ABSTRACT

Honeypots are computer systems that deceive cyber attackers into believing they are ordinary computer systems designed for invasion, when in fact they are primarily designed to collect data about attack methods, resulting in better protection and defense against malicious actors. As a result, developing reliability metrics for measuring the performance, strength, and effectiveness of honeypot deception is advantageous. Despite extensive and mature research on honeynet system, reliability modeling, analysis and performance prediction and evaluation, based on copula techniques for accurately testing, estimating and optimizing the overall performance of honeynet systems remain lacking. To start, a copula approach for analyzing and optimizing the performance of honeynet systems was proposed. Any honeynet system’s performance can be classified based on its availability, dependability and profit generated. As a result, the current paper sought to investigate the performance of a multi-state honeynet system in terms of availability, dependability and expected profit. This paper examines two types of repairs. Type I repairs are known as general repairs and they are used to recover from a partial or non-lethal failure to a perfect state, whereas Type II repairs are known as copula repairs they are used to recover from a complete or lethal failure to a perfect state. For the sake of generality, the supplementary variable technique and Laplace transforms were used to develop the performance models that are essential to this research, such as availability, reliability, mean time to failure (MTTF), sensitivity and profit function. The models’ numerical validation was fully carried out. The results are shown in tables and figures, enabling us to draw the conclusion that Type II repair is a superior repair policy. Type II repair, according to the findings, can more accurately portray system structure and states while still allowing for efficient assessment.

INTRODUCTION

In today’s technological and computerized world, the internet stands as an important system for both service providers and consumers. The accuracy and consistent availability of service are critical to a successful venture. As a result, it is critical for service providers to safeguard their servers against numerous cyber-attacks. Due to the use of network explosives in recent years, computer systems and the internet have raised numerous security concerns. Computer crime is constantly on the rise. Based on known facts, mitigation strategies are devised for safeguard and prevention of attacks. Security preventive and corrective measures range from keeping intruders away from a network or system, to protecting and preventing internet communication, to limiting the spread and serious harm caused by computer viruses.

A honeynet is a network that is designed to capture hackers by hosting deliberate vulnerabilities on a decoy server. The primary goal is to put network security to the test by inviting attacks. This method enables security experts to investigate a real attacker’s activities and strategies for enhancing network security. The penetration testing of intrusion detection system (IDS) has become a critical component of enterprises that prevents cybercriminal activity by protecting the network, resources and sensitive data. So far, several ways to thwarting harmful activity have been presented and implemented.

Albahar et al. (2020), Althubiti et al. (2018) and AlHamouz et al. (2017) an intrusion detection system (IDS) detects intrusions in two ways: signature-based IDS and anomaly-based IDS. Signature-based detection looks for a “signature” pattern or known attacks. This type of IDS requires regular updates to currently common signatures or signatures that do not exist in the database. Furthermore, the larger the databases, the more processing is required to analyse and verify each connection. In contrast to signature-based IDS, anomaly-based detection is used to detect known and unknown attacks based on learning their behaviour in a computer network by specifying observations that deviate from a basic model and informing the network’s administrator to take necessary actions. The ability to detect unknown attacks is the primary advantage of anomaly-based detection.

Many researchers have proposed various intrusion detection systems as a result of their importance. Among these systems, machine learning models, specifically neural networks, can effectively detect malicious network activity by being trained with enough intrusion detection recorded data. Non-neural network machine learning models, such as SVM, have limitations such as low repetition attack detection rates, detection instability, and training process complexity.

Auto encoders and variational auto encoders (VAEs) are two neural network models that have been used for anomaly detection. Auto encoders are made up of sequentially linked encoder and decoder networks. An encoder can compress the input data, and a decoder can reconstruct the input data. Auto encoders try to reduce reconstruction error (the difference between decoder output and original input). To detect anomalies, this error is used as an anomaly score. Small reconstruction errors are associated with normal data, whereas larger reconstruction errors are associated with anomalous data.

Related Work

Researchers have put in significant effort to developed methods of defending, protecting, and improving the honeypot’s security system. To cite few, Agrawal and Tapaswi (2017) proposed intrusion detection mechanism called honeypot intrusion detection system meant for detecting and preventing external and internal malicious users gaining access to wireless network. Kondra et al. (2016) developed an intrusion detection technique which will extract the details of the attacker. Naik et al. (2021) proposed method that allow honeypot to explore and estimate the malicious users’ fingerprint using fuzzy inference and principal components analysis. Parrathia et al. (2021) analyzes the technique of anti-identification thinking, signature, and the theoretical basis of game. Isa et al. (2023) explore on reliability analysis of computer network which comprises of three subsystems: router, workstation and hub. Yusuf et al. (2021) consider a distributed system with five standby subsystems A (the clients), B (two load balancers), C (two distributed database servers), D (two mirrored distributed database servers) and E (centralized database server) is considered arranged as series-parallel system. Kasongo and Sun (2020) created five supervised models using a filter-based information reduction method and compared their performance on the UNSW-NB 15 dataset, the UNSW-NB15 is a network intrusion dataset that contains nine different attacks, includes DoS, worms, Backdoors, and Fuzzers. The dataset contains raw network packets. Disha and Waheed (2022) proposed machine learning techniques for intrusion detection systems and analyzed model performance by training and testing the Long-Short Term Memory, Multilayer Perceptron, Decision Tree, Gradient Boosting Tree, AdaBoost and Gated Recurrent Unit for the binary classification task. Isa et al. (2021) investigate the performance measures of network with transparent bridge as follows 1-out-of-2: G, 2-out-of-3: F, a bridge unit and 3-out-of-5: G schemes.

