Game Theory Approach to Intrusion Detection System

Ajayi Ebenezer Akinyemi, Alese Boniface Kayode & Iwasokun Gabriel Babatunde
Faculty of Computing and Informatics,
Multimedia University,
Cyberjaya Campus, Persiaran Mutimedia, 63100 Cyberjaya, Malaysia.
E-mail: ebeconsult@myself.com

Ayodele Oluwakemi Sade & Ajayi Banke Funmilayo
Computer Science Department
Kogi State Polytechnic
Lokoja, Nigeria
E-mail: kemtemmy2009@gmail.com & ebeseun@gmail.com

Musa Ugbede & Ilugbusi Abiodun Adebowale
Computer Science Department
Federal Polytechnic
Idah, Nigeria
E-mail: musa.ugbedeojo@yahoo.com & ilugbusi.abiodun@fedpodak.edu.ng

ABSTRACT

This ongoing research work presents a new approach to Intrusion Detection System called Game theory approach to Intrusion Detection System. The new concepts of ubiquitous computing and high capacity data transfer have turned the internet into today's commerce. An intrusion detection system (IDS) comprises of hardware and software elements that work together to find unexpected events that may indicate an attack will happen, is happening, or has happened. This research work is trying to look at developing an intrusion detection system using Instance Based Learning Model in conjunction with Attack Graph Techniques and evaluation of the model based on results obtained from case study of intrusion detection in some selected networks. It is expected that the result will determine attackers' behavioral pattern on a network and also provide an enhanced intrusion detection model that prevents attackers' actions to be carried out on a network.

Keywords: Information Security, Instance Based Learning Model, Intrusion Detection System, Attack Graph

ISTEAMS Cross-Border Conference Proceedings Paper Citation Format
Ajayi, E.A., Alese, B.K., Iwasokun, G.B., Ayodele, O.S., Ajayi, B.K., Musa, U & Ilugbusi, A.A. (2017): Game Theory Approach to Intrusion Detection System. Proceedings of the 9th iSTEAMS Multidisciplinary Conference, University of Ghana, Legon, Accra Ghana. Pp 185- 192

1. BACKGROUND TO THE STUDY

The new concepts of ubiquitous computing and high capacity data transfer have turned the Internet into today's main area for information interchange and electronic commerce. As network systems become more and more complex and interconnected, their security plays an increasingly important role mainly because they are supporting critical applications. Attacks against computer networks used by modern society and economics for communication and finance can therefore threaten the economical and physical well-being of people and organizations. The security of an Information Communication Technology (ICT) system and its components is hence a research area of ever increasing interest. To this effect, Information security has become one of the major concerns since critical decisions are made based on information stored and analysed by software systems. As a result of this, the need for effective techniques to protect software systems from malicious attacks has increased the level of significance of the software security field to meet industry needs.

Attacks can range from viruses/worms, Internet browser exploits through the identity theft to more severe threats such as cyber-attacks and cyber-terrorism. Wired and wireless infrastructure-based networks are designed to secure networks by using firewalls and encryption techniques but they still suffer from different types of intrusions.

As there is increasing reliance on computer and network systems to support critical operations in defense, banking, telecommunication, transportation, school, insurance, electric power etc., computer system and network insecurity become important threat to our society with severe potential consequences. Cyber–attack and cyber insecurity are launched through a series of computer actions to compromise the security (such as service availability, integrity, and confidentiality) of computer and network systems.

Network Attack can be defined as any attempt to destroy, disable, steal or gain unauthorized access to a network asset**.**
Some of Classes of Network Attacks on Computer Network System

i. Side Channel Attacks: The attacks are based on information that is gained from the physical implementation of a cryptosystem rather than brute force or theoretical weakness in the algorithms. Timing analysis, acoustic analysis and power consumption analysis are some instances that belong to this class.

ii. Cryptographic/ Protocol Attack: This is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme.

iii. Implementation Attack: This attack refers to a type of cryptanalysis attack that does not target cryptographic algorithms and protocols directly. This attack aims at implementation of cryptographic systems (the smartcards and USB tokens) to gain knowledge about secret information. These attacks refer only to certain implementations of the SSH- Server or the SSH-Client. Since the number of SSH implementation is usually high, the attacks appear very frequently.

