, and recreation. The growing number of mobile phones and various IT implementations have made inserting malicious software into servers or endpoints in a network a huge possibility in institutions that use the World Wide Web to accomplish tasks. Machine learning (ML) and deep learning (DL) models are also being applied to a range of programs used in big data analytics and data mining. A computer model for modeling the behaviors and interactions of autonomous agents, on the other hand, is known as an agent-based model (ABM). We did notice, however, that neither ABM nor ML/DL have been used for epidemics in communication networks. As a result, we examined the literature on the aforementioned topics in the article. Specifically, after the definition of these terms, we presented a tabular review of several studies, highlighting their aims, strengths and weaknesses. Finally, we proposed the merger of two prominent methodologies, i.e. the A2CDSADM and the AI Model Training and Testing Process. We expect that this will provide the necessary context for building ABM to DL network transitional techniques. In the future, we will explore the actual implementation of an ABM for a computer network and the transition to the use of LSTM RNN for prediction.

Bibliography

1. Aldweesh A., *et al*. "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues". *Knowledge-Based Systems* 189 (2020).

2. Nwokoye C H., *et al*. "Evaluating degrees of differential infections on sensor networks' features using the SEjIjR-V epidemic model". *Egyptian Computer Science Journal* 44.3 (2020).

3. Crowdstrike Global Threat Report (2020).

4. Rhode M., *et al*. "Early-stage malware prediction using recurrent neural networks". *Computer and Security* 77 (2018): 578-594.

5. Xiaofeng L., *et al*. "ASSCA: API-based Sequence and Statistics features combined malware detection Architecture". *Procedia Computer Science* 129 (2018): 248-256.

6. Batista F K., *et al*. "A new individual-based model to simulate malware propagation in wireless sensor networks". *Mathematics* 8 (2020): 1-23.

7. Hong Guo., *et al*. "Impact of Network Structure on Malware Propagation: A Growth Curve Perspective". *Journal of Management Information Systems* 33.1 (2016): 296-325.

8. Davis J J and Clark A J. "Data preprocessing for anomaly based network intrusion detection: A review". *Computers and Security* 30.6 (2011): 353-375.

9. Wehle HD. "Machine Learning, Deep Learning and AI: What's the Difference?" (2017).

10. Nwokoye C and Umeh I. "Analytic-agent cyber dynamical systems analysis and design method for modeling spatio-temporal factors of malware propagation in wireless sensor networks". *MethodsX* 5 (2018): 1373-1398.

11. Peng S., *et al*. "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones". *Journal of Computer and System Sciences* 79 (2013): 586-595.

12. Pellis L., *et al*. "Eight challenges for network epidemic models". *Epidemics* 10 (2015): 58-62.

13. Cunniffea NJ., *et al*. "Thirteen challenges in modelling plant diseases". *Epidemics* 10 (2015): 6-10.

14. Roberts M Andreasen., *et al*. "Nine challenges for deterministic epidemic models". *Epidemics* 10 (2015): 49-53.

15. Kotenko I. "Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in internet". Paper presented at the 19th European Conference on Modelling and Simulation, Riga, Latvia, Germany (2015).

16. Kotenko I. "Agent-based modeling and simulation of network infrastructure cyber-attacks and cooperative defense mechanisms". *Discrete Event Simulations* 3.56 (2019): 34-67.

17. Pan J and Fung CC. "An agent-based model to simulate coordinated response to malware outbreak within an organization". *International Journal of Information and Computer Security* 5.2 (2012): 115-131.

18. Niazi M and Hussain A. "Agent-based tools for modeling and simulation of self-organization in peer-to-peer, ad hoc, and other complex networks". *IEEE Communications Magazine* 47.3 (2009): 166-173.

19. Wasti BK. "Usability of multi-agent simulators in simulation of wireless networks". (Master's thesis. The University of Oulu, US) (2014).

20. Mojahedi E and Azgomi MA. "Modeling the propagation of topology-aware P2P worms considering temporal parameters". *Peer-to-Peer Networking and Applications* 8.1 (2015): 171-180.

21. Shone N., *et al*. "A Deep Learning Approach to Network Intrusion Detection". *IEEE Transactions on Emerging Topics in Computational Intelligence* (2017): 1-10.

22. Chawla S. "Deep Learning based Intrusion Detection System for Internet of Things". Master Thesis, University of Washington (2017).

23. Hijazi A., *et al*. "A Deep Learning Approach for Intrusion Detection System in Industry Network" (2018).

24. Kang J., *et al*. "Long short-term memory-based Malware classification method for information security". *Computers and Electrical Engineering* 77 (2019): 366-375.

25. Fang X., *et al*. "A deep learning framework for predicting cyberattacks rates". *EURASIP Journal on Information Security* 5.1 (2019): 1-11.

26. Thamilarasu G and Chawla S. "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things". *Sensors* 19.1 (2019): 1-19.

27. Ren J., *et al*. Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms. Security and Communication Network, 7130868 (2019): 1 – 11. https://doi.org/10.1155/2019/7130868.

28. Boukhalfa A., *et al*. "LSTM deep learning method for network intrusion detection system". *International Journal of Electrical and Computer Engineering* 10.3 (2020): 3315-3322.

29. Almseidin M., *et al*. "Evaluation of Machine Learning Algorithms for Intrusion Detection System" (2020).

30. Wuke L., *et al*. "Application of Deep Extreme Learning Machine in Network Intrusion Detection Systems". *IAENG International Journal of Computer Science* 47.2 (2020): 136-143.

31. Kim K. "Intrusion Detection System Using Deep Learning and Its Application to Wi-Fi Network". *IEICE Transactions on Information and Systems* 103.7 (2020): 1433-1447.

32. Bediako P K. "Long Short-Term Memory Recurrent Neural Network for detecting DDoS flooding attacks within TensorFlow Implementation framework". Master's Thesis submitted to Lulea University of Technology (2017).

33. Batista F K., *et al*. "A new individual-based model to simulate malware propagation in wireless sensor networks". *Mathematics* 8 (2020): 1-23.

34. Bose A and Shin K. "Agent-based modeling of malware dynamics in heterogeneous environments". *Security and Communication Networks* 6 (2013): 1576-1589.

35. Hosseini S., *et al*. "Agent-based simulation of the dynamics of malware propagation in scale-free networks". *Simulation* 92.7 (2016): 709-722.

36. Mwangi K E., *et al*. "Modelling malware propagation on the internet of things using an agent based approach on complex networks". *Jordanian Journal of Computers and Information Technology (JJCIT)* 6.1 (2020).

Volume 3 Issue 10 october 2021