Arqub and Hammour (2014) explore on continuous genetic algorithm as an efficient solver for systems of second-order boundary value problems where smooth solutions were used throughout the evolution of the algorithm to obtain the required nodal values of the unknown variables, Aydin et al. (2022) estimate the coliform values of the Tekkekoy deep sea discharge system, which is chosen as...
an application area, by using a radial-based artificial neural network structure, Sekerci and Aydin (2022) writes on production-distribution network system for a company, which is active in producing bottled natural spring water was established. In Kenan et al. (2021) classification algorithms were used to classify electromyography and depth sensor data. Tolga and Ali (2022) use artificial neural networks to predict the risk size of the BLEVE event. Bakar and Murat (2022) examine the net single premiums of multiple life annuities using stochastic rates of return and dynamic life table under the assumption of dependency of spouses’ future lifetimes. In pology, Adem (2023) introduces the concept of intuitionistic fuzzy hyper soft. Certain properties of intuitionistic fuzzy hyper soft (IFH) topology are investigated, including the IFH basis, IFH subspace, IFH interior, and IFH cloure. Arqul et al. (2021) use extended reproducing kernel Hilbert space technique toanalyse and numerically solve fuzzy fractional differential equations with Atangana-Baleanu-Caputo differential operators. Maryam et al. (2023) investigate codes over the direct product of two finite commutative chain rings. The parity-check matrix’s standard form is determined. Alazzam et al. (2020) examined the performance of IDS using a binary classifier called Decision Tree (DT). Belgrana et al. (2021) suggested a condensed nearest neighbors neural network to reduce feature dimensionality and computational time, as well as a radial basis function neural network to achieve performance learning on the network security laboratory-knowledge discovery in databases (NSL-KDD) dataset. Gu and Lu (2021) suggested an effective solution for intrusion detection that combines SVM with the NaveBayes algorithm to differentiate intrusion and normal cases. Lee et al. (2020) offered a hybrid technique in which the authors recommend a deep sparse auto encoder for feature selection in the data pre-processing step. Isa et al. (2022) Explore on reliability analysis of computer network which comprises of three subsystems: router, workstation and hub. Mauro et al. (2020) gave an experimental study for Network Intrusion Mitigation application of Neural Network methods. Arqub et al. (2014) publish an article on numerical approximation of solutions with Troesch’s and Bratu’s problems.

Kelly et al. (2020) emphasize the necessity of using publicly accessible vulnerability intelligence information and indicators of compromise obtained via honeypots to inform an organization’s Situational Awareness operations, using a similar methodology as in this paper. Sethia and Jeyasekar (2019) developed a honeypot as a security measure to protect an establishment from the detrimental and malicious acts of malwares by examining the honeypot’s network logs. Arqub et al. (2021) consider a numerical approach to solve groups of fuzzy fractional integrodifferentials (FFDIEs) with Atangana–Baleanu–Caputo (ABC) fractional distributed order derivatives. The solution-based approach lies in generating infinite orthogonal basis from kernel functions, where an uncertain condition is fulfilled.

Numerous studies in the field of reliability engineering have shown that effective performance analysis can help to avoid disasters, protection, safety and save time, money, or both. To cite few, Xie et al. (2021) investigated and examined the performance of a safety system that is vulnerable to cascading failures that cause the appearance of further failures. In the paper, a unique technique for mitigating and preventing cascading failure is provided. Xie et al. (2019) suggested performance and an approximation approach for medium-frequency hazardous failures in safety instrumental systems prone to cascade failures. Yusuf et al. (2020) analyzed the performance of computer system using copula linguistic. Colledani et al. (2019) offer a method for evaluating the performance of unstable manufacturing systems that takes into account unknown machine reliability predictions.

Reliability modeling or analysis and performance prediction and evaluation, based on copula techniques for accurately testing, estimating and optimizing the overall performance of honeynet systems remain lacking, copula technique is a powerful tool for describing variable dependence and has received much attention in a variety of fields of study. Numerous researchers have used the copula method to explore the performance of complex repairable systems and have reported improved operational performance. However, the issue of whether copula-based reliability, performance, strength, and effectiveness of the given honeynet system has not been thoroughly investigated. This motivates us to evaluate and investigate the honeypot’s availability and performance analysis using the gumbel hougaard family copula.

