*Nigerian Journal of Technology (NIJOTECH)*
*Vol. 36, No. 4, October 2017, pp.* **1271 – 1285**

Print ISSN: 0331-8443, Electronic ISSN: 2467-8821
www.nijotech.com
http://dx.doi.org/10.4314/njt.v36i4.38

# A REVIEW OF GAME THEORY APPROACH TO CYBER SECURITY RISK MANAGEMENT

**D. A. Akinwumi[1], G. B. Iwasokun[2,*], B. K. Alese[3] and S. A. Oluwadare[4]**
[1,] ICTA CENTRE, ADEKUNLE AJASIN UNIVERSITY, AKUNGBA-AKOKO, ONDO STATE, NIGERIA
[2,3,4] DEPARTMENT OF COMPUTER SCIENCE, FEDERAL UNIVERSITY OF TECHNOLOGY, AKURE, ONDO STATE, NIGERIA
***E-mail addresses:*** [1] *david.akinwumi@aaua.edu.ng,* [2] *gbiwasokun@futa.edu.ng,* [3] *bkalese@futa.edu.ng,* [4] *aoluwadare@futa.edu.ng*

**ABSTRACT**
***Cyber security is among the most complex and rapidly evolving issues and has been the focus of present day organizations. Cyber security risk management is the process of managing or reducing potentially harmful and uncertain events that posse as threats to cyber security. It involves looking at what could go wrong on the cyber space and deciding on ways to prevent or minimize their occurrences or effects. One of the prominent cyber security risk management techniques is the Game Theoretic Approach (GTA), which focuses on the use of resources, internal controls, information sharing, technical improvements, behavioral or organizational scale-ups and cyber insurance for cyber risk management. This paper presents a review of game theoretic-based model for cyber security risk management. Specifically, issues on modeling, some related works and significance of game theoretic approach to cyber security risk management are presented. Findings from the review revealed the peculiarities and specificity of each model. It is also revealed that the models are just evolving and require much improvement.***

***Keywords:*** *Cyber Security, Risk Management, Game Theory,* Model

## 1. INTRODUCTION

Risk is present in all spheres of human endeavors and demands efficient management strategies for profit maximization, loss minimization, safety of lives and properties among others. If the risk is associated with cyber activities, it is referred to as cyber risk. Cyber risk is among the most complex and rapidly evolving issues with which present day organizations must contend with [1-2]. In recent years, there are frequent reports of major breaches of proprietary information and damage to organizational Information Technology (IT) infrastructure. It is equally being noted that developments in mobile technology, cloud computing and social media has continued to impact the IT risk landscape and all other critical infrastructures [3]. However, traditional cyber security techniques involve a never-ending cycle of detection and response to new vulnerabilities and threats. This patches-on-patches approach is a short term fix and attests to the failure of many of the present cyber security paradigm as well as points to the need for a new and better approach [4-5]. Presently, there is a proportionate increase in the number of users of cyber space and the number of cyber criminals. This explains why increasing organizations' reliant on information systems and the Internet has resulted in increased cyber risks with potentials for severe disruption to an organization's business functions. There are also threats to operational supply chain, negative impact on reputation and compromise of sensitive customer data and intellectual property [6-9]. The threats confronting information system include complexities as well as technological changes. The threats are dynamic, hence the need for continuous monitoring and management of the information security plan [10]. Threats could be countered through adoption of robust cyber risk management techniques that identify possible risks, reduce or allocate risks as well as provide a rational basis for better decision making in regards to all risks and adequate planning. Cyber security risk management also increases the likelihood of an organization achieving its objectives by taking advantage of opportunities that may arise [11-12]. Consistent risk management ensures cost-effective risk

*** Corresponding author tel: +234 – 813 – 062 – 2747**

management with high priority risks aggressively managed all in a bid to provide information required for making better and informed decisions [13]. Managing cyber security risk may not result in the elimination of all risks but is effective for determining and understanding risk rating of events and putting the right processes or controls in place to guarantee that the organization operates at risk tolerance levels. It is a continuous process and not a one-time event [14-15]. The crimes associated to cyber activities include identify theft, hacking, virus distribution, computer fraud and any other related incidence. Cyber-criminals may be categorized into political and non-politically motivated. Politically motivated cyber crimes are perpetuated by extremist groups as a way of using cyberspace to foster falsehood, online attack, monetary gain or plan and coordinate physical-act of terrorism [16]. Non-politically motivated attacks are mostly for financial gain and other deeply-rooted socio-cultural issues [16-17]. The broad classification of cyber crimes as acts from within and outside an organization is presented in Figure 1 [18].

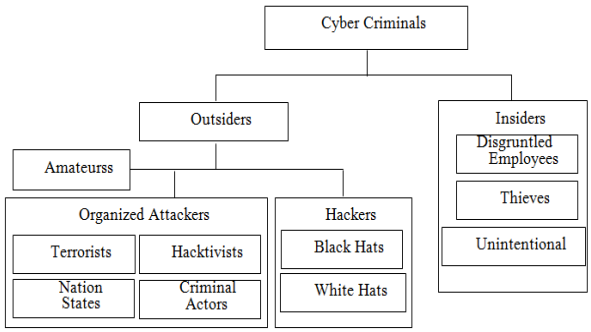


*Figure 1: Categories of Cyber criminals*

Cybercrime is a complex area of crime that requires utmost attention due to prevalence of computer as a tool in different areas of human endeavors. Similar to other forms of crime, causes of cybercrime are difficult to establish, however, it is generally attributed to some factors which include high financial gain, personal emotion and vendetta as well as ethical, ideological, moral and environmental issues [19]. Various models for management of cybercrime risks include Bayesian Network [20-25], Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) [26], Central Computer and Telecommunications Agency Risk Analysis and Management (CRAMM) [27] and GTA just to mention a few. Game theory provides a mathematical framework for modeling conflict and cooperation between two or more individuals. It is presumed that individuals are rational in their behaviors. This implies they are triggered by self-motivated goal of optimizing their respective benefit, usually expressed in terms of a utility function. The game adheres to some rules and players can choose and implement a strategy from a set of different behavioral options, in order to optimize the likely payoff as an outcome of the game. Formally a game is described by n players with strategy spaces and their payoff functions, $S_i$ and $U_i$, respectively and for each player i($1 \leq i \leq n$):

$$\boldsymbol{G} = \{\boldsymbol{n}; \boldsymbol{S_1}, \boldsymbol{S_2}, \dots, \boldsymbol{S_n}; \ \boldsymbol{U_1}, \boldsymbol{U_2}, \dots, \boldsymbol{U_n}\} \qquad (\mathbf{1})$$

Based on this description, game-theoretic analysis focuses on revealing the likely behaviour of the players, regarding their choice of strategy, thereby determining the presumable outcome for the game. It has been noted that GTA-based models exhibit performance and cost advantages over other models for the management of risks associated to cybercrimes [27]. Sections 2 and 3 of the paper present some GTA-based cyber security risk management models and the review of some research works on cyber security risk management respectively. The strengths and weaknesses of game theory approach to cyber security risk management and the conclusion drawn are also presented in Sections 4 and 5 respectively.

## 2. GTA RISK MANAGEMENT MODELS

The summaries of the various GTA-based cyber security risk management models are presented below [28-33]:

### 2.1 Chain-of-Events Model (CEM)

CEM is conceptualized in Figure 2 and it is concerned with managing the risks that may emanate from any future cyber-attack based on counter-measure strategies driven by the elimination of events and/or intervention between events in a chain, so that the chain is broken.

CEM chronologically arranges causal factors into chains which may account for recorded losses in some events. For instance, identity theft is a global event and its *Event Chain 1* may be taken as a chain of acts of stealing a purse or wallet and other dishonest acts of obtaining vital identity information. From stolen purse or wallet, personal information such as name, driver's license number, social security or credit card number may be acquired by criminals. Similarly, dishonest pair of eyes may spot credit card or social security number on a straying piece of paper or improperly guided computer screen. *Event Chain* 2 is a chain of events carried out by criminals to purnish their victims after obtaining their identity information by falsehood. Such events may include impersonation and unauthorized access to credit card accounts. In-between the two

chains are arrays of strategies or tactics the criminals would adopt or deploy to achieve their aims. The chain-of-event strategy for managing risks associated with identity theft will therefore require breaking (guiding against) events that can lead to misplacement or loss of wallet or purse as well shielding of papers and computer screen detailing identity information from intruders or impostors. Event chain may also include proximate, root or contributory environmental aspects and risk behaviours. Circumstances responsible for such behaviors are used in the event chains [34-35]. The strategies for dealing with risks management using event chain model principle include risk acceptance (excited state of the activity is considered to be acceptable) and risk transfer (the impact of the original event is its execution in another activity as shown in Figure 3). Others are risk mitigation (which represents an event chain in which the original event transforms an activity to a ground or a lower excited state (Figure 4) and risk avoidance (in which the original event plan is built in such a way that none of the states of the activities is subscribed to this event).

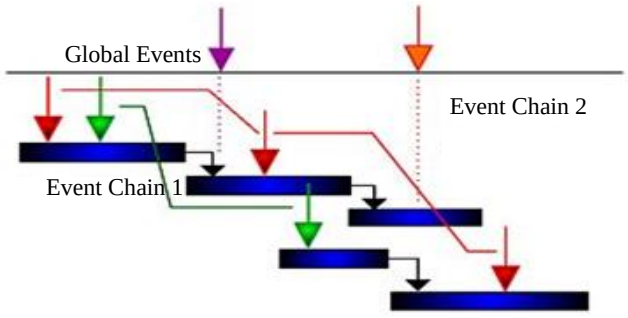


*Figure 2: Event chain model*

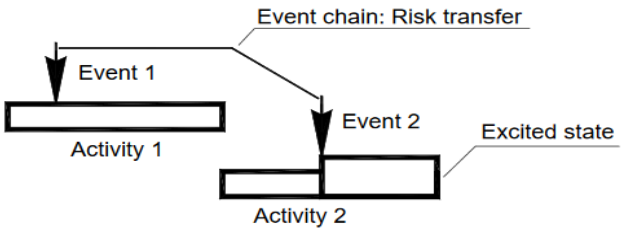


*Figure 3: Event chain risk transfer*

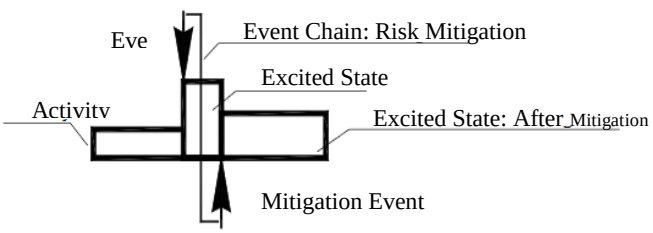


*Figure 4: Event chain risk mitigation*

Excitation indicates that the existing order of activity has changed. For instance, a new order may be require if it takes a lengthy time for an activity to enter into completion, or must be performed under different conditions, as a result, this may alter the activity's cost and duration. The original or planned state of the activity is called a ground state while other states that are associated with different events are the excited states [36]. CEM enjoys simplicity of learning and is reasonably easy to create in comparison with some other existing models. Furthermore, casual factors can be identified quickly based on event chain and environmental factors or conditions, thereby promoting the implementation of counter measures in a timely manner. The design of CEM gives consideration for risky behaviour and the contributing factors to failure events. The limitations of this model include incompleteness and ineffectiveness in the explanation and investigation of causal factors in the context of cyber security, lack of support for the determination of the terminal point when traversing from an accident event, problem solving and investigation are limited to technical events and conditions and failure to account for non-linear causalities. Other limitations are low possibility of addressing all known vulnerabilities, poor foresight about undiscovered vulnerabilities and failure to account for systemic factors including management deficiencies and/or structural weaknesses [37-38].

### 2.2 Fault Tree Analysis (FTA) Model

FTA model offers effective and reliable hazard analyses in the context of cyber security. It uses graphical depiction of events and relationship as well as top down method for studying causes of hazards in a system via a tree-like structure and Boolean logic for its construction [39]. A fault tree with a voting gate and the Reliability Block Diagram (RBD) equivalent is presented in Figure 5.

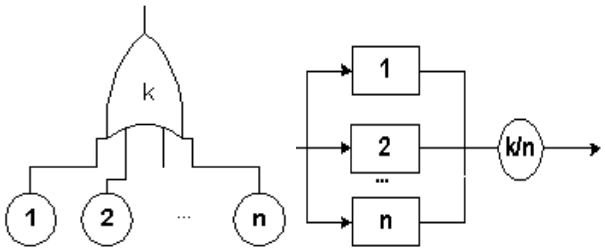


*Figure 5: Event chain risk transfer*

It is a widely adopted model for analyzing systems safety, with the idea that failures at system or sub-

system level could be caused by lower level system(s) or sub-system(s). FTA comprises of system definition, fault tree construction as well as qualitative and quantitative analyses. Its tree-like format promotes a high level understanding with little attention to detailed analysis, thereby, promoting timely detection of hazard-prone scenarios [40]. An FT is a 4-tuple F = {BE,G, T, I}, where BE is the set of basic events, G is the set of gates, with BE ∩ G = Ø, and E = BE ∪G for the set of elements. T is the set of gates and I is a set of inputs to the gates.

An event is an occurrence within the system, typically the failure of a subsystem down to an individual component and can be divided into basic events *(BEs)*, which occur spontaneously, and intermediate events, which are caused by one or more other events [39]. Fault Tree Analysis can be used to understand the logic leading to the top event or undesired state, show compliance with the (input) system safety/reliability requirements, prioritize the contributors leading to the top event and monitor and control the safety performance of the complex system. Other usages include minimization/optimization of resources, system design and diagnosis of causes of event [41-42].

One of the risks that have been posing serious threat to information security across the globe is data leakage from the outbound emails. Although such leakages are sometimes accidental than intentional, the repercussions are often times very severe. A related risk is a case of information leakage through accidental transfer of name, phone and insurance policy numbers, date of birth and Social Security (SS) number to an incorrect email address. Upon the recognition of this error, the email provider is contacted to know the activeness of the account at the time the email was sent.

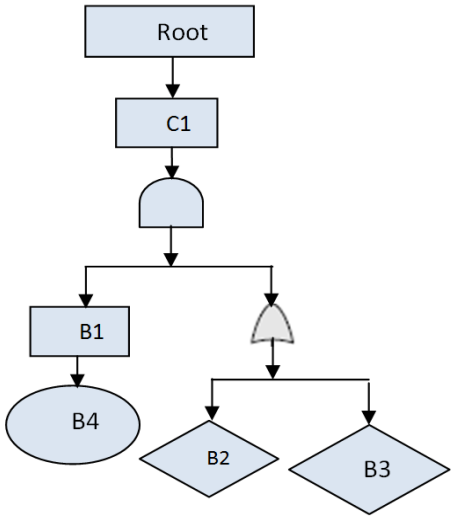


*Figure 6: A fault tree analysis of an accidental data leakage via outbound email*

The emails later bounced back to state that the account was disabled without the original email in question. The causal factors of this error include failure to embrace diligence verification of the recipient of the email as well as lack of policy and procedures for controlling outbound email contents. Absence of control measures such as email encryption or attachment password protection or software is another factor. A fault tree analysis of this error is presented in Figure 6.

C1, B1, B2, B3 and B4 represent incorrect entry of the email recipient, failure to verify email recipient, lack of policy and procedures to monitor outbound emails, lack of technical controls to monitor outbound emails and lack of due diligence respectively. The fault tree reveals that Root Event = C1= B1 ⋂ (B2 ⋃ B3). Since B1=B4, then Root Event = B4 ⋂ (B2 ⋃ B3)= (B4 ⋂ B2) ⋃ (B4 ⋂ B3) and Minimum Cut Sets (MCS) = {B2, B4}, {B3, B4}. MCS implies that if the basic event(s) enclosed in any of the two sets happen, then the root event is likely to take place. For example, with MCS {B2, B4}; an employee in an organization that lacks policy and procedures to control the content in the files attached with the outbound emails will exhibits lack of due diligence and be exposed to accidental data leakage. A countermeasure would therefore require increased awareness and understanding of a policy on the avoidance of the occurrence of the root event amongst the employees [43].

The limitations of FTA model, which have rendered it ineffective for performing causal analysis within the context of cyber security, include lack of standard tools for tree construction specifically applicable for verification, extreme difficulty in the implementation insights and presentation of dynamic behaviours [35].

### 2.3 Control Objectives for Information and Related Technology (COBIT)5

COBIT 5 manages information security base on a set of enablers that are tailored toward an organization's environment. The enablers help organizations to fundamentally change with reference to managing information security by also focusing on non-technical aspects of information security. COBIT 5 offers general guidelines for information security on meeting stakeholder needs, covering enterprise end-to-end, integrated framework, enabling a holistic approach and separating governance from management. The model is suitable for integrating platforms for initiating holistic changes needed for managing cyber security risks. COBIT 5 is designed to be an overarching framework that can integrate with other standards

such as ISO/IEC 27002 framework for good practices and standards, thereby allowing for flexibility and broader coverage with reference to standards as shown in Figure 7. Some security breaches have been attributed to careless handling of credit card information, uncontrolled or unrestricted access to customers' information, absence of countermeasure against system hacking and reconfiguration and weak or vulnerable username and password. COBIT 5 strategy for managing threats or risks arising from these breaches involves strict adherence to some standard management practices; namely APO13.01, DSS5.01, DSS5.02, DSS5.03, DSS5.04, DSS5.05 and DSS5.06. These practices require effective monitoring mechanisms and their implementation is conceptualized in Figure 8 [44].

However, the model could only support causal factor analysis, therefore requiring additional methods or models for implementation which is dependent on effective management change within an organization such that time frame can be an issue in order to achieve the desired level of information security. Furthermore, COBIT 5 requires broader in-house expertise to manage an integrated framework of multiple standards [45-46].

### 2.4 ISO/IEC 27002

This model was developed to provide international standard and best practices for dozens of controls and mechanisms for information security management including security policy, asset management, communications and operations management, access control and information security incident management. The objective is to provide guidance on network access control and cover areas of policy on use of network services and user authentication for external connections. ISO/IEC 27002 standards incorporate lessons from past experiences accumulated over many years, making them valuable tools for managing cyber security risks. It also provides detailed guidelines at a much lower level that is very close to implementation layer.

With this model, risks due to territorial intrusion, unauthorized access to secure areas, unlawful image acquisition, absence of video surveillance cameras among others are managed using some facility and human resource-based strategies. The strategies include strict monitoring of physical access to premises and infrastructure, regular review and approval of people authorized to access secured areas, placing of embargo on photography or video recording inside restricted areas and all-time escort for visitors to important, sensitive and special areas.

Regular screening of employee prior to employment, sworn to oath of secrecy, regular update of physical access right, lengthy, complex and well secured password and disabling of write access to removable media on all desktops are other very important strategies. The main limitation is its static nature. In addition, the standard states that new controls or guidelines not in the standard may be required and should be included resulting in subjectivity and bias in deciding what controls will be effective and should be included, possibly leading to ignoring guidelines and controls that are more relevant [47-48].

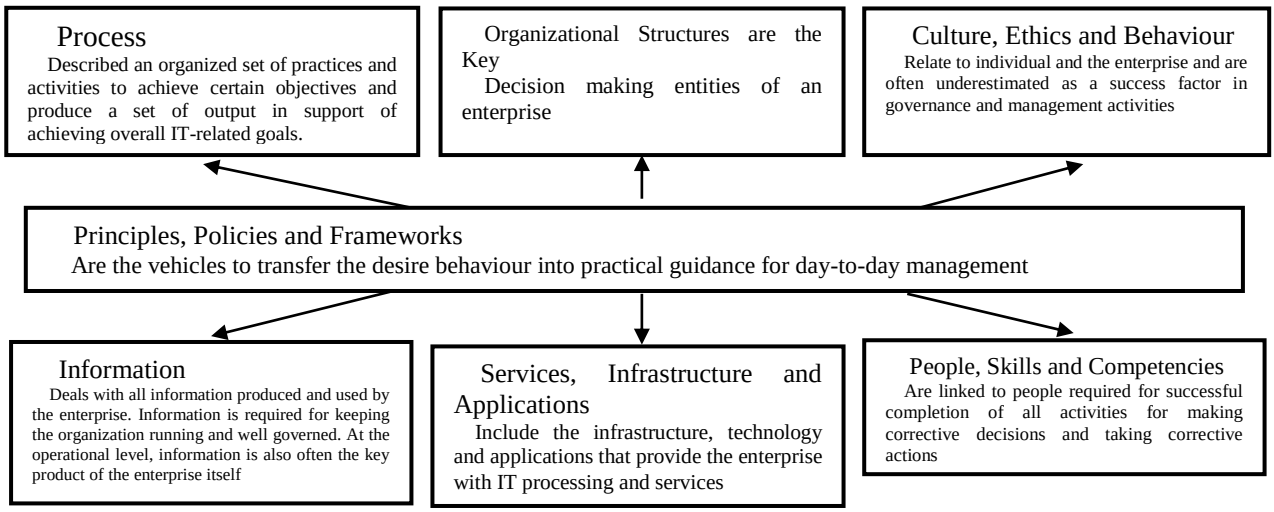


*Figure 7: COBIT 5 Enabler: Systemic model with interacting enablers [45*]

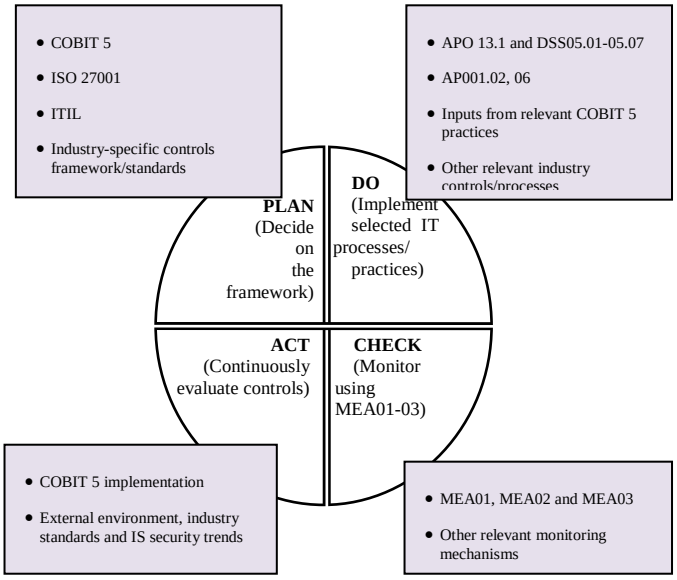


*Figure 8: Proposed COBIT 5-based Implementation framework for Data breach prevention*

### 2.5 Systems-Theoretic Accident Model and Processes (STAMP)

Due to the inability of existing models to take into account organizational and social factors, human decisions or behaviors and software design flaws, individuals, businesses and governments are exposed to cyber security risks. This necessitated the formulation of STAMP to complement traditional approaches for managing cyber security risks that focuses mostly on technical and alternative solutions that also address non-technical aspects of cyber security.

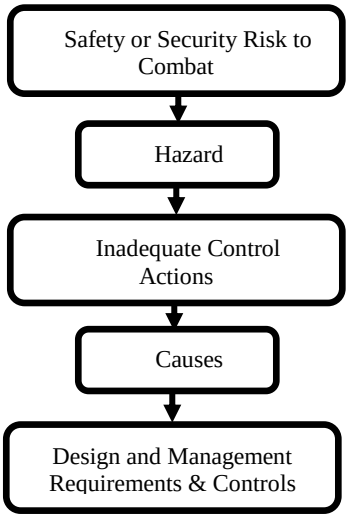


*Figure 9: STAMP Process*

Furthermore, STAMP serves in the development of a framework for managing cyber security risks holistically and is based on the process illustrated in Figure 9 [49]. Accident is an unplanned and undesired event which may lead to death, injury or property, financial or information loss [50-51].

Within the context of technology assets, accidental losses may include data and/or unauthorized access (loss of credentials) or denial of access. With the STAMP model, understanding the causal factors such as negligence and uncontrolable circumstances that may lead to the risk of an accident requires knowing the reasons for the failure of the safety strategies in such cases.

Focus is not on preventing failure event(s) but on implementing effective controls for enforcing relevant constraints, with safety constraints, hierarchical safety control structures and process model as core concepts. With STAMP, safety constraints are the foundation, while missing constraints or lack of enforcement of relevant constraints leads to elevated cyber safety risks, which may cause loss event(s). Hence, the main essence of STAMP is to manage cyber safety risks, using carefully defined constraints analysis base on hierarchical safety control structures where a higher level imposes constraints over the lower level. Processes at lower level of hierarchy are managed by control process that operates between levels. Despite the reported strengths, it is still noted that STAMP has not been useful in the design of a system for providing safety and guidance on the implementation of STAMP in the context of cyber security [52].

## 3. SYNOPSIS OF SOME RESEARCH WORKS ON CYBER-SECURITY RISK MANAGEMENT

The summary of the objectives, methodologies and the limitations of some research works that are based on

the models presented in the preceeding Section is presented in this Section. In [53], an Attack Tree Based Comprehensive Framework (ATBCF) for the Risk and Security Assessment of Vehicular Ad-hoc Network (VANET) using the concepts of game theory and fuzzy logic is presented. VANET is a class of Mobile Ad-hoc Network that enables vehicles to communicate with each other as well as with the roadside units. It uses wireless medium as a mean of communication among the vehicles, it support a large range of promising applications with high level of securities. VANET faces a lot of research challenges in terms of security because its existing risk and security analysis approach failed to work well as it is purely based on the ideological beliefs and it does not reflect any realistic conditions. The research explored and discussed the usage of game theory and fuzzy logic in analysis of the attack and defense equilibrium. The authors carried out systematic study of the various algorithms for finding the inflection points of equilibrium that further reflects a trade-off between the attacker and the defender's gain or loss payoff for pursuing their pursuit. This approach does not conduct the assessment of the assets, which could support comparative analysis of the risk.

The authors in [54] proposed a game-theoretic modeling of computer security using security attack scenarios as an optimization game comprising of multiple players, the attackers and the defenders. The research analyzed a two-player zero-sum stochastic game model of the interaction between malicious users and network administrators and also introduced a hypothetical network of a typical scenario to show the applicability of the model. State games were encoded using a binary scheme resulting in the reduction of each state game into a min and max linear programming problems for both the defender and attacker. A combination of pivotal and custom stochastic algorithms was proposed for computing the optimal strategies for the players at each state. Though the model produced promising results, it could not predict how vulnerabilities are exploited by attackers nor analyze their behaviours. The authors in [55], presented a game-theoretic analysis of attack and defense in cyber-physical network infrastructures. The research is motivated by the fact that game theory has been used in studying the strategic interactions between attackers and defenders for critical infrastructure protection, but has not been extensively used in complex cyber-physical networks. The research focused on using game theory to model the probabilities of successful attacks in both cyber and physical spaces as functions of the number of components that are attacked and defended. The Cyber-Physical Network Infrastructure (CPNI) consists of hardware, software, people, organizational policies and procedures, all linked by high speed networks. The successful functioning of CPNI requires that both cyber and physical components run smoothly including the functionality after being attacked. The model assume that the defender wants to minimize the cost and system loss; that is, to maximize her utility and for simplicity, analyze cyber and physical spaces separately and compute attacker's and defender's best response accordingly. Some insights into the survival of cyber-physical networks infrastructures and optimal resource allocation under various costs and target valuations that players may have was given. However, this approach does not include the study of interdependent coupling effect between the cyber and physical components in the CPNI, as well as the game with incomplete information. The authors in [56] proposed a game theory approach to communication security by modeling the interactions between attackers and defenders as games in three types of communication scenarios. In the first scenario, a simple intruder game is modeled as showed in Figure 10. Alice, Trudy and Bob represented the agents or components that are capable of storing, traferring or processing information on the game.

Alice sends a message X to Bob through an insecure channel. The channel is insecure because Trudy, an intruder, is present to corrupt $X$ which, is viewed to be a binary random variable ($\boldsymbol{X} \in \{\mathbf{0}, \mathbf{1}\}$) drawn from the set {0,1} according to a probability distribution $\mathbf{Pr}[\boldsymbol{X} = \boldsymbol{x}] = \boldsymbol{\pi}(\boldsymbol{x}), \boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}\}$ that is assumed to be known to Bob and Trudy. Y is a designate of X that Bob receives. Trudy is present with a probability $p$ known to Trudy and Bob. In the absence of Trudy, Bob correctly receives the message sent by Alice $Y = X$ and when Trudy is present, her possibly randomized strategy that modifies $X$ into $Y$ *is modelled* by the probabilities:

$$\mathbf{P}(\mathbf{x}, \mathbf{y}) = \mathbf{Pr}[\boldsymbol{Y} = \boldsymbol{y} | \boldsymbol{X} = \boldsymbol{x}] \, \boldsymbol{for} \boldsymbol{x}, \boldsymbol{y} \in \{\mathbf{0}, \mathbf{1}\}$$

The second scenario considered cases of a virus making an attempt of carrying out a simultaneous infection of several machines in a simple IDS-protected network as presented in Figure 11. The normal traffic going through the network is assumed to have a known rate $\alpha$. When present, the virus, while trying to infect parts of the network, generates some additional traffic with a rate, $\beta$ that the virus designer needs to set. The IDS needs to detect the virus early enough while limiting false alarms.

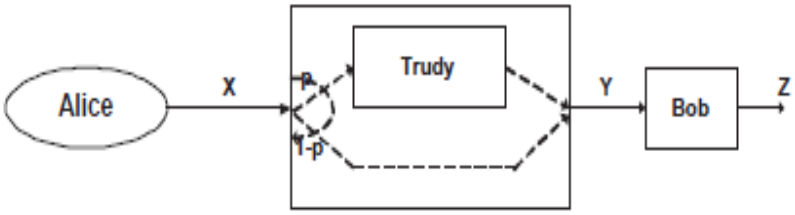


*Figure 10: Intruder game model*

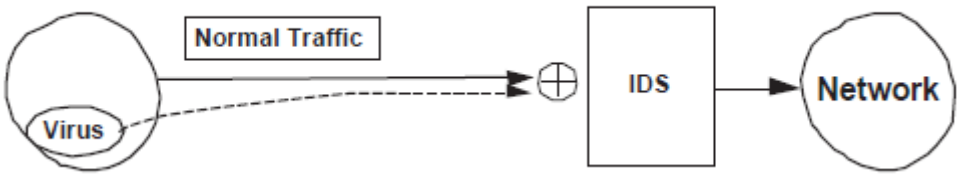


*Figure 11: Intelligent virus game model*

For intrusions detection, the IDS check the volume of traffic going through the network against a chosen threshold.

The third scenario considered availability (or denial of service) attacks where resources that are (or might be) needed by a defender are the target of a cognitive attacker. More precisely, consideration was given to a situation with a finite set $S$ and two collections $\boldsymbol{\tau}$ and $\boldsymbol{\varepsilon}$ of subsets of $S$. The defender selects a subset $\boldsymbol{T} \in \boldsymbol{\tau}$ to perform a *mission critical* task. Each subset $\boldsymbol{T} \in \boldsymbol{\tau}$ needs some set of resources $e_{T1}, e_{T2}, \ldots, e_{Tp} \in \boldsymbol{\varepsilon}$ in order to fulfil the task. To disrupt the mission, an attacker will need to targets one resource $\boldsymbol{e} \in \boldsymbol{\varepsilon}$ *for* attack. Based on the computation and analysis of the Nash equilibria of the games, the work predicted the adversaries' attacks, determined the set of assets that are most likely to be attacked and suggested defense strategies for the defenders

It determined the structure of a particular Nash equilibrium for a class of bimatrix games and completely characterized the structure of all Nash equilibria for a subset of those games. The limitation of the work is that, in Nash equilibrium, while the attacker always targets a critical subset of resources, the defender should only use a minimal amount of resources in the critical subset. In [57], a model that supports an attacker and the network administrator participation in a two-player zero-sum stochastic game is presented. At each state $k$, $k = 1, \ldots, p$ of the model, the Attacker's pure strategies in a network with n nodes consist of $m_k = n+1$ actions and it is either one of $n$ nodes is being attacked (represented as $\boldsymbol{c_i^k}$, where $i = 1, \ldots, n$) or nothing is happening (represented as $\boldsymbol{m_{m_k}^k} = \emptyset$). Attack to any of the nodes may be denial of service, password compromise, data corruption among others. With the payoff formulation, the Attacker is focusing on attacking an uncompromised node, except if all the nodes have been compromised. For every $k$, the Defender will either defend the node i by any known method such as encryption or token passing (represented as $\boldsymbol{d_i^k}$, $i = 1, \ldots, n_k-1$) or remain idle (represented by $\boldsymbol{d_{n_k}^k} = \emptyset$) where $n_k = m_k = n+1$. For every combination of the Attacker's and the Defender's strategies, the payoff entries matrix is presented as follow:

$$\boldsymbol{\alpha_{ij}^i} = \boldsymbol{a_{ij}^i} + \sum_{i=1}^{p} \boldsymbol{q_{ij}^{kl}} \boldsymbol{\tau_l} \qquad (2)$$

$$\boldsymbol{a_{ij}^i} = \boldsymbol{p_s^k}\left(\boldsymbol{c_i^k}, \boldsymbol{d_j^k}\right)\boldsymbol{x^k}(\boldsymbol{i}) \qquad (3)$$

$\boldsymbol{p_s^k}\left(\boldsymbol{c_i^k}, \boldsymbol{d_j^k}\right)$ represents the probability of a successful attack while $\boldsymbol{x^k}$(i) is the effective security asset of node i, being attached. Once a node is compromised, the effective security assets and the supports of the remaining nodes have to be recalculated. The work assumed that the network consists of a set of interdependent nodes whose security assets and vulnerabilities are correlated. It utilized the concept of linear influence networks and modeled the interdependency among nodes by two weighted directed graphs, one signifying the relationship of security assets and the other denoting vulnerability correlation among the nodes. However, due to node correlation, during cases of compromises, the effective security assets and vulnerabilities of the remaining ones will be altered leading to complex system dynamics.

In [58], the authors investigated the problem of design

of Nash Equilibrium for quite a general class of games from an optimization and control theoretic perspective with a view to analyzing how long the game tends to Nash equilibrium when several players are trying to solve it in a distributed way. The essense of the analysis was to suggest a feedback control system with pricing as a control input, make the system robust, control the system's progress and investigates system's controllability. Treatment and investigations were restricted to a class of games where players do not manipulate the game by deceiving the system designer and where utility functions accurately reflect user preferences. The games were discussed with incomplete information of two objective functions; namely quality of service (QoS) and utility maximization. The pricing dynamics in different conditions were explored and inferred that loss of efficiency is not an inherent feature of a broad class of games with built-in pricing systems, but merely a misconception that often stems from arbitrary choice of game parameters. The limitation is that the model does not apply Nash equilibrium design methods to specific problems such as power control in optical networks and spectrum allocation in wireless networks. Similarly, the analysis of estimation methods under limited information and the effect of estimation errors on performance were not considered.

The authors in [59] presented a computational approach to quantitative risk assessment for investment efficient strategies in cyber security. The work focused on protection of critical intellectual property in private and public sectors by placing assumption on the possibility of reverse engineering attacks. An attack/protect economic modelcast in a game theoretic context was also developed. A small scale simulation was done, which may be unrealistic in complex systems under attack by rational and capable adversaries. The authors in [60] modeled intrusion response as a resource allocation problem based on game theory. A cost is associated with attacks and responses that include imperfections in the sensor outputs were modeled as a continuous game.

The vectors $c^I := [c_1^I, c_2^I, \dots, c_{R_{max}}^I]$ and $c^A := [c_1^A, c_2^A, \dots, c_{A_{max}}^A]$ represent the costs (to the owner) and gains (to the attacker) respectively. Attacking a network takes time and effort, and response strategies usually involve some negative externalities. Hence, the cost of responding to an attack is captured in the vector $\alpha = \alpha_1 \dots, \alpha_{R_{max}}$ and the cost of attempting an attack is captured in the vector $\beta = \beta_1 \dots, \beta_{A_{max}}$. Due to conscious decisions or security imperfections, vulnerability to attacks vary across systems and this factor is captured by a nonnegative matrix Q with diagonal entries greater than or equal to 1. The $\bar{Q}$ matrix is the correlation between the response and attack strategies. It is made up of ones and zeros with dimension $A_{max} \times R_{max}$. The scalar, cost for the IDS, $J^I(U^A, U^A, P)$ and the attacker(s) $J^A(U^A, U^A, P)$ are presented as follow:

$$J^I(U^A, U^I, P) = \gamma(U^A)^T P \bar{Q} U^I + (U^I)^T diag(\alpha) U^I + c^I(QU^A - \bar{Q}U^I) \quad (4)$$

$$J^A(U^I, U^A, P) = \gamma(U^A)^T P \bar{Q} U^I + (U^A)^T diag(\beta) U^A + c^A(QU^I - \bar{Q}U^A) \quad (5)$$

$\gamma$ presents the relative value of various cost terms in the equations, T represents the transpose function and $diag(\alpha)$ and $diag(\beta)$refer to diagonal matrices with diagonal entries containing the corresponding entries in vectors $\alpha$ and $\beta$ respectively. The first terms of these equations are zero-sum and represent the cost of false-alarms and benefit of detection for the IDS and the cost of capture and benefit of deception for the attacker. The second terms characterize the cost of effort associated with responding to or generating an attack. The actual benefit or cost of a successful attack is represented in the third term.

The strategies are discretized both in time and intensity of actions, which eventually leads to a discretized model. After discretization, the reaction functions uniquely minimize the strictly convex cost functions that become a constrained integer optimization problem. The authors introduced a dynamic algorithm called Automatic or Administrator Response algorithm (AOAR) (conceptualized in Figure 12) to solve the problem and the results showed that the introduction of the algorithm contributed to improved performance.

The limitation of the model is that while laying out a practical implementation of the algorithm and demonstrating its utility, there is lack of a formal theoretical framework and the algorithm have not been applied to more elaborate models to ascertain its practicability.

In [61], the authors presented an intrusion detection algorithm in mobile ad-hoc networks with two-player game model. Game theory was used to model the interactions between the intrusion detection system and the attacker resulting in a Bayesian game–based framework (conceptualized in Figure 13). The existence of Nash Equilibria in static scenario was analyzed with defender updates based on new observations. Bayesian Nash Equilibria in the static model was investigated with results showing how IDS could work intermittently without compromising its effectiveness. The research placed assumption that an

IDS needs not be running all the time, thereby creating idle time for the wireless ad hoc network. Malicious players can take advantage of the idle periods to launch attack.

The authors in [62] proposed a methodology for modelling the interactions between a Distributed Denial of Service (DDoS) attacker and the network administrator. This approach observed that the ability to model and infer Attacker Intent Objectives and Strategies (AIOS) can lead to effective risk assessment and harm prediction. An incentive-based game-theoretic model to infer AIOS (conceptualized in Figure 14) was presented using bandwidth parameters to measure the impact of the attack (such as infection with daemon program or use of zombies to send constant bit rates (CBR)) and the countermeasure (such as enforce pushback or set the target drop rate for each router), which in turn measures the attackers' and defenders' incentive. The attacker was modeled as the attacking system and the environment only includes the set of good accesses from legitimate users.

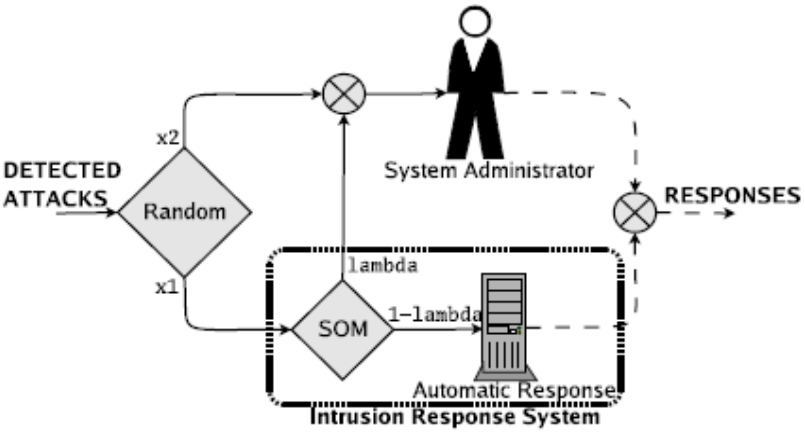


*Figure 12: The conceptualized of AOAR algorithm*

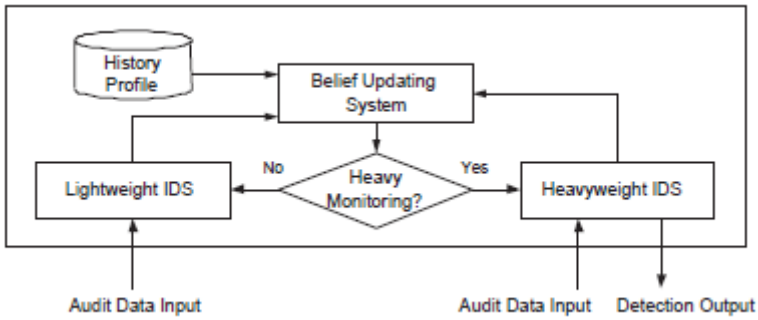


*Figure 13: The Bayesian hybrid detection framework*

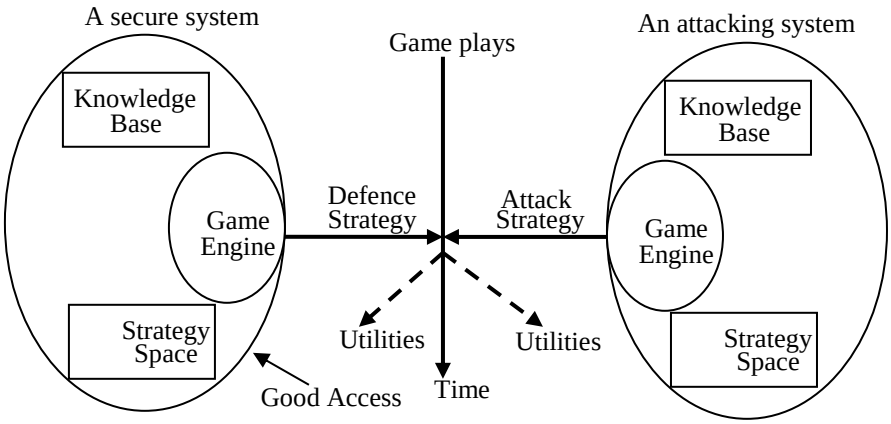


*Figure 14: An incentive-basedgame-theoretic model to infer AIOS*

The attacking system is splinted into the service and protection parts. While the service part includes all and only the components that provide computing services to users, such as the hardware and software components that route packets, the protection part includes the set of protection components. The relation between the system and the attacker is modeled as a game (or battle) across the time dimension for effective defensive actions rather that passive monitoring, detection and reaction to attacks. The work also observed that the best game model to choose depends on the degree of accuracy of the employed Intrusion Detection System (IDS) and the degree of correlation among the attack steps. However, this work gives no consideration to inference accuracy and sensitivity analyses that can model and predict the influence of incomplete information, asymmetric information (between the attacker and the system) and uncertainty.

In [63], the authors presented examples of static information on strategies, countermeasures, payoffs and costs of warfare games on terrorism, evil act, vandalism and rebellion. Pure strategies for the player *i* is modelled as $\boldsymbol{S_i}$. For player i with M pure strategies $\boldsymbol{S_i} = \{\boldsymbol{S_{i1}}, \boldsymbol{S_{i2}}, \dots, \boldsymbol{S_{iM}}\}$, then a mixed strategy is a probability distribution $\boldsymbol{P_i} = \{\boldsymbol{P_{i1}}, \boldsymbol{P_{i2}}, \dots, \boldsymbol{S_{iM}}\}$, $\boldsymbol{0 \le p_{im} \le 10}$ for m = 1, ..., M and $\boldsymbol{P_{i1} + P_{i2} = \cdots + P_{iM} = 1}$. A mixed strategy indicates one player's uncertainty about what another player will do. A pure strategy $\boldsymbol{S_{im}}$ was represented as a mixed strategy by setting $\boldsymbol{P_{im}}$ to 1 (and the remaining terms in the probability distribution being 0). The expected payoff $\boldsymbol{v_i}$ for player *i* in an *n* -player static game $\boldsymbol{G} = \{\boldsymbol{S_1}, \dots, \boldsymbol{S_n}, \boldsymbol{u_1}, \dots, \boldsymbol{u_n}$when player $\boldsymbol{j}(\boldsymbol{1 \le j \le n})$ plays the mixed strategy $\boldsymbol{P_j}$, is based on the formula:

$$v_i(p_1, \dots, p_n) = \sum_{m_1=1}^{M_1} \dots \sum_{m_{n=1}}^{M_n} [\prod_{k=1}^{n} P_{km_k}] u_i(S_{1m_1}, \dots, S_{nm_n}) \quad (6)$$

$M_j$ is the number of pure strategies available to player *j.* For a two-player case (1) is:

$$v_i(p_1, p_2) = \sum_{m_1=1}^{M_1} \sum_{m_{2=1}}^{M_2} P_{1m_1} P_{2m_2} u_1(S_{1m_1}, \dots, S_{2m_2}) \quad (7)$$

Game theory were studied with emphasis on how a bold playing strategy can lead to domination, how a mixed playing strategy can reduce domination, how it can be useful to play a dominating strategy only part of the time and how excessive domination can lead to rebels where all playing parties lose. Investigation was also conducted to know if more than one Nash Equilibria exist and if so, then which one is most likely to appear as the outcome given the players' strategies. The practicality test showed that depending on the scenario the players could get the benefit of a bold strategy or a mixed strategy. The limitation of the work is that only credible threats can have an effect on current behaviour. Attackers can exploit this fact, by modifying the opponent's observations and perceptions of the payoff functions and strategies in the game. A game theoretic approach to model intrusion detection in mobile ad-hoc networks proposed in [64] is conceptualized in Figure 15. Based on the approach, the IDS will record a gain of $-\boldsymbol{\gamma_{success}}$ in the detection of an attack while it also record a cost whenever the IDS misses an attack ($-\boldsymbol{\gamma_{miss}}$) or when a false alarm ($\boldsymbol{\gamma_{falarm}}$) is raised. Conversely, the intruder will record $-\boldsymbol{\delta_{intrude}}$ and $\boldsymbol{\delta_{caught}}$ as a gain of a successful (undetected) intrusion and a cost of being detected and blocked respectively. False alarms have a zero cost value to the attacker whose expected payoff (*p*) and IDS, *d* in all possible cases are as follows:

$$\mathbf{p = s[t\delta_{caught} - (1 - t)\delta_{intrude}]} \quad (8)$$

$$\mathbf{d = s\gamma_{miss} + t\gamma_{alarm} - st(\gamma_{detect} + \gamma_{falarm} + \gamma_{miss}} \quad (9)$$

The models viewed risk intrusion and its detection as a game played between the attacker node and the IDS hosted on the target node with the attacker sending a malicious message with the intention of attacking the target node. However, this approach does not take into account selfish nodes and groups of colluding attackers. Such security countermeasures against node misbehavior and denial of service attacks are necessary for the model to be practicable.

The authors in [65] proposed a game model for the security of a computer network. An enterprise network is envisioned as a graph of 4 nodes (web server, file server, work station and external world) along with the traffic state for all the links.

It is a two-player (administrator, attacker), stochastic, general-sum game and the authors focused on 3 attack scenarios; namely defaced website, denial-of-service and stealing confidential data. With different initial conditions a set of Nash equilibria were calculated using a nonlinear program. The model underperforms with cases of full state space extremely large. Also in building the game model, it may be difficult to quantify the costs for some actions and transition probability may not be easily available.

## 4. STRENGTHS AND WEAKNESSES OF GTA

Findings from the survey have shown that game theory models are generally explicit and unambiguous in nature and are easy to criticize or subscribe to. The model provides a limited representation of reality; hence real problems can easily be tackled.