iv. Denial of service attacks: Denial of service (DoS) attacks against Network system providers may leave tenants without access to their accounts. This can occur by sending a flood of traffic to overwhelm websites to make them inaccessible to legitimate users. When a DoS attack is conducted using a botnet (a network of compromised machines), this is referred to as a distributed denial of service attack, or DDoS. DoS attacks aimed at individual accounts may be accomplished by changing the tenant's password or maliciously continuing to enter the incorrect password so that the account becomes locked.

v. Man-in-the-middle attacks: Here, the attacker intercepts traffic between a website and a Browser [19]. This occurs when the browser believes that the attacker is the legitimate website and the website authenticates the attacker as the browser. The attacker can then read and alter the data being transmitted, including account passwords that may be used to login to a network system.

vi. Network/Packet sniffing: Network or packet sniffing involves the interception and monitoring of network traffic [10]. Data that are being transmitted across a network, such as passwords, can therefore be captured and read if not adequately encrypted.

1.1 Intrusion Detection System (IDS)

An intrusion detection system (IDS) comprises of hardware and software elements that work together to find unexpected events that may indicate an attack will happen, is happening, or has happened [2]. An intrusion detection system (IDS) examines system or network activity to find possible intrusions or attacks. Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffics and thereafter analyzes such traffic for possible attacks originating from outside or within the organization. Intrusion detection systems can

be categorized into network-based intrusion detection system (NIDS), host-based intrusion detection system (HIDS) and stack-based intrusion detection system (SIDS).

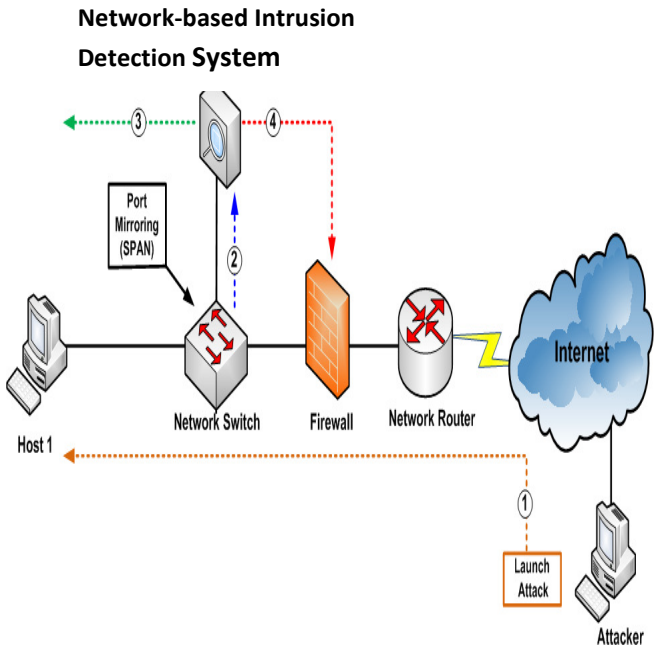

Fig. 1.: Network-Based Intrusion Detection System (ieee 2014 java project)

1.2 Game Theory

Game theory is a branch of applied mathematics that uses models to study interactions with formalized incentive structures (“games"). Game theory usually considers a multiplayer decision problem where multiple players; the attackers (malicious users) and the defenders (network/system administrator) [4, 20] with different objectives can compete and interact with each other. Game theory describes the decision scenarios of two or more players as games in which each player chooses actions to bring the best possible payoffs for the player while anticipating the rational actions from other players [11].

1.3 Stochastic Modeling

This is a model that involves probabilities associated with time. System behaviour in stochastic model is represented by a stochastic process such that:

i. an event that will occur next is random.
ii. the time until the next event is random.

In Stochastic Model, systems behaviour is modelled as ”states” and “transitions” between states. This modelling approach captures dynamic system behavior (sequences of events) and can be used as a basis for quantitative analysis. Therefore a ***stochastic model*** is a tool for estimating probability distributions of potential outcomes by allowing for random variation in one or more inputs over time. The random variation is usually based on fluctuations observed in historical data for a selected period using standard time-series techniques.