**DESCRIPTION AND NOTATION OF THE SYSTEM**

**Notations**

$q$: Variable representing time.
$s$: representing variable of Laplace transform
$m_1$: stand for rate of failure of unit in production subsystem
$m_2$: stand for rate of failure of honeypot in honeypot subsystem
$m_{11}$: stand for rate of failure of switch I
$m_{12}$: stand for rate of failure of switch II
$m_2$: stand for rate of failure of router
$m_3$: stand for rate of failure of honey sensor
$l_1(x)$: stand for rate of repair by general repair of unit in production subsystem
$l_2(y)$: stand for rate of repair by general repair of honeypot in honeypot subsystem
$\eta_1(x)$: stand for rate of repair by copula of unit in production subsystem
$\eta_2(y)$: stand for rate of repair by copula of honeypot in honeypot subsystem
$\eta_1(n)$: stand for rate of repair by copula of switch I
$\eta_2(z)$: stand for rate of repair by copula of switch II
$\eta_3(r)$: stand for rate of repair by copula of router
\( \eta_o(z) \): stand for rate of repair by copula of honey sensor 
\( H_i(t) \): stand for chance of the system sojourning in \( S_i \) state at instants for \( i = 0 \) to 14.

\( \bar{H}(s) \): stand for Laplace transformation of state transition probability \( H(t) \).

\( H_i(x, q) \): stand for chance of the system sojourning in \( S_i \) with \( x \) variable of repair and variable time \( q \).

\( P_i(y_2, t) \): stand for chance of the system sojourning in \( S_i \) with \( y_2 \) variable of repair variable \( y_1 \) and variable time \( t \).

\( P_i(y_3, t) \): stand for chance of the system sojourning in \( S_i \) with \( y_3 \) variable of repair variable \( y_1 \) and variable time \( t \).

\( P_i(y_4, t) \): stand for chance of the system sojourning in \( S_i \) with \( y_4 \) variable of repair variable \( y_1 \) and variable time \( t \).

\( P_i(y_5, t) \): stand for chance of the system sojourning in \( S_i \) with \( y_5 \) variable of repair variable \( y_1 \) and variable time \( t \).

\( E_p(t) \): Expected profit during the time interval \([0, t)\)

\( Z_1, Z_2 \): Revenue and service cost per unit time, respectively.

\( m_0(x) \): The expression of joint probability according to Gumbel-Hougaard family Copula definition is given as:

\[ c_\theta(u_1(x), u_2(x)) = \exp \left( x^\theta + \{ \log \phi(x) \}^\theta \right), 1 \leq \theta \leq \infty \]

Where \( \mu_1 = \phi(x) \) and \( u_2 = e_\chi \).

**System Description**

The diagram, depicted in Figure 1, portrays a Honeynet system that implements Gen III honeynet solution architecture. The system consists of system users that include an attacker on one side, accessing production systems network via the Internet, a router, a honeynet sensor called a honeywall gateway, a real service network of production systems (system-1, system-2 and system-3) and the network of honeypots with data capture capability (OS-1, OS-2 and OS-3).

The router typically implements a hidden firewall, which serves as first access control mechanism. The production system network applies a honeynet security technology. The honeynet implements a honeynet sensor which is the most important tool in the entire honeynet solution. The honeywall is a computer server that serves as a layer 2 gateway device to supervise outbound data and separate the honeynet from other production systems. The honeynet sensor supports interception of SSL connections and make decision about the incoming traffic into the system. It determines if the traffic is malicious and thus redirect it to a honeypots or it is valid and thus redirect it to the real production system. Ultimately, the honeynet sensor performs three essential functions, viz: data control, which involves controlling the flow of data so that the attacker does not realize being in the honeynet and ensuring that the honeynet system is not used to attack other systems in the event of system compromise; data capture, which involves capturing all the data regarding movements and actions within the honeynet; and data collection, which involves the ability to securely transfer all the captured data to a central database/log service, also implemented within the honeynet sensor. Furthermore, the honeypots are computer systems that duplicate and disguise themselves as real production systems in order to lure an attacker. The honeypots are controlled by the honeywall. They typically implements Sebek/Qebek monitoring tool. When the honeypots receive a malicious request from attacker, the systems invisibly monitor and capture

![Figure 1](image-url). Reliability block diagram of the honeynet system.
activities of the attacker in the honeypots and send the captured data to the central log in the honeynet sensor for analysis.

**HONEYNET MODEL FORMULATION**

The supplementary variable technique and Laplace transforms were used to create reliability models for honeynet system analysis. A probabilistic approach was used to generate the differential equations from the transition diagram above. These equations were then solved using initial and boundary conditions to obtain steady state probabilities, which serve as the basis for the development of reliability models.

The following partial differential equations are obtained via Figure 2:

\[
\left( \frac{\partial}{\partial q} + 3m_i + m_r + m_S + m_n + m_e \right) H_i(q) - \int_0^q f_i(x) H_i(x, q) dq \\
+ \int_0^q f_i(y) H_i(x, y) dq - \int_0^q f_i(z) H_i(x, z) dq + \int_0^q f_i(t) H_i(x, t) dq \\
+ \int_0^q f_i(x) H_i(x, q) dq + \int_0^q f_i(x) H_i(x, q) dq + \int_0^q f_i(h) H_i(h, q) dq \\
+ \int_0^q f_i(n) H_i(n, q) dq \\
= 0
\]

(1)

\[
\left( \frac{\partial}{\partial x} + \frac{\partial}{\partial q} + 2m_i + 3m_i + m_r + m_n + m_n + l_i(x) \right) H_i(x, q) = 0
\]

(2)

\[
\left( \frac{\partial}{\partial q} + m_i + m_n + m_r + l_i(x) \right) H_i(x, q) = 0
\]

(3)

**Figure 2.** Transition diagram of the honeynet system.
\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial y} + 3m_1 + 2m_2 + m_3 + m_\text{n} + m_\text{y} + l_\text{y}(y) \right\} H_\text{yy}(y, q) = 0 \quad (4)
\]

\[
H_1(0, q) = 3m_2 H_1(0, q) \quad (20)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial y} + m_1 + n_\text{y} + l_\text{y}(y) \right\} H_\text{y}(y, q) = 0 \quad (5)
\]

\[
H_6(0, q) = 2m_2 H_6(0, q) \quad (21)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial y} + 2m_2 + m_3 + m_\text{n} + l_\text{y}(y) \right\} H_\text{yy}(y, q) = 0 \quad (6)
\]

\[
H_7(0, q) = 3m_1 H_7(0, q) \quad (22)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial y} + m_2 + m_3 + m_\text{n} + l_\text{y}(y) \right\} H_\text{y}(y, q) = 0 \quad (7)
\]

\[
H_8(0, q) = 2m_2 H_8(0, q) \quad (23)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_1 + m_2 + m_3 + l_\text{x}(x) \right\} H_\text{x}(x, q) = 0 \quad (8)
\]

\[
H_9(0, q) = m_1 \left( H_2(0, q) + H_8(0, q) \right) \quad (24)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_2 + m_3 + m_\text{n} + l_\text{x}(x) \right\} H_\text{xx}(x, q) = 0 \quad (9)
\]

\[
H_{10}(0, q) = m_2 \left( H_4(0, q) + H_6(0, q) \right) \quad (25)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_3 + m_\text{n} + m_\text{y} + l_\text{x}(x) \right\} H_\text{yy}(y, q) = 0 \quad (10)
\]

\[
H_{11}(0, q) = m_2 \left( H_4(0, q) + H_6(0, q) \right) \quad (26)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_1 + m_2 + m_\text{n} + l_\text{x}(x) \right\} H_\text{xx}(x, q) = 0 \quad (11)
\]

\[
H_{12}(0, q) = m_2 \left( H_4(0, q) + H_6(0, q) \right) \quad (27)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_1 + m_2 + m_\text{n} + l_\text{x}(x) \right\} H_\text{yy}(y, q) = 0 \quad (12)
\]

\[
H_{13}(0, q) = m_2 \left( H_4(0, q) + H_6(0, q) \right) \quad (28)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_3 + m_\text{n} + m_\text{y} + l_\text{x}(x) \right\} H_\text{yy}(y, q) = 0 \quad (13)
\]

\[
H_{14}(0, q) = m_2 \left( H_4(0, q) + H_6(0, q) \right) \quad (29)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_1 + m_2 + m_\text{n} + l_\text{x}(x) \right\} H_\text{xx}(x, q) = 0 \quad (14)
\]

\[
\left\{ \frac{\partial}{\partial q} + \frac{\partial}{\partial x} + m_3 + m_\text{n} + m_\text{y} + l_\text{x}(x) \right\} H_\text{yy}(y, q) = 0 \quad (15)
\]

**Initial condition**

\[
H_1(0) = \begin{cases} 1, & t = 0 \\ 0, & t \neq 0 \end{cases}
\]