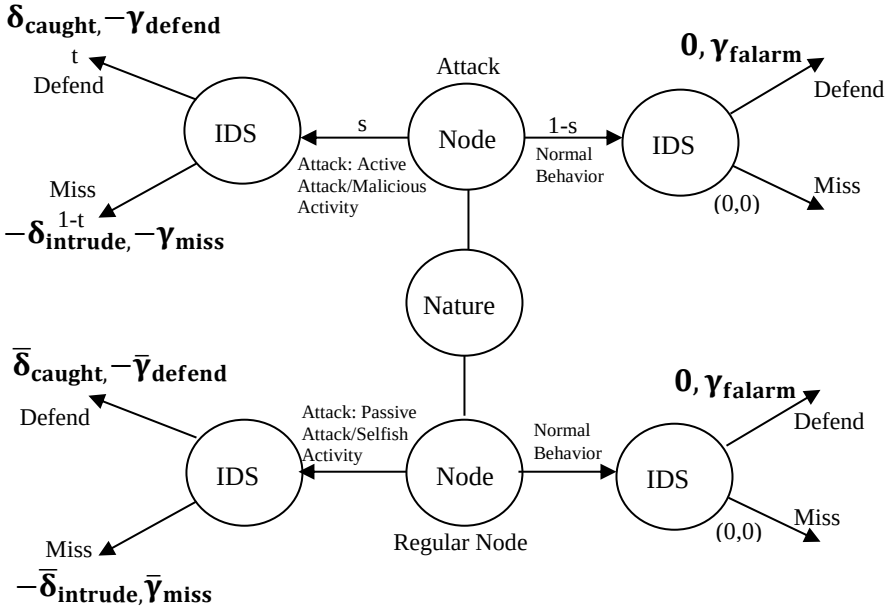


*Figure 15: Intrusion detection in mobile ad-hoc networks*

A game theory solution is reliable, consistent and can easily be manipulated, augmented and eliminated. It offers to the knowledge on acceptance or rejection of a hypothesis and is applicable to a close system because the payoffs of all participants are added up to be zero (winning = (+) and loses = (-)) and then the game is called zero-sum game, otherwise, it is known as non-zero-sum game [66]. However, in game theory, players are rarely fully rational and do not have complete information about each others' payoffs and strategies. Hence, modelling the decision process by means of a few equations and parameters is questionable. There is also the difficulty of quantifying the value added by cyber security. The lack of quantification affects the decision making process regarding security investments. Hence, the attitudes towards security seem unstable depending on the economic situation. This shows that quantifying security related concepts such as trust, privacy and risk in game-theoretic models calls for special attention. Finally, game theory always imposed constraints being the only way to correctly formulate the problem and it is based on the assumption that the parties are rational and few in numbers and that each player knows the objectives of his opponent [66-67].

The complexity of computing an equilibrium strategy and difficulties in quantifying security parameters (such as risk, privacy and trust), choosing the appropriate game model for a given security problem and reaching consensus on how to interpret a mixed strategy further compounded the woes of game theory to cyber security risk management. Despite these challenges, the strength of game theory over other existing techniques suggests that it would be unreasonable to abandon the technique, especially in the absence of a reliable alternative. Security games study the interaction between malicious attackers and defenders which serve as basis for formal decision making and algorithm development as well as for predicting attacker behaviour. The applicability of game theory is due to the fact that it is a context-free mathematical toolbox that can be used in any situation of interactive decision making.

## 5. CONCLUSION

Findings from the survey of some existing models for game theoretic approach to cyber security risk management has been presented with emphasis on strengths, weaknesses, opportunities and threats. The models include Chain-of-Events, Fault Tree Analysis, COBIT 5, ISO/IEC 27002 and System-Theoretic Accident Model and Processes. Findings reveal that these models are still in their developmental stages with much improvement needed. Synopsis of some recent research works on cyber security risk management that are premised on these methods is also presented with focus on the motivations, objectives, methodologies and the attendant limitations. In view of the fact that threats to cyber security change with advent of new technology, hence, the need for continuous monitoring and management of the cyber security plan. Future research therefore

aims at the experimental study of these models and proposing models that will address existing and envisaged threats or risks to cyber security as well as some of the limitations of the reviewed works.

## 6. REFERENCES


[1] Adeyinka, O., "Internet Attack Methods and Internet Security Technology", *Second Asia International Conference on Modeling & Simulation,* 13-15 May, pp.77-82. 2008

[2] Ateeq, A., "Type of Security Threats and It's Prevention", International Journal of Computer Technology & Applications, Vol. 3, Number 2, pp 750-752 (2012), Available: http://ijcta.com/documents/volumes/vol3issue2/ijcta2012030240.pdf, Assessed on 30th December, 2014.

[3] Deloitte Development LLC Audit Committee Brief, 2013, Available: http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Deloitte%20Periodicals/Audit%20Committee%20Brief/ACBrief_October2013.pdf, Accessed 21/04/2014

[4] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V. and Wu, Q. "A Survey of Game Theory as Applied to Network Security", 43rd HICSS, Hawaii, IEEE Press, pp 1-10, 2010.

[5] Ehrlich, J. and Becker, G. "Market Insurance, Self-Insurance and Self-Protection", *Journal of Political Economy,* Vol. 80, pp 623-648, 1972.

[6] Alese, B. K. "Security Issues in Nigeria: Getting ready for the Digital Challenge", Annual Lecture, First Bank of Nigeria Plc Professorial Chair in Computer Science, Federal University of Technology, Akure, Nigeria, 2014

[7] Alese, B. K., Iwasokun, G. B. and Haruna, D. I. "DGM Approach to Network Attacker and Defender Strategies", *World Congress on Internet Security Technologies and Secured Transactions*, UK, Vol. 3, Number. 2, pp 374-382. 2013,

[8] Frank, B. and Strickland, G. L. "The Cyber Underground Economy: Unconventional Thinking for a Fundamentally Different Problem", IBM Center for The Business of Government, 2011, Available: http://www.businessofgovernment.org/article/cyber-underground-economy-unconventional-thinking-fundamentally-different-problem, Accessed: 14/12/2015.

[9] Geers, K. "Strategic Cyber-security", NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, 2011

[10] Baldi, S., Gelbstein, E. and Kurbalija, J. "Hacktivism, Cyber-Terrorism and Cyberwar", The Information Society Library, DiploFoundation, Geneva, Switzerland, 2003 and US Government Accountability Office (GAO) Report on Cyberspace, Washington, DC, GAO-10-606, 2010

[11] National Guidance on Implementing ISO 31000 NSAI, Ireland 2009.

[12] Alazzawe, A., Nawaz, A. and Bayaraktar, M. M. "Game theory and intrusion detection systems", unpublished, Available: http://theory.stanford.edu/~iliano/courses/06S-GMUISA767/project/papers/alazzawe-mehmet-nawaz.pdf, Accessed 06/07/2014.

[13] Gordon, L. "Cyber-security management, 2014, Available: http://www.rhsmith.umd.edu/ faculty/lgordon/cybersecurity/Cybersecurity, Accessed 23/01/2015

[14] Diana, K. "Application Security Risk Management and the NIST Cyber Security Framework", 2014, Available: https://securityintelligence.com/nist-cybersecurity-framework-application-security-risk-management/, Accessed 17/07/2015.

[15] Artz, M. L. "A Network Security Planning Architecture", Master's Thesis in Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2002, Available: https://dspace.mit.edu/bitstream/handle/1721.1/29899/51072296-MIT.pdf?sequence=2. Accessed: 30/12/2014.

[16] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., andLaplante, P. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political", *IEEE Technology and Society Magazine*, Vol. 30, Number 1, 2011, pp28-38, Available: http://dx.doi.org/10.1109/MTS.2011.940293, 2011.

[17] Andreasson, K. J., 2011. "Cybersecurity: Public Sector Threats and Responses", In K. J. And reason (Ed.),: XIII-XXV. Boca Raton, FL: CRC Press

[18] Russell, D. and Gangemi, G. T. "Computer Security Basics". Sebastopol, CA: O'Reilly & Associates, 1993.

[19] Edward, M. "Causes of Cyber Crime", Available: http://itstillworks.com/causes-cyber-crime-1846.html, Accessed 15/07/2017

[20] Bode, M. A., Alese, B. K., Thompson A. F. and Iyare O. "A Bayesian Network Model for Risk Management in Cyber Situation", World Congress on Engineering and Computer Science, 22-24 October, , San Francisco, USA, Vol. I, 2014.

[21] Xie, P., Li, J. H., Ou, X., Liu, P. and Levy, R "Using Bayesian Networks for Cyber Security Analysis", 2010, Available: https://pdfs.semanticscholar.org/c0bc/ffddd322236c8800680f5ebd59ed5923ea6c.pdf, Accessed 12/04/2016

[22] Kehe, W. and Shichao, Y. "An Information Security Threat Assessment Model based on

Bayesian Network and OWA Operator", *Application of Mathematics in Information Science*, Vol. 8, Number 2, pp833-838, 2014.

[23] Xiaochun, X., Tiange, Z. and Gendu, Z."Extended Abstract: Access Graph Based Risk Analysis for Network Information System", International Conference on Security Technology, 2008 Available: https://www.computer.org/csdl/proceedings/sectech/2008/3486/00/3486a129.pdf, Accessed 16/07/2017

[24] Jason, L., Xinming, O., and Raj, R. "Uncertainty and Risk Management in Cyber Situational Awareness", 2010, Available: http://www.cse.usf.edu/~xou/publications/uncertainty_ca10.pdf, Accessed 17/07/2017

[25] Muckin, M. and Fitch S. C. "A Threat-Driven Approach to Cyber Security: Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization", Lockheed Martin Corporation, Available: http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf, Accessed 12/07/2017

[26] Alberts, C. Dorofee, A..Stevens, J. and Woody, C. "Introduction to the OCTAVE approach", Software Engineering Institute; 2003.

[27] Yazar, Z. "A qualitative risk analysis and management tool", CRAMM. SANS Institute; 2002.

[28] Karin, S., Knapskog, S. J. and Helvik, B. E. "Using Stochastic Game Theory to Compute the Expected Behavior of Attackers", International Symposium on Applications and the Internet, Trento, Italy, 2005.

[29] Lewis, J. A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies (CSIS) (2002), Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, Accessed 14/05/2013

[30] Lindstrom, G. "Meeting the security Challenge", Geneva Centre for Security Policy, 2012, Available: https://www.ciaonet.org/attachments/21111/uploads, Accessed 16/02/2014

[31] Stallings, W. "Network Security Essentials, Applications and Standards", 4th Edition, *Prentice Hall,* Boston Columbus Indianapolis, 2002

[32] Theodore, L. T. and Bernhard, V. S. "CDAM Research Report", LSE-CDAM-2001-09, 2001

[33] Whitman, M. E. and Mattord, H. J. "Management of Information Security", Course Technology, 2004.

[34] Leveson, N. G. "Accident Models, Safeware", Addison-Wesley, pp. 185-224, 1995

[35] Leveson, N. G. "Fault Tree Analysis, Safeware", Addison-Wesley, pp. 317-326, 1995

[36] Intaver Institute. "Event Chain Methodology in Project Management", Interver Institute Inc. 2013, Available: www.intaver.com/Articles/Article_EventChain Methodology.pdf), Accessed 12/08/2015

[37] Ludmila, M. "Experimental Testing of Game-Theoretical Predictions: The Ultimatum Game", Charles University in Prague. Faculty of Social Sciences, Institute of Economic Studies, 2011.

[38] Marin, G. A. "Network security basics, Security & Privacy", IEEE , Vol. 3, Number 6, , pp68-72,2005.

[39] Ruijters, E. and Stoelinga, M. "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools", Elsevier Computer Science review, 2015, Available:nwww.sciencedirect.com, Accessed 14/09/2016

[40] Codetta-Raiteri, D., Franceschinis, G., Iacono, M. and Vittorini, V. "Repairable fault tree for the automatic evaluation of repair policies*", IEEE International Conference on Dependable Systems and Networks*, pp. 659–668, 2004.

[41] Goldberg, B. E., Everhart, K., Stevens, R., Babbitt, N., Clemens, P. and Stout, L. "System engineering toolbox for design-oriented engineers", Marshall Space Flight Center, pp35-48, 1994.

[42] Lacey, P. "An Application of Fault Tree Analysis to the Identification and Management of Risks in Government Funded Human Service Delivery", *2nd International Conference on Public Policy and Social Sciences*, 2011, Available: http://ssrn.com/abstract=2171117, Accessed09/07/2013.

[43] Pallavi, P., Pavol, Z., Dale, L. and Ron, R. "Fault Tree Analysis of Accidental Insider Security Events", *International Conference on Cyber Security*, 2012

[44] Mathew, N. and Hussein, F. "Using COBIT 5 for Data Breach Prevention", ISACA Journal Vol. 5, 2013

[45] ISACA. "COBIT 5 for Information Security, Rolling Meadows, IL: ISACA, pp. 23, 55-59, 2012.

[46] Pasquini, A. andGalièl, E. "COBIT 5 and the Process Capability Model, Improvements Provided for IT Governance Process", FIKUSZ Symposium for Young Researchers, Obuda University Keleti, , pp 67-76, 2013.

[47] International Organization for Standardization, ISO."ISO/IEC 27002:",2005, Available:http://www.iso.org/iso/home/store/catalogueics/,catalogue_detail_ics.htm?csnumber=50297, Accessed: 23/01/2015.

[48] Kuligowski, C. "Comparison of IT Security Standards", 2009, Available: www.federalcybersecurity.org, Accessed: 23/02/2016.

[49] Hommes, Q. V. E., Salim, H. andMadnick, S. "System Theoretic Approach To Cyber Security", 2015, Available: http://www.arcweb.com/events/arc-industry-forum-orlando/arcindustryforum 2015presentations/QVanEikemaHommes-MIT.pdf, Accessed 25/04/2015

[50] Leveson, N. G. "A Systems-Theoretic View of Causality, Engineering a Safer World: Systems Thinking Applied to Safety", Cambridge, The MIT Press, pp. 73-102, 2011.

[51] Leveson, N. G. "Questioning the Foundations of Traditional Safety Engineering, Engineering a Safer World: Systems Thinking Applied to Safety", Cambridge, MA: MIT Press, pp. 7-60, 2011.

[52] Salim, H. "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks", Dissertation for Master of Science in Engineering and Management, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, 2014.

[53] Garg, S. andAujla, G. S. "An Attack Tree Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic", *Journal Of Emerging Technologies In Web Intelligence*, Vol. 6, Number 2, 2014.

[54] Ibidunmoye, E. O., Alese, B. K. andOgundele, O. S. "Modeling Attacker-Defender Interaction as a Zero-Sum Stochastic Game", *Journal of Computer Sciences and Applications*, Vol. 1, Number 2, , pp 27-32, 2013.

[55] He, F., Zhuang, J. and Rao, N. S. V. "Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures", Industrial and Systems Engineering Research Conference, G. Lim and J.W. Herrmann, eds, 2012

[56] Gueye, A. "A Game Theoretical Approach to Communication Security", PhD Thesis, Electrical Engineering and Computer Sciences Department. University of California, Berkeley, 2011.

[57] Nguyen, K. C., Alpcan, T. andBasar, T. "Stochastic games for security in networks with interdependent nodes", International. Conference.on Game Theory for Networks, 2009, Available: https://ai2-s2-pdfs.s3.amazonaws.com/30f7/ee17b09ea9c31943ecb0d983f84ccd68df46.pdf, Accessed 15/07/2015

[58] Alpcan, T. and Pavel, L. "Nash equilibrium design and optimization", International Conference on Game Theory for Networks, 2009.

[59] Carin, L., Cybenko, G. and Hughes, J. "Quantitative evaluation of risk for investment efficient strategies in cyber-security: The queries methodology", IEEE Computer, 2008.

[60] Bloem, M., Alpcan, T. and Basar, T. "Intrusion response as a resource allocation problem", IEEE Conference on Decision and Control, 2006, Available: ieeexplore.ieee.org/iel5/4176992/4176993/04177356.pdf, Accessed 18/03/2014

[61] Liu, Y., Comaniciu, C. and Man, H. "A Bayesian game approach for intrusion detection in wireless ad hoc networks", ACM *International Conference*, Vol. 199. 2006,

[62] Liu, P., Zang, W. and Yu, M. "Incentive-based modeling and inference of attacker intent, objectives and strategies", ACM *Transactions on Information and System Security*, Vol. 8, Number 1, pp78–118, 2005.

[63] Jormakka, J. and Molsa, J. V. E. "Modeling information warfare as a game*", Journal of Information Warfare*, Vol. 4, Number 2, 2005.

[64] Patcha, A. and Park, J. "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks", IEEE workshop on Information Assurance and Security, 2004.

[65] Lye, K. and Wing, J. "Game strategies in network security, Proceedings of the Foundations of Computer Security", 2002, Available: www.cs.cmu.edu/~wing/publications/CMU-CS-02-136.pdf, Accessed: 6/08/2014

[66] Aigbokhaevbolo, O. "Application of Game Theory to Business Strategy in Undeveloped Countries: A Case for Nigeria", *Journal of Social Sciences*, Vol. 27, Number 1, pp1-5, 2011.

[67] Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T. and Hubaux, J. "Game Theory Meets Network Security and Privacy", EPFL Technical Report, EPFL-REPORT-151965, Available: http://publish.illinois.edu /science-of-security-lablet/files/2014/06/Game-Theory-Meets-Network-Security-and-Privacy.pdf, Accessed 23/06/2017.