1.4 Attack Graph Techniques

An attack graph is a succinct representation of all paths through a system that end in a state where an intruder has successfully achieved his goal. Attack-graph techniques can automatically discover all possible ways an attacker can compromise an enterprise network by analysing configuration information of the hosts and network [6]

1.5 Statement of Problem

Information security has become one of the major concerns since critical decisions are made based on information stored and analysed by software systems. Attacks against computer networks used by modern society and economics for communication and finance can therefore threaten the economical and physical well-being of people and organizations. Wired and wireless infrastructure-based networks are designed to secure networks by using firewalls and encryption techniques but they still suffer from different types of intrusions. In view of the above problems, our work will looks at Game Based Approach with Attach Graph Technique to resolve the problem of intrusion by hackers in a network environment.

1.6 Objective

The object of the work is as follows:

i. develop a game based model for network intrusion detection.
ii. implement the model formulated in (i) above.
iii. evaluation of the model based on results obtained from case study of intrusion detection in some selected networks.

2. REVIEW OF RELATED WORK

Due to the importance of Intrusion Detection System in security system, so many researches have been carried out on it in different direction. In [10], Network Packet Sampling strategy to reduce the success chances of an intruder was proposed. The difference in the form of intrusions experienced by wired-based networks using fire-wall and encryption techniques is the key motivation for this work. In their work, they develop a network packet sampling strategy for reducing the success chances of an intruder in a wired infrastructure based networks. Their work is limited to Network Packet Sampling strategy which led to the problem of missing some intrusions due to its sampling budget constraints.

In [17], a self-adaption mechanism for network intrusion detection system which uses a game-theoretical mechanism to increase system robustness against targeted attacks on Intrusion Detection System was developed. When adaption techniques were deployed improperly, it can allow the attackers to reduce the system performance against one or more critical attacks which can lead to a potential attacked for an informed and sophisticated attackers. The research work is on the design of a self-adaptation mechanism for network intrusion detection system. The method adopted in the work was the concept of challenge insertion and used for the design which help in inject a small sample of simulated attacks into the unknown traffic and use the system response to these attacks to define the game structure and utility functions. The work is only based on a distributed agent-based Intrusion Detection System without looking into other form of Intrusion Detection System. In [2], the basis trade-offs, analysis and decision process involved in information security and intrusion detection as well as possible application of game theoretic concepts to develop a formal decision and control framework was documented. Current IDS's rely mostly on human intervention in decision and response processes against attackers, that are often automatic and script based.

Today's IDS are inefficient and delayed in responding to security breaches in the network. Due to the distributed nature of the networked system, a centralized security system poses scalability and efficiency problems. The researchers developed a security warning system with network sensors. GAMBIT game theory analysis tool was adopted and used in investigating the basic decision and analysis processes involved in the research work. The work did not develop a practical algorithms to be used and decentralization of the decision and processes were not developed and implemented.

In [21], an ad-hoc intrusion detection model based on the game theory was presented . Since mobile Ad-hoc network are kind of temporary autonomous network system which comprised of a number of wireless mobile node without control center through which the nodes of mutual cooperation network interconnection is possible, intrusion of such network is at high risk. The research work entails the designs of the response scene between the attacker and defender in the Ad-hoc network and Compare node survival and success rate of defense in two scene networks. GloMoSim platform was used to test the model developed. The experimental scene is limited to 500m*500m and experimental time is 60s which has greater effects on the security management of the network.

In [3], Game theory and intrusion detection system was documented. Intrusion detection system has long been utilized in detection and response strategy to potential attacks. However, effective policing and finding a right balance between tradeoffs has always been an issue. The work analyzed the available game theoretic approaches for intrusion detection systems. Adaptive snort were adopted and used for the analysis of the available game theoretic approaches. The work only stopped at the review stage. No specific implementation was proposed.

In [1], documentation on Intrusion detection in sensor networks and non-cooperative game approach is presented. The need to unravel the factors responsible for the insufficiency of memory and battery power of sensors which makes the security of networks very tasking. This also contributes to the unstable form of networks on the sensor. The researchers developed a game theoretic framework for defending nodes in a sensor network by formulating an attack-defence problem as a two-player, nonzero-sum, non-cooperative game between an attacker and a sensor network. Markov decision process to predict the most vulnerable sensor node, intuitive metric (node's traffic) and protect the node with the highest value of this metric was used in the framework. The most vulnerable node in a sensor network is their main concerned leaving the less vulnerable nodes unprotected thus, create another set of risk in sensor network.