**MODEL’S SOLUTION**

The Laplace transformation of equations (1) to (29) with the help of initial condition to obtain:

\[
\left\{ s + 3m_1 + 2m_2 + m_3 + m_\text{n} + m_\text{y} \right\} \tilde{H}_1(s) = 1 + \int_0^\infty \tilde{H}_1(x) \tilde{H}_1(x,s) dx
\]

\[
\int_0^\infty \tilde{H}_1(x) dx dy + \int_0^\infty \tilde{H}_1(x) \tilde{H}_1(x,s) dr + \int_0^\infty \tilde{H}_1(y) \tilde{H}_1(y,s) dy
\]

\[
* \int_0^\infty \tilde{H}_1(r) dr + \int_0^\infty \tilde{H}_1(h) dr + \int_0^\infty \tilde{H}_1(n) \tilde{H}_1(n,s) dn
\]

\[
\tilde{H}_1(s) = \left\{ s + 3m_1 + 2m_2 + m_3 + m_\text{n} + m_\text{y} \right\} \tilde{H}_1(s) = 0
\]

\[
\left\{ s + m_1 + m_2 + m_3 + m_\text{n} + m_\text{y} + l_\text{x}(x) \right\} \tilde{H}_1(x, s) = 0
\]

\[
\left\{ s + m_1 + m_2 + m_3 + m_\text{n} + l_\text{x}(x) \right\} \tilde{H}_1(x, s) = 0
\]
\[
\begin{align*}
(s + \frac{\partial}{\partial y} + 3m_y + 2m_z + m_x + m_n + m_s + l_y(y))H_1(y,s) = 0 \quad (33) \\
(s + \frac{\partial}{\partial y} + m_z + m_x + m_s + l_y(y))H_2(y,s) = 0 \quad (34) \\
(s + \frac{\partial}{\partial y} + 2m_z + m_x + m_s + l_y(y))H_3(y,s) = 0 \quad (35) \\
(s + \frac{\partial}{\partial y} + m_z + m_x + m_s + l_y(y))H_4(y,s) = 0 \quad (36) \\
(s + \frac{\partial}{\partial x} + 2m_n + m_z + m_s + l_x(x))H_1(x,s) = 0 \quad (37) \\
(s + \frac{\partial}{\partial x} + m_n + m_z + m_s + l_x(x))H_2(x,s) = 0 \quad (38) \\
(s + \frac{\partial}{\partial x} + m_n + m_z + m_s + l_x(x))H_3(x,s) = 0 \quad (39) \\
(s + \frac{\partial}{\partial x} + m_n + m_z + m_s + l_x(x))H_4(x,s) = 0 \quad (40) \\
(s + \frac{\partial}{\partial r} + n_y(r))H_1(r,s) = 0 \quad (41) \\
(s + \frac{\partial}{\partial h} + n_y(h))H_2(h,s) = 0 \quad (42) \\
(s + \frac{\partial}{\partial n} + n_y(n))H_3(n,s) = 0 \quad (43) \\
(s + \frac{\partial}{\partial z} + n_y(z))H_4(z,s) = 0 \quad (44)
\end{align*}
\]

\[
H_1(0,s) = 3m_2H_1(0,s) \quad (49) \\
H_2(0,s) = 2m_2H_2(0,s) \quad (50) \\
H_3(0,s) = 3m_2H_3(0,s) \quad (51) \\
H_4(0,s) = 2m_2H_4(0,s) \quad (52)
\]

\[
\begin{align*}
H_0(0,s) &= m_2(H_3(0,s) + H_4(0,s)) \quad (53) \\
H_1(0,s) &= m_2(H_0(0,s) + H_3(0,s)) \quad (54) \\
H_0(0,s) &= m_2(H_0(0,s) + H_1(0,s) + H_3(0,s)) \quad (55) \\
H_0(0,s) &= m_2(H_0(0,s) + H_1(0,s) + H_2(0,s)) \quad (56)
\end{align*}
\]

**Condition of Initials**

\[H_1(0) = 1, \text{ but other state transition probability is 0 at this time.} \quad (59)\]

Therefore, we have the following solution.

\[
H_0(s) = \frac{1}{K(s)} \quad (60)
\]

\[
H_1(s) = \frac{3m_2}{K(s)} \left\{ 1 - \frac{5}{s + 2m_n + 3m_z + m_s + m_x + m_n} \right\} \quad (61)
\]

\[
H_2(s) = \frac{6m_2}{K(s)} \left\{ 1 - \frac{5}{s + m_n + m_x + m_n} \right\} \quad (62)
\]

\[
H_3(s) = \frac{3m_2}{K(s)} \left\{ 1 - \frac{5}{s + m_n + m_x + m_n} \right\} \quad (63)
\]

**Boundary conditions**

\[
\begin{align*}
H_1(0,s) &= 3m_2H_1(0,s) \quad (45) \\
H_2(0,s) &= 2m_2H_2(0,s) \quad (46) \\
H_3(0,s) &= 3m_2H_3(0,s) \quad (47) \\
H_4(0,s) &= 2m_2H_4(0,s) \quad (48)
\end{align*}
\]
However, $K(s)$ is:

$$K(s) = \left\{ \begin{array}{l}
(53)
(54)
\end{array} \right.$$  

The sum of Laplace transformed state transition probabilities that the system is working are as follows:

$$\bar{H}_w(s) = \left[ \bar{H}_1(s) + \bar{H}_1(s) + \bar{H}_1(s) + \bar{H}_1(s) + \bar{H}_1(s) \right]$$  

Table 1. Availability analysis of the system

<table>
<thead>
<tr>
<th>q</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>1.0000</td>
<td>0.9832</td>
<td>0.9816</td>
<td>0.9795</td>
<td>0.9771</td>
<td>0.9744</td>
<td>0.9717</td>
<td>0.9691</td>
<td>0.9664</td>
<td>0.9637</td>
<td>0.9610</td>
</tr>
</tbody>
</table>

When time (t) is use as $q = 0, 1, ..., 10$ in equation (79), Table 1 obtained
If \( l, n \) are declared to be zero and values of failure rate as follows:

\[
\begin{align*}
    m_1 &= 0.011, \\
    m_2 &= 0.012, \\
    m_r &= 0.013, \\
    m_h &= 0.014, \\
    m_{s_1} &= 0.015, \\
    m_{s_1} &= 0.016.
\end{align*}
\]

Then we have,

\[
\text{Rel}(q) = \left\{ 3e^{-0.011q} + 0.008884e^{-0.012q} + 0.00606e^{-0.013q} + 0.001926e^{-0.014q} \right\} (80)
\]

For \( q = 0, 1...10 \) in equation (80),

**Mean Time to Failure (MTTF)**

Assuming all repairs to zero while \( s \) tends zero in equation (77), MTTF expression is obtained as:

\[
\text{MTTF} = \lim_{s \to 0} \frac{1}{s + 2m_1 + 2m_2 + 2m_r + 2m_h + 2m_{s_1} + 2m_{s_1}}
\]

**Table 2. Reliability analysis of the system**

<table>
<thead>
<tr>
<th>q</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>1.0000</td>
<td>0.9455</td>
<td>0.8907</td>
<td>0.8363</td>
<td>0.7830</td>
<td>0.7311</td>
<td>0.6811</td>
<td>0.6332</td>
<td>0.5875</td>
<td>0.5442</td>
<td>0.5032</td>
</tr>
</tbody>
</table>

**Figure 3.** Honeynet availability analysis.

**Figure 4.** Honeynet Reliability Analysis.
Assuming $m_1 = 0.011$, $m_2 = 0.012$, $m_r = 0.013$, $m_h = 0.014$, $m_1 = 0.015$, $m_2 = 0.016$ and varying the required failure rate as 0.001, 0.002...0.009 in equation (81) while others kept constant Table 3 below is obtained.

### Table 3. MTTF of the system

<table>
<thead>
<tr>
<th>Failure Rate</th>
<th>$MTTF m_1$ (a)</th>
<th>$MTTF m_2$ (b)</th>
<th>$MTTF m_r$ (c)</th>
<th>$MTTF m_h$ (d)</th>
<th>$MTTF m_1$ (e)</th>
<th>$MTTF m_2$ (f)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.001</td>
<td>4.4962</td>
<td>15.4494</td>
<td>15.2130</td>
<td>15.4035</td>
<td>15.9030</td>
<td>16.1377</td>
</tr>
<tr>
<td>0.002</td>
<td>4.5353</td>
<td>15.2001</td>
<td>15.0268</td>
<td>15.2130</td>
<td>15.6754</td>
<td>15.9030</td>
</tr>
<tr>
<td>0.003</td>
<td>4.5692</td>
<td>14.9628</td>
<td>14.8449</td>
<td>15.0268</td>
<td>15.4546</td>
<td>15.6754</td>
</tr>
<tr>
<td>0.004</td>
<td>4.5987</td>
<td>14.7365</td>
<td>14.6670</td>
<td>14.8449</td>
<td>15.2403</td>
<td>15.4546</td>
</tr>
<tr>
<td>0.005</td>
<td>4.6246</td>
<td>14.5202</td>
<td>14.4931</td>
<td>14.6670</td>
<td>15.0321</td>
<td>15.2403</td>
</tr>
</tbody>
</table>

### Figure 5. Honeynet MTTF Analysis.

**Sensitivity Analysis**

The computation of sensitivity MTTF is studied through the partial differentiation of MTTF with respect to the failure rates $m_1 = 0.011$, $m_2 = 0.012$, $m_r = 0.013$, $m_h = 0.014$, $m_1 = 0.015$, and $m_2 = 0.016$.

### Table 4. Sensitivity analysis of the system.

<table>
<thead>
<tr>
<th>Failure Rate</th>
<th>$\frac{\partial (MTTF)}{m_1}$ (I)</th>
<th>$\frac{\partial (MTTF)}{m_2}$ (II)</th>
<th>$\frac{\partial (MTTF)}{m_r}$ (III)</th>
<th>$\frac{\partial (MTTF)}{m_h}$ (IV)</th>
<th>$\frac{\partial (MTTF)}{m_1}$ (V)</th>
<th>$\frac{\partial (MTTF)}{m_2}$ (VI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.001</td>
<td>42.0655</td>
<td>-255.6961</td>
<td>-188.3255</td>
<td>-192.7575</td>
<td>-231.0825</td>
<td>-238.4650</td>
</tr>
<tr>
<td>0.002</td>
<td>36.3253</td>
<td>-243.1247</td>
<td>-184.0386</td>
<td>-188.3255</td>
<td>-224.1070</td>
<td>-231.0825</td>
</tr>
<tr>
<td>0.003</td>
<td>31.5751</td>
<td>-231.6505</td>
<td>-179.8908</td>
<td>-184.0386</td>
<td>-217.5019</td>
<td>-224.1070</td>
</tr>
<tr>
<td>0.004</td>
<td>27.6088</td>
<td>-221.1508</td>
<td>-175.8762</td>
<td>-179.8908</td>
<td>-211.2352</td>
<td>-217.5019</td>
</tr>
<tr>
<td>0.005</td>
<td>24.2705</td>
<td>-211.5148</td>
<td>-171.9893</td>
<td>-175.8762</td>
<td>-205.2790</td>
<td>-211.2352</td>
</tr>
<tr>
<td>0.007</td>
<td>19.0249</td>
<td>-194.4527</td>
<td>-164.5782</td>
<td>-168.2250</td>
<td>-194.2023</td>
<td>-199.6086</td>
</tr>
<tr>
<td>0.008</td>
<td>16.9513</td>
<td>-186.8651</td>
<td>-161.0443</td>
<td>-164.5782</td>
<td>-189.0406</td>
<td>-194.2023</td>
</tr>
<tr>
<td>0.009</td>
<td>15.1615</td>
<td>-179.8160</td>
<td>-157.6187</td>
<td>-161.0443</td>
<td>-184.1061</td>
<td>-189.0406</td>
</tr>
</tbody>
</table>
Table 5. Profit of the system

<table>
<thead>
<tr>
<th>q</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$D_2 = 0.1$</td>
<td>$D_2 = 0.2$</td>
<td>$D_2 = 0.3$</td>
<td>$D_2 = 0.4$</td>
<td>$D_2 = 0.5$</td>
<td>$D_2 = 0.6$</td>
</tr>
<tr>
<td>0</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>1</td>
<td>0.8878</td>
<td>0.7878</td>
<td>0.6878</td>
<td>0.5878</td>
<td>0.4878</td>
<td>0.3878</td>
</tr>
<tr>
<td>2</td>
<td>1.7702</td>
<td>1.5702</td>
<td>1.3702</td>
<td>1.1702</td>
<td>0.9702</td>
<td>0.7702</td>
</tr>
<tr>
<td>3</td>
<td>2.6509</td>
<td>2.3509</td>
<td>2.0509</td>
<td>1.7509</td>
<td>1.4509</td>
<td>1.1509</td>
</tr>
<tr>
<td>4</td>
<td>3.5293</td>
<td>3.1293</td>
<td>2.7293</td>
<td>2.3293</td>
<td>1.9293</td>
<td>1.5293</td>
</tr>
<tr>
<td>5</td>
<td>4.4051</td>
<td>3.9051</td>
<td>3.4051</td>
<td>2.9051</td>
<td>2.4051</td>
<td>1.9051</td>
</tr>
<tr>
<td>6</td>
<td>5.2782</td>
<td>4.6782</td>
<td>4.0782</td>
<td>3.4782</td>
<td>2.8782</td>
<td>2.2782</td>
</tr>
<tr>
<td>7</td>
<td>6.1487</td>
<td>5.4487</td>
<td>4.7487</td>
<td>4.0487</td>
<td>3.3487</td>
<td>2.6487</td>
</tr>
<tr>
<td>8</td>
<td>7.0164</td>
<td>6.2164</td>
<td>5.4164</td>
<td>4.6164</td>
<td>3.8164</td>
<td>3.0164</td>
</tr>
<tr>
<td>9</td>
<td>7.8815</td>
<td>6.9815</td>
<td>6.0815</td>
<td>5.1815</td>
<td>4.2815</td>
<td>3.3815</td>
</tr>
<tr>
<td>10</td>
<td>8.7439</td>
<td>7.7439</td>
<td>6.7439</td>
<td>5.7439</td>
<td>4.7439</td>
<td>3.7439</td>
</tr>
</tbody>
</table>

Figure 6. Honeynet Profit Analysis.

Table 6. Profit of the system

<table>
<thead>
<tr>
<th>q</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
<th>$E_p(q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$D_1 = 2$</td>
<td>$D_1 = 4$</td>
<td>$D_1 = 6$</td>
<td>$D_1 = 8$</td>
<td>$D_1 = 10$</td>
<td>$D_1 = 12$</td>
</tr>
<tr>
<td>0</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>1</td>
<td>0.9757</td>
<td>2.9514</td>
<td>4.9272</td>
<td>6.9029</td>
<td>8.8787</td>
<td>10.8544</td>
</tr>
<tr>
<td>2</td>
<td>1.9405</td>
<td>5.8811</td>
<td>9.8217</td>
<td>13.7622</td>
<td>17.7028</td>
<td>21.6434</td>
</tr>
<tr>
<td>3</td>
<td>2.9019</td>
<td>8.8038</td>
<td>14.7057</td>
<td>20.6076</td>
<td>26.5095</td>
<td>32.4114</td>
</tr>
<tr>
<td>4</td>
<td>3.8586</td>
<td>11.7172</td>
<td>19.5759</td>
<td>27.4345</td>
<td>35.2932</td>
<td>43.1518</td>
</tr>
<tr>
<td>5</td>
<td>4.8102</td>
<td>14.6204</td>
<td>24.4307</td>
<td>34.2409</td>
<td>44.0512</td>
<td>53.8614</td>
</tr>
<tr>
<td>6</td>
<td>5.7565</td>
<td>17.5130</td>
<td>29.2695</td>
<td>41.0260</td>
<td>52.7825</td>
<td>64.3590</td>
</tr>
<tr>
<td>7</td>
<td>6.6974</td>
<td>20.3948</td>
<td>34.0922</td>
<td>47.7896</td>
<td>61.4870</td>
<td>75.1844</td>
</tr>
<tr>
<td>8</td>
<td>7.6329</td>
<td>23.2658</td>
<td>38.8987</td>
<td>54.5331</td>
<td>70.1646</td>
<td>85.7975</td>
</tr>
<tr>
<td>9</td>
<td>8.5630</td>
<td>26.1261</td>
<td>43.6892</td>
<td>61.2522</td>
<td>78.8153</td>
<td>96.3784</td>
</tr>
<tr>
<td>10</td>
<td>9.4878</td>
<td>28.9757</td>
<td>48.4636</td>
<td>67.9514</td>
<td>87.4393</td>
<td>106.9272</td>
</tr>
</tbody>
</table>
Sensitivity. In another dimension, the average time to system failure (MTTF) were analyzed based on different failure rate by varying it from 0.001, ..., 0.009 fixing.

MTTF decreases with increase in failure rate in all the cases, MTTF Sensitivity was checked in this article to determine how the system was sensitive to the change in parameter and was identified that as the failure rate increases seems to be decreasing. Cost analysis on the other hand have been investigated on the service cost from (0.0) through (10) for the honeypot system throughout the findings it was observed that cost in terms of fixed revenue it happens that cost increases with time, also if the service is fixed the cost increases. To this fact, the honeypot system require optimal maintenance action in order to avoid huge downfall and adequate the life span of the network.

CONCLUSION

In this research, the honeypot sensor supports interception of SSL connections and make decision about the incoming traffic into the system. It determines if the traffic is malicious and thus redirect it to a honeypots or it is valid and thus redirect it to the real production system. Ultimately, the honeypot sensor performs three essential functions, viz: data control, which involves controlling the flow of data so that the attacker does not realize being in the honeypot and ensuring that the honeypot system is not used to attack other systems in the event of system compromise; data capture, which involves capturing all the data regarding movements and actions within the honeypot; and data collection, which involves the ability to securely transfer all the captured data to a central database/log service, also implemented within the honeypot sensor. Furthermore, the honeypots are computer systems that duplicate and disguise themselves as real production systems in order to lure
an attacker. The honeypots are controlled by the honeywall. They typically implement Sebek/Qebek monitoring tool. When the honeypots receive a malicious request from attacker, the systems invisibly monitor and capture activities of the attacker in the honeypots and send the captured data to the central log in the honeynet sensor for analysis, this implies that the availability of all the honeypot need to be checked and protected at all cost. Despite extensive and mature research on honeynet system, reliability modeling, analysis, and performance prediction and evaluation, copula-based techniques for accurately testing, estimating and optimizing the overall performance of honeynet systems remain lacking.

The research work presented will help plant management to shun away an erroneous performance assessment caused by poor system design. Failure occurrence, monitoring of condition can be extended and incorporated to allow management in approving the optimal replacement/maintenance time.

ACKNOWLEDGEMENT

This research is supported by the National Social Science Foundation of China (Grant No. 20BTJ044) and the Provincial Natural Science Foundation of Hunan Grant (Grant No. 2024JJ5453).

AUTHORSHIP CONTRIBUTIONS

Muhammad Salihu Isa initiate the model and do all the writing and mathematical analysis while Jinbiao Wu and Ibrahim Yusuf helps in editing and supervision.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES


[21] AlHamouz S, Abu-Shareha A. Hybrid Classification Approach Using Self-Organizing Map and Back Propagation Artificial Neural Networks for Intrusion Detection. In: 10th International Conference on Developments in eSystems Engineering (DeSE); 2017. [CrossRef]