[12], A game-theoretic scenario for modelling the Attacker Defender Interaction was presented. Exiting Computer Security techniques lack decision frame work required to defend against highly organized attacks. Many mathematical models such as Machine Learning, Control Theory, Data Mining etc. have been used to model and analyse the decision making problems but they all the models fail to capture the rationality and dynamic nature of players involved in security provisioning large scale network. The researchers developed a stochastic game-model that view the interaction between malicious users and network administrators a two-player zero sum game. A binary coding scheme was employed for identifying game states and game transition diagrams were generated to describe possible movements of player. A stochastic algorithm was developed to solve the game and compute the optimal strategies for the players. Their emphasis was not on how the attackers operate and their pattern on the network. Also risk computation was not done which supposed to help in analysis of the attacks and predicting attacker's behaviours on network.

3. METHODOLOGY

A detailed review of existing literature in the area of game theoretic based intrusion detection system was carried out. The review highlighted the fundamental concept of game theoretic based intrusion detection system, their strength and limitation. A typical game scenario is played over a computer network environment made up of several interconnected components (asset) and game actors. Network assets consist of firewalls, databases, file/print, application servers, routers and cryptographic devices. The game actors are network/virtual users, normal users attempting to accomplish a task, attackers who exploit vulnerabilities and defenders whose responsibility is to secure the network from malicious threats to both internal and external factor. The game model for the ongoing research work is model by considering a multiple-player zero-sum game played on a finite state space, where each player has a finite set of actions to choose from. The multiple-player stochastic game is defined as a tuple in the equation below:

$$G = (S, M, (A_i, \propto_i, U_i)_{1 \le i \le |p|}, Q) \ldots \quad (1.1)$$

where

S is a State $S = \{s_1, s_2, s_3, \ldots s_t\}_{1 \le t \le |s|}$

M is a Player $M = \{M_k\}_{k=1,2,3,\ldots n}$

A_i is an Action $\forall (p_k \in M) \exists A_i = \{a_1, a_2, \ldots a_n\}$

$\propto_i$ is a State Action $\propto_i : S \to A, i = 1,2,3 +$

$S\alpha$ is a player profile

$$S\alpha = \{(s, a) : s \in S, a = (a_i), a_i \in \alpha_i(s); 1 \le i \le |M|\}$$

U_i is a Payoff $U_i : S\alpha \to R, i = 1,2,3 \ldots$

Q is the Probability Distribution $Q : SA \to M(S)$

The research work presents the player of the game as the defender M_1 and the attacker M_2 and the action spaces of the players are the sets of possible attack moves and defense counter measures respectively. The work encapsulates each attack or defence as a single action achieving a specific goal. The finite action spaces for both the defender (M_1) and attacker (M_2) are defined as follows in equation below:

$$A_1 = M_1^a = \{a_1, a_{2n}, \ldots a_n\} \ldots \quad (1.2)$$

$$A_2 = M_2^a = \{a_1, a_{2n}, \ldots a_n\} \ldots \quad (1.3)$$

At every state of the game, players have at their disposal a finite set of actions from the nature of the configuration of the network if the actions are unique across states.

3.1 Attacker's Behaviors Computation on Network

Identifying the game element

From the stochastic model, we will pick all states where the system is vulnerable to attacks. Each of the state can be viewed as game element in multiple-player, Zero-Sum stochastic game.

Construct the action set

This consists of all possible attacks action. For all transitions out of the game elements which represent intrusions, there will be corresponding attacker's action.

$$A_i = \{a_1, a_2, a_3 \ldots\ldots\ldots\ldots a_n, \emptyset\} \ldots \quad (1.4)$$

where Ø is inaction

Assign Reward and Cost

In the game element, we assign two values to each attack action r_i= a|undetected and r_i= a|detected.

a) Compute transition probabilities between game states.
b) Solve the game model using matrices.

The ongoing research work will make use of **Instance Based Learning Model (IBL) and attach graph techniques** to identify attackers on the network and prevent the attacker(s) from carrying-out its intended action. **Instance-based learning or memory-based learning** is a family of learning algorithms that, instead of performing explicit generalization, compare new problem instances with instances seen in training, which have been stored in memory.

3.2 Tools for System Implementation

The following are the tools to be used in implementing the work: Java Script, Java Programming Language, Js/Flash, MathLab package, Linux Operating System, Nmap, hping and wget for network probing. A detailed analysis of the results comparing the various models from case study of intrusion detection in some selected networks will be carried out.

4. CONTRIBUTION OF THE RESEARCH TO KNOWLEDGE

The research is expected to:

i. Determine attackers' behavioural pattern on a network.
ii. Provide an enhanced stochastic security game based intrusion detection model that prevents attackers' actions to be carried out on a network.

REFERENCES

1. Agah, A., Das, K. and Basu, K. (2004, April). "A Game theory based approach for security in wireless sensor Networks". International Performance Computing and Communications Conference (IPCCC).
2. Alpcan, T., and Basar, T. (2003, December)," A game theoretic approach to decision and analysis in network intrusion detection", In Decision and Control, 2003 Proceedings 42nd IEEE Conference on (Vol. 3, pp. 2595-2600). IEEE.
3. Anis A., Asad N., and Murad , B. (2006). "Game Theory and Intrusion Detection Systems" ISA 767- Secure E-Commerce Spring.
4. Balepin, I., Maltsev, S., Rowe, J. and Levitt, K.(2003, September). "Using specification-based intrusion detection for automated response". In International Workshop on Recent Advances in Intrusion Detection", Springer Berlin Heidelberg, (pp.136-154).
5. Bishop, M. (2003). "Computer Security: Art and Science", Addison Wesley Professional, USA.
6. Burguera, I., Zurutuza, U. and Nadjm-Tehrani, S. (2011,October). "Crowdroid: behavior-based malware Detection system for android". In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 15-26). ACM.
7. Garfinkel, S., Gene S. and Alan S., (2003). "Practical UNIX and Internet security", "O'Reilly Media, Inc."
8. Hamou-Lhadj, A. (2009), "A Governance Framework for Building Secure IT Systems", International Journal of Security and Its Applications, 3(2), 15-20.
9. Grobauer, B., Walloschek, T., and Stöcker, E. (2011)." Understanding cloud computing vulnerabilities", Security and privacy, IEEE, 9(2), 50-57.
10. Hadi, O.,Mona M., Chadi A., Mourad D., and Prabir B. (2008). "Game theoretic Models for detecting Network intrusions". Computer Security Laboratory, Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Que., Canada H3G 1M8 Received 28 February 2007; received in revised form 22 December 2007; accepted 23December 2007 Available online 3 January 2008.
11. He, J., Ma, S., and Zhao, B. (2013)," Analysis of Trust-based Access Control Using Game Theory", International Journal of Multimedia & Ubiquitous Engineering, 8(4).
12. *Ibidunmoye, E.O., Alese, B.K., and Ogundele, O.S. (2013)," A Game theoretic Scenario for Modelling the Attacker- Defender Interaction",* Journal of Computer Engineering & Information Technology.
13. Intrusion detection system buyer's guide: http://www.icsa.net/html/communities/ids/buyers_guide/index.shtml
14. Lakshman, T. and Kodialam, M.(2003). "Detecting network intrusions via sampling: a game theoretic approach".IEEE INFOCOM, San Francisco, California, USA.
15. Liao, H.J., Lin, C.H.R., Lin, Y.C. and Tung, K.Y., (2013). Intrusion Detection System: A comprehensive review. Journal of Network and Computer Applications, 36(1), pp.16-24.
16. Karin S. (2007). "Stochastic Models for Combined Security and Dependability Evaluation. PhD Thesis", Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology.

17. Martins, R, M. Pechoucek, M. and Grill, M. (2011). “Game Theoretical Adaptation Model for Intrusion Detection System”. Proceeding of 10th Int. Conf. on Autonomous Agents and Multiagent Systems– Innovative Applications Track, Tumer, Yolum, Sonenberg and Stone (eds.), May, 2–6, 2011, Taipei, Taiwan, pp.1123-1124.
18. Otrok, H., Mehrandish, M., Assi, C., Debbabi, M., and Bhattacharya, P. (2008). ”Game theoretic models for detecting network intrusions”, *Computer Communications*, *31*(10), 1934-1944.
19. Sallhammar, K., Knapskog, S., and Helvik, B. E. (2005, January), “Using Stochastic Game Theory to Compute the Expected Behavior of Attackers”, In *SAINT Workshops* (pp. 102-105).
20. Subashini, S,. and Kavitha, V. (2011). ”A survey on security issues in service delivery models of cloud computing”, Journal of network and computer applications, *34*(1), 1-11.
21. Xiao, H., and Long C.(2013). “Model of Intrusion Detection Based on the Game Theory” Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering.