Sigma J Eng Nat Sci, Vol. 42, No. 4, pp. 1169−1182, August, 2024

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2024.00095

Research Article

Performance estimation of honeynet system for network security enhancement via copula linguistic

Muhammad SALIHU ISA[1,2], Jinbiao WU[1,*], Ibrahim YUSUF[3]

[1]*School of Mathematics and Statistics, Central South University, Changsha 410083, China*
[2]*Department of Mathematics, Yusuf Maitama Sule University, Kano, 700282, Nigeria*
[3]*Department of Mathematical Sciences, Bayero University, Kano, 700006, Nigeria*

ARTICLE INFO

Article history
Received: 31 January 2023
Revised: 18 April 2023
Accepted: 04 April 2023

Keywords:
Cyber; Honeynet; Intrusion detection system (IDS); Network; Security

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.

Cite this article as: Salihu Isa M, Wu J, Yusuf I. Performance estimation of honeynet system for network security enhancement via copula linguistic. Sigma J Eng Nat Sci 2024;42(4):1169−1182.

***Corresponding author.**
*E-mail address: wujinbiao@csu.edu.cn

This paper was recommended for publication in revised form by Editor in Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

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 of any 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 identities to ensure that the intruders' database is up to date. However, attackers can change minor details in signatures so that databases do not recognize them. As a result, a new attack type may not be detected because the signature does 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. Paryathia 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 serves) 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 solution curves 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 to analyse 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 Nave Bayes algorithm to differentiate intrusion and normal cases. Lee et al. (2020) offered a hybrid technique in which the authors recommended 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 (FFIDEs) 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_{s1}: stand for rate of failure of switch I

m_{s2}: stand for rate of failure of switch II

m_r: stand for rate of failure of router

m_h: 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

$\eta_o(x)$: stand for rate of repair by copula of unit in production subsystem

$\eta_o(y)$: stand for rate of repair by copula of honeypot in honeypot subsystem

$\eta_o(n)$: stand for rate of repair by copula of switch I

$\eta_o(z)$: stand for rate of repair by copula of switch II

$\eta_o(r)$: 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: $c_\theta(u_1(x), u_2(x)) = exp\left(x^\theta + \{log\,\phi\,(x)^\theta\}^{\frac{1}{\theta}}\right)$, $1 \le \theta \le \infty$. Where $\mu_1 = \phi(x)$ and $u_2 = e_x$.

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 honeyewall 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 tranfer 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

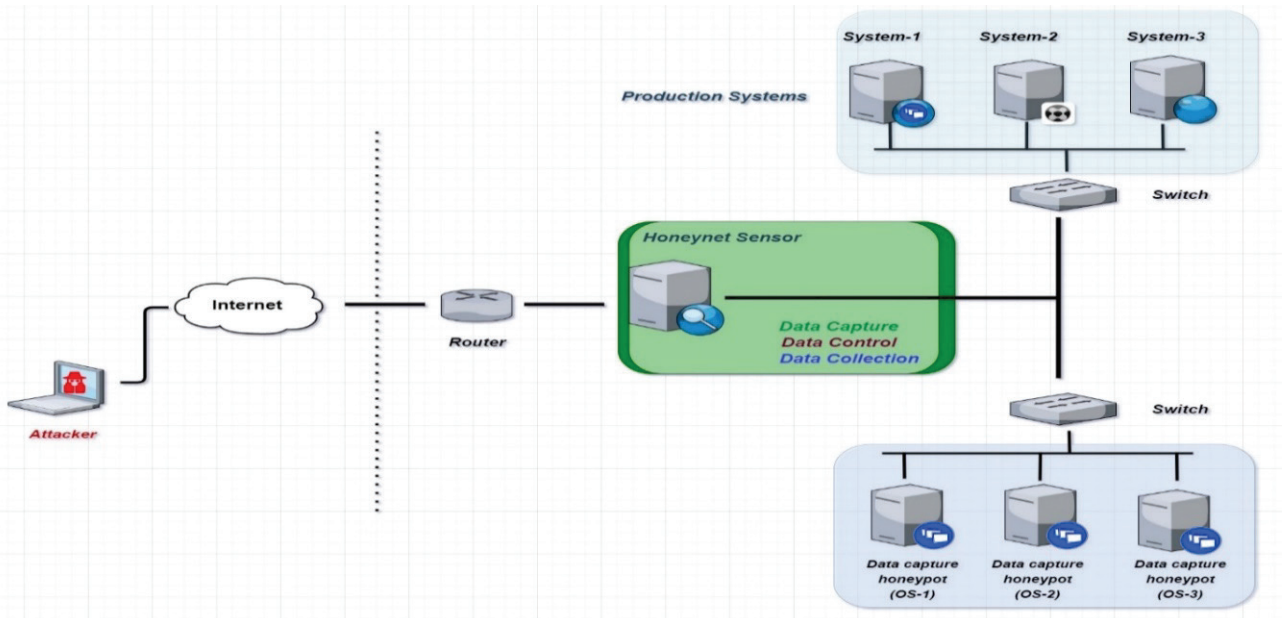

Figure 1. Reliability block diagram of the honeynet system.

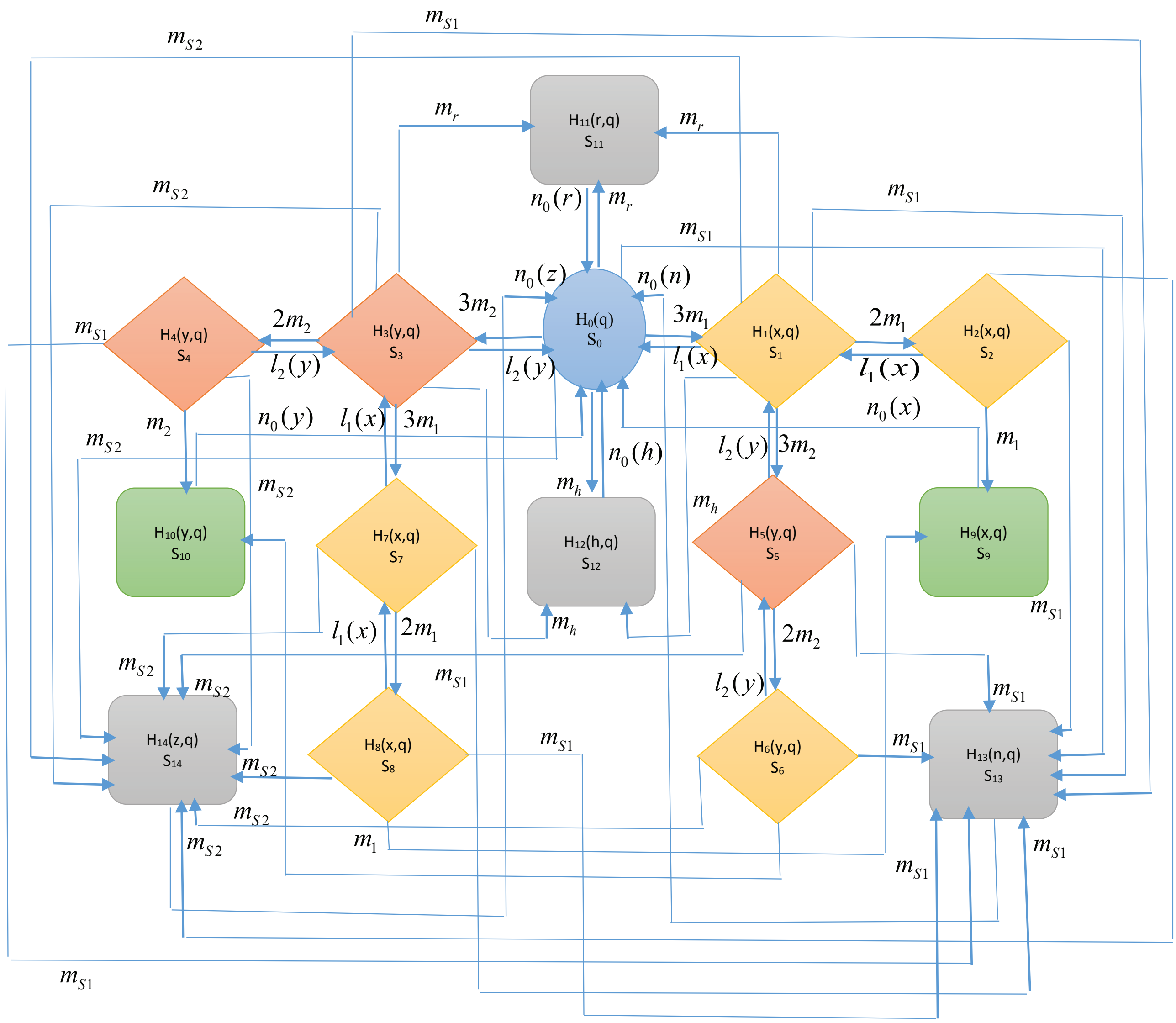

Figure 2. Transition diagram of the honeynet system.

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:

$$\left(\frac{\partial}{\partial q}+3m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)H_0(q)=\int_0^\infty l_1(x)H_1(x,q)dq+\int_0^\infty l_2(y)H_3(y,q)dq+\int_0^\infty n_0(z)H_{14}(z,q)dq+\int_0^\infty n_0(x)H_9(x,q)dq+\int_0^\infty n_0(y)H_{10}(y,q)dq+\int_0^\infty n_0(r)H_{11}(r,q)dq+\int_0^\infty n_0(h)H_{12}(h,q)dq+\int_0^\infty n_0(n)H_{13}(n,q)dq \tag{1}$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial x}+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}+l_1(x)\right)H_1(x,q)=0 \tag{2}$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial x}+m_1+m_{s_1}+m_{s_2}+l_1(x)\right)H_2(x,q)=0 \tag{3}$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial y}+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}+l_2(y)\right)H_3(y,q)=0 \quad (4)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial y}+m_2+m_{s_1}+m_{s_2}+l_2(y)\right)H_4(y,q)=0 \quad (5)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial y}+2m_2+m_{s_1}+m_{s_2}+l_2(y)\right)H_5(y,q)=0 \quad (6)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial y}+m_2+m_{s_1}+m_{s_2}+l_2(y)\right)H_6(y,q)=0 \quad (7)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial x}+2m_1+m_{s_1}+m_{s_2}+l_1(x)\right)H_7(x,q)=0 \quad (8)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial x}+m_1+m_{s_1}+m_{s_2}+l_1(x)\right)H_8(x,q)=0 \quad (9)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial x}+n_0(x)\right)H_9(x,q)=0 \quad (10)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial y}+n_0(y)\right)H_{10}(y,q)=0 \quad (11)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial r}+n_0(r)\right)H_{11}(r,q)=0 \quad (12)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial h}+n_0(h)\right)H_{12}(h,q)=0 \quad (13)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial n}+n_0(n)\right)H_{13}(n,q)=0 \quad (14)$$

$$\left(\frac{\partial}{\partial q}+\frac{\partial}{\partial z}+n_0(z)\right)H_{14}(z,q)=0 \quad (15)$$

Boundary conditions

$$H_1(0,q)=3m_1H_0(q) \quad (16)$$

$$H_2(0,q)=2m_1H_1(0,q) \quad (17)$$

$$H_3(0,q)=3m_2H_1(q) \quad (18)$$

$$H_4(0,q)=2m_2H_3(0,q) \quad (19)$$

$$H_5(0,q)=3m_2H_1(0,q) \quad (20)$$

$$H_6(0,q)=2m_2H_5(0,q) \quad (21)$$

$$H_7(0,q)=3m_1H_3(0,q) \quad (22)$$

$$H_8(0,q)=2m_1H_7(0,q) \quad (23)$$

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

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

$$H_{11}(0,q)=m_r\left(H_0(q)+H_1(0,q)+H_3(0,q)\right) \quad (26)$$

$$H_{12}(0,q)=m_h\left(H_0(q)+H_1(0,q)+H_3(0,q)\right) \quad (27)$$

$$H_{13}(0,q)=m_{s_1}\begin{pmatrix}H_0(q)+H_1(0,q)+H_2(0,q)+H_3(0,q)+H_4(0,q)\\ +H_5(0,q)+H_6(0,q)+H_7(0,q)+H_8(0,q)\end{pmatrix} \quad (28)$$

$$H_{14}(0,q)=m_{s_2}\begin{pmatrix}H_0(q)+H_1(0,q)+H_2(0,q)+H_3(0,q)+H_4(0,q)\\ +H_5(0,q)+H_6(0,q)+H_7(0,q)+H_8(0,q)\end{pmatrix} \quad (29)$$

Initial condition

$$H_t(0)=\begin{cases}1, & t=0\\ 0, & t\neq 0\end{cases}$$

MODEL'S SOLUTION

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

$$\begin{aligned}&\left(s+3m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)\overline{H}_0(s)=1+\int_0^\infty l_1(x)\overline{H}_1(x,s)dx\\&+\int_0^\infty l_2(y)\overline{H}_3(y,s)dy+\int_0^\infty n_0(x)\overline{H}_9(x,s)dr+\int_0^\infty n_0(y)\overline{H}_{10}(y,s)dy\\&+\int_0^\infty n_0(r)\overline{H}_{11}(r,s)dr+\int_0^\infty n_0(h)\overline{H}_{12}(h,s)dr+\int_0^\infty n_0(n)\overline{H}_{13}(n,s)dn\\&+\int_0^\infty n_0(z)\overline{H}_{14}(z,s)dz\end{aligned} \quad (30)$$

$$\left(s+\frac{\partial}{\partial x}+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}+l_1(x)\right)\overline{H}_1(x,s)=0 \quad (31)$$

$$\left(s+\frac{\partial}{\partial x}+m_1+m_{s_1}+m_{s_2}+l_1(x)\right)\overline{H}_2(x,s)=0 \quad (32)$$

$$\left(s+\frac{\partial}{\partial y}+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}+l_2(y)\right)\overline{H}_3(y,s)=0 \quad (33)$$

$$\left(s+\frac{\partial}{\partial y}+m_2+m_{s_1}+m_{s_2}+l_2(y)\right)\overline{H}_4(y,s)=0 \quad (34)$$

$$\left(s+\frac{\partial}{\partial y}+2m_2+m_{s_1}+m_{s_2}+l_2(y)\right)\overline{H}_5(y,s)=0 \quad (35)$$

$$\left(s+\frac{\partial}{\partial y}+m_2+m_{s_1}+m_{s_2}+l_2(y)\right)\overline{H}_6(y,s)=0 \quad (36)$$

$$\left(s+\frac{\partial}{\partial x}+2m_1+m_{s_1}+m_{s_2}+l_1(x)\right)\overline{H}_7(x,s)=0 \quad (37)$$

$$\left(s+\frac{\partial}{\partial x}+m_1+m_{s_1}+m_{s_2}+l_1(x)\right)\overline{H}_8(x,s)=0 \quad (38)$$

$$\left(s+\frac{\partial}{\partial x}+n_0(x)\right)\overline{H}_9(x,s)=0 \quad (39)$$

$$\left(s+\frac{\partial}{\partial y}+n_0(y)\right)\overline{H}_{10}(y,s)=0 \quad (40)$$

$$\left(s+\frac{\partial}{\partial r}+n_0(r)\right)\overline{H}_{11}(r,s)=0 \quad (41)$$

$$\left(s+\frac{\partial}{\partial h}+n_0(h)\right)\overline{H}_{12}(h,s)=0 \quad (42)$$

$$\left(s+\frac{\partial}{\partial n}+n_0(n)\right)\overline{H}_{13}(n,s)=0 \quad (43)$$

$$\left(s+\frac{\partial}{\partial z}+n_0(z)\right)\overline{H}_{14}(z,s)=0 \quad (44)$$

Boundary conditions

$$\overline{H}_1(0,s)=3m_1\overline{H}_0(s) \quad (45)$$

$$\overline{H}_2(0,s)=2m_1\overline{H}_1(0,s) \quad (46)$$

$$\overline{H}_3(0,s)=3m_2\overline{H}_0(s) \quad (47)$$

$$\overline{H}_4(0,s)=2m_2\overline{H}_3(0,s) \quad (48)$$

$$\overline{H}_5(0,s)=3m_2\overline{H}_1(0,s) \quad (49)$$

$$\overline{H}_6(0,s)=2m_2\overline{H}_5(0,s) \quad (50)$$

$$\overline{H}_7(0,s)=3m_1\overline{H}_3(0,s) \quad (51)$$

$$\overline{H}_8(0,s)=2m_1\overline{H}_7(0,s) \quad (52)$$

$$\overline{H}_9(0,s)=m_1\left(\overline{H}_2(0,s)+\overline{H}_8(0,s)\right) \quad (53)$$

$$\overline{H}_{10}(0,s)=m_2\left(\overline{H}_4(0,s)+\overline{H}_6(0,s)\right) \quad (54)$$

$$\overline{H}_{11}(0,s)=m_r\left(\overline{H}_0(s)+\overline{H}_1(0,s)+\overline{H}_3(0,s)\right) \quad (55)$$

$$\overline{H}_{12}(0,s)=m_h\left(\overline{H}_0(s)+\overline{H}_1(0,s)+\overline{H}_3(0,s)\right) \quad (56)$$

$$\overline{H}_{13}(0,s)=m_{s_1}\begin{pmatrix}\overline{H}_0(s)+\overline{H}_1(0,s)+\overline{H}_2(0,s)+\overline{H}_3(0,s)+\overline{H}_4(0,s)\\+\overline{H}_5(0,s)+\overline{H}_6(0,s)+\overline{H}_7(0,s)+\overline{H}_8(0,s)\end{pmatrix} \quad (57)$$

$$\overline{H}_{14}(0,s)=m_{s_2}\begin{pmatrix}\overline{H}_0(s)+\overline{H}_1(0,s)+\overline{H}_2(0,s)+\overline{H}_3(0,s)+\overline{H}_4(0,s)\\+\overline{H}_5(0,s)+\overline{H}_6(0,s)+\overline{H}_7(0,s)+\overline{H}_8(0,s)\end{pmatrix} \quad (58)$$

Condition of Initials

$H_0(0)=1$, but other state transition probability is 0 at this time. (59)

Therefore, we have the following solution.

$$\overline{H}_0(s)=\frac{1}{K(s)} \quad (60)$$

$$\overline{H}_1(s)=\frac{3m_1}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)}{s+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}}\right\} \quad (61)$$

$$\overline{H}_2(s)=\frac{6m_1^2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+m_1+m_{s_1}+m_{s_2}\right)}{s+m_1+m_{s_1}+m_{s_2}}\right\} \quad (62)$$

$$\overline{H}_3(s)=\frac{3m_2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)}{s+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}}\right\} \quad (63)$$

$$\overline{H}_4(s)=\frac{6m_2^2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+m_2+m_{s_1}+m_{s_2}\right)}{s+m_2+m_{s_1}+m_{s_2}}\right\} \quad (64)$$

$$\overline{H}_5(s)=\frac{9m_1m_2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+2m_2+m_{s_1}+m_{s_2}\right)}{s+2m_2+m_{s_1}+m_{s_2}}\right\} \tag{65}$$

$$\overline{H}_6(s)=\frac{18m_1m_2^2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+m_2+m_{s_1}+m_{s_2}\right)}{s+m_2+m_{s_1}+m_{s_2}}\right\} \tag{66}$$

$$\overline{H}_7(s)=\frac{9m_1m_2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+2m_1+m_{s_1}+m_{s_2}\right)}{s+2m_1+m_{s_1}+m_{s_2}}\right\} \tag{67}$$

$$\overline{H}_8(s)=\frac{18m_1^2m_2}{K(s)}\left\{\frac{1-\bar{s}_l\left(s+m_1+m_{s_1}+m_{s_2}\right)}{s+m_1+m_{s_1}+m_{s_2}}\right\} \tag{68}$$

$$\overline{H}_9(s)=\left(\frac{6\xi_1^3+18m_1^3m_2}{K(s)}\right)\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{69}$$

$$\overline{H}_{10}(s)=\left(\frac{6\xi_2^3+18m_2^3m_1}{K(s)}\right)\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{70}$$

$$\overline{H}_{11}(s)=\left(\frac{m_r+3m_1m_r+3m_2m_r}{K(s)}\right)\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{71}$$

$$\overline{H}_{12}(s)=\left(\frac{m_h+3m_1m_h+3m_2m_h}{K(s)}\right)\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{72}$$

$$\overline{H}_{13}(s)=\frac{1}{K(s)}\begin{pmatrix}m_{s_1}+3m_1m_{s_1}+3m_1^2m_{s_1}+3m_2m_{s_1}+6m_2^2m_{s_1}+9m_1m_2m_{s_1}\\+18m_1m_2^2m_{s_1}+9m_1m_2m_{s_1}+18m_1^2m_2m_{s_1}\end{pmatrix}\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{73}$$

$$\overline{H}_{14}(s)=\frac{1}{K(s)}\left\{\begin{matrix}m_{s_2}+3m_1m_{s_2}+3m_1^2m_{s_2}+3m_2m_{s_2}+9m_1m_2m_{s_2}\\6m_2^2m_{s_2}+9m_1m_2m_{s_2}+18m_1m_2^2m_{s_2}+18m_1^2m_2m_{s_2}\end{matrix}\right\}\left\{\frac{1-\bar{s}_{n0}(s)}{s}\right\} \tag{74}$$

However, K(s) is;

$$K(s)=\left\{\begin{pmatrix}s+3m_1+3m_2+\\m_r+m_h+m_{s_1}+m_{s_2}\end{pmatrix}-\left(\Delta_0+\left[\Delta_1+\Delta_2+\Delta_3\right]\bar{s}_{n0}(s)\right)\right\} \tag{75}$$

Where

$$\Delta_0=\left\{3m_1\bar{s}_l\left(s+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)+3m_2\bar{s}_l\left(s+3m_1+m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)\right\},$$
$$\Delta_1=\left\{\left(6m_1^3+18m_1^3m_2\right)+\left(6m_2^3+18m_2^3m_1\right)+\left(m_r+3m_1m_r+3m_2m_r\right)+\left(m_h+3m_1m_h+3m_2m_h\right)\right\},$$
$$\Delta_2=\left\{m_{s_1}+3m_1m_{s_1}+3m_1^2m_{s_1}+3m_2m_{s_1}+6m_2^2m_{s_1}+9m_1m_2m_{s_1}+18m_1m_2^2m_{s_1}+9m_1m_2m_{s_1}+18m_1^2m_2m_{s_1}\right\}$$
and
$$\Delta_3=\left\{m_{s_2}+3m_1m_{s_2}+3m_1^2m_{s_2}+3m_2m_{s_2}+6m_2^2m_{s_2}+9m_1m_2m_{s_2}+18m_1m_2^2m_{s_2}+9m_1m_2m_{s_2}+18m_1^2m_2m_{s_2}\right\}$$

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

$$\begin{aligned}\overline{H}_{up}(s)=\big[&\overline{H}_0(s)+\overline{H}_1(s)+\overline{H}_2(s)+\overline{H}_3(s)+\overline{H}_4(s)\\&+\overline{H}_5(s)+\overline{H}_6(s)+\overline{H}_7(s)+\overline{H}_8(s)\big]\end{aligned} \tag{76}$$

$$\overline{H}_{up}(s)=\frac{1}{K(s)}\left\{\begin{matrix}1+3m_1\left(\frac{1-\bar{s}_l\left(s+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)}{s+2m_1+3m_2+m_r+m_h+m_{s_1}+m_{s_2}}\right)+6m_1^2\left(\frac{1-\bar{s}_l\left(s+m_1+m_{s_1}+m_{s_2}\right)}{s+m_1+m_{s_1}+m_{s_2}}\right)+\\3m_2\left(\frac{1-\bar{s}_l\left(s+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}\right)}{s+3m_1+2m_2+m_r+m_h+m_{s_1}+m_{s_2}}\right)+6m_2^2\left(\frac{1-\bar{s}_l\left(s+m_2+m_{s_1}+m_{s_2}\right)}{s+m_2+m_{s_1}+m_{s_2}}\right)+\\9m_1m_2\left(\frac{1-\bar{s}_l\left(s+2m_2+m_{s_1}+m_{s_2}\right)}{s+2m_2+m_{s_1}+m_{s_2}}\right)+18m_1m_2^2\left(\frac{1-\bar{s}_l\left(s+m_2+m_{s_1}+m_{s_2}\right)}{s+m_2+m_{s_1}+m_{s_2}}\right)+\\9m_1m_2\left(\frac{1-\bar{s}_l\left(s+2m_1+m_{s_1}+m_{s_2}\right)}{s+2m_1+m_{s_1}+m_{s_2}}\right)+18m_1^2m_2\left(\frac{1-\bar{s}_l\left(s+m_1+m_{s_1}+m_{s_2}\right)}{s+m_1+m_{s_1}+m_{s_2}}\right)\end{matrix}\right\} \tag{77}$$

$$\overline{H}(s)_{down}(s)=1-\overline{H}_{up}(s)) \tag{78}$$

ANALYSIS OF THE MODEL FOR DIFFERENT CIRCUMSTANCES

Availability Analysis

Suppose that $S_{n_0}(s)=\bar{S}_{\exp[r^\theta+\{\log l(r)\}^\theta]^{1/\theta}}(s)=\frac{\exp[r^\theta+\{\log l(r)\}^\theta]^{1/\theta}}{s+\exp[r^\theta+\{\log l(r)\}^\theta]^{1/\theta}}$, $\bar{S}_l(s)=\frac{l}{s+l}$, assuming failure rates as $m_1=0.011$, $m_2=0.012$, $m_r=0.013$, $m_h=0.014$, $m_{s_1}=0.015$, $m_{s_1}=0.016$, $l_1(\mathrm{r})=l_2(\mathrm{r})=1$. Therefore, substituting those values in equation (77), the subsequent equation follows :

$$\overline{H}_{up}(q)=\begin{bmatrix}-0.000384e^{-1.04200q}-0.000453e^{-1.04300q}\\-0.000557e^{-1.05300q}-0.000547e^{-1.05500q}\\+0.023049e^{-2.78291q}-0.009251e^{-1.17509q}\\+5.615146e^{-1.11551q}+0.988140e^{-0.00925q}\end{bmatrix} \tag{79}$$

When time (t) is use as q = 0, 1,...,10 in equation (79), Table 1 obtained

Table 1. Availability analysis of the system

q	0	1	2	3	4	5	6	7	8	9	10
Availability	1.0000	0.9832	0.9816	0.9795	0.9771	0.9744	0.9717	0.9691	0.9664	0.9637	0.9610

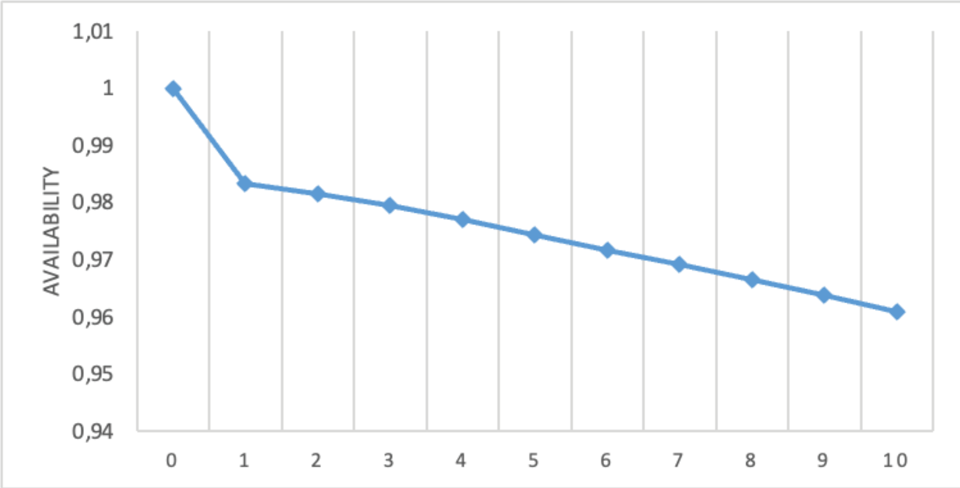

Figure 3. Honeynet availability analysis.

Reliability Analysis

If *l, n* are declared to be zero and values of failure rate as follows: $m_1 = 0.011$, $m_2 = 0.012$, $m_r = 0.013$, $m_h = 0.014$, $m_{s_1} = 0.015$, $m_{s_1} = 0.016$. Then we have,

$$\mathrm{Re}\,l(q) = \begin{bmatrix} 3e^{-0.11600q} + 0.008848e^{-0.02100j} + 0.016054e^{-0.05300q} + 0.010625e^{-0.04300q} \\ -5.052027e^{-0.12700q} + 0.016500e^{-0.05500q} + 3e^{-0.11500q} \end{bmatrix} \quad (80)$$

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:

$$MTTF = \lim_{s \to 0} \overline{H}_{up}(s) = \frac{1}{\begin{matrix} s + 3m_1 + 3m_2 + \\ m_r + m_h + m_{s_1} + m_{s_2} \end{matrix}} \left\{ \begin{matrix} 1 + \dfrac{3m_1}{2m_1 + 3m_2 + m_r + m_h + m_{s_1} + m_{s_2}} + \\ \dfrac{6m_1^2}{m_1 + m_{s_1} + m_{s_2}} + \dfrac{18m_1^2 m_2}{m_1 + m_{s_1} + m_{s_2}} + \\ \dfrac{3m_2}{3m_1 + 2m_2 + m_r + m_h + m_{s_1} + m_{s_2}} \\ + \dfrac{3m_2^2}{m_2 + m_{s_1} + m_{s_2}} + \dfrac{9m_1 m_2}{2m_2 + m_{s_1} + m_{s_2}} \\ + \dfrac{18m_1 m_2^2}{m_2 + m_{s_1} + m_{s_2}} + \dfrac{9m_1 m_2}{2m_1 + m_{s_1} + m_{s_2}} \end{matrix} \right\} \quad (81)$$

Table 2. Reliability analysis of the system

q	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Reliability	1.0000	0.9455	0.8907	0.8363	0.7830	0.7311	0.6811	0.6332	0.5875	0.5442	0.5032

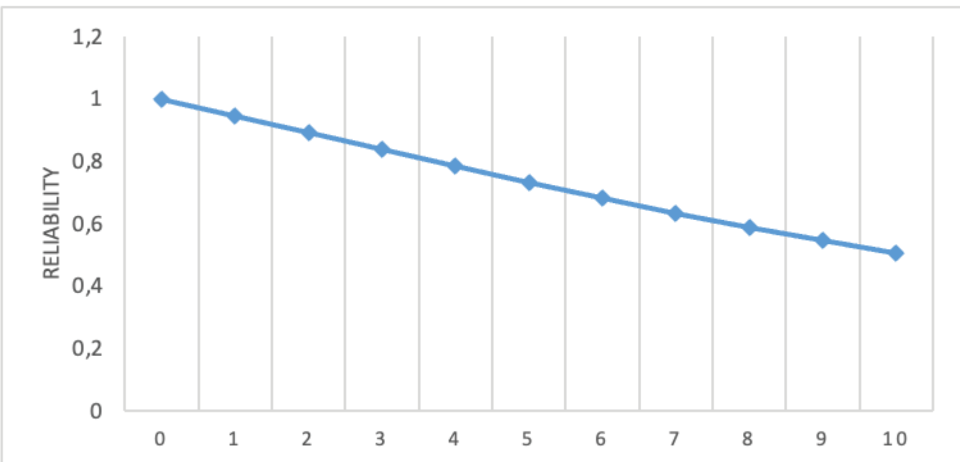

Figure 4. Honeynet Reliability Analysis.

Table 3. MTTF of the system

Failure Rate	MTTF m_1 (a)	MTTF m_2 (b)	MTTF m_r (c)	MTTF m_h (d)	MTTF m_{s_1} (e)	MTTF m_{s_2} (f)
0.001	4.4962	15.4494	15.2130	15.4035	15.9030	16.1377
0.002	4.5353	15.2001	15.0268	15.2130	15.6754	15.9030
0.003	4.5692	14.9628	14.8449	15.0268	15.4546	15.6754
0.004	4.5987	14.7365	14.6670	14.8449	15.2403	15.4546
0.005	4.6246	14.5202	14.4931	14.6670	15.0321	15.2403
0.006	4.6474	14.3132	14.3230	14.4931	14.8296	15.0321
0.007	4.6676	14.1147	14.1566	14.3230	14.6327	14.8296
0.008	4.6856	13.9241	13.9938	14.1566	14.4411	14.6327
0.009	4.7016	13.7408	13.8345	13.9938	14.2546	14.4411

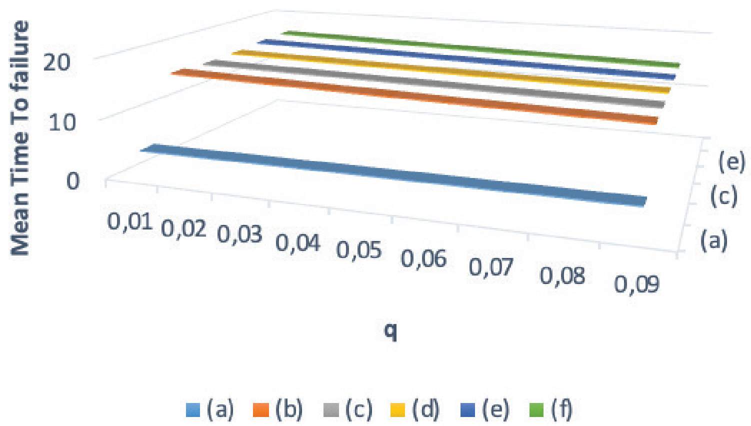

Figure 5. Honeynet MTTF Analysis.

Assuming 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 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

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_{s_1}

Table 4. Sensitivity analysis of the system.

Failure Rate	$\frac{\partial(MTTF)}{m_1}$ (I)	$\frac{\partial(MTTF)}{m_2}$ (II)	$\frac{\partial(MTTF)}{m_r}$ (III)	$\frac{\partial(MTTF)}{m_h}$ (IV)	$\frac{\partial(MTTF)}{m_{s_1}}$ (V)	$\frac{\partial(MTTF)}{m_{s_2}}$ (VI)
0.001	42.0655	-255.6961	-188.3255	-192.7575	-231.0825	-238.4650
0.002	36.3253	-243.1247	-184.0386	-188.3255	-224.1070	-231.0825
0.003	31.5751	-231.6505	-179.8908	-184.0386	-217.5019	-224.1070
0.004	27.6088	-221.1508	-175.8762	-179.8908	-211.2352	-217.5019
0.005	24.2705	-211.5148	-171.9893	-175.8762	-205.2790	-211.2352
0.006	21.4402	-202.6442	-168.2250	-171.9893	-199.6086	-205.2790
0.007	19.0249	-194.4527	-164.5782	-168.2250	-194.2023	-199.6086
0.008	16.9513	-186.8651	-161.0443	-164.5782	-189.0406	-194.2023
0.009	15.1615	-179.8160	-157.6187	-161.0443	-184.1061	-189.0406

Table 5. Profit of the system

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

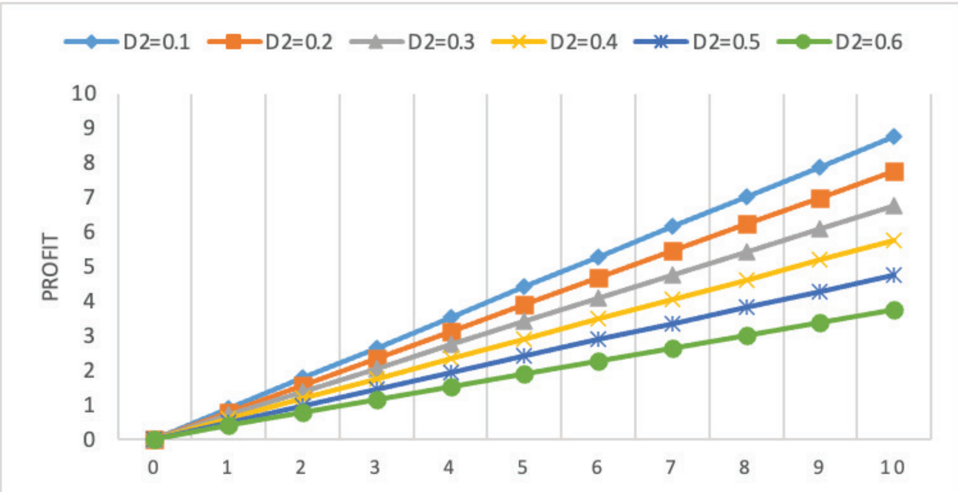

Figure 6. Honeynet Profit Analysis.

Table 6. Profit of the system

q	$E_p(q)$ $D_1 = 2$	$E_p(q)$ $D_1 = 4$	$E_p(q)$ $D_1 = 6$	$E_p(q)$ $D_1 = 8$	$E_p(q)$ $D_1 = 10$	$E_p(q)$ $D_1 = 12$
0	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
1	0.9757	2.9514	4.9272	6.9029	8.8787	10.8544
2	1.9405	5.8811	9.8217	13.7622	17.7028	21.6434
3	2.9019	8.8038	14.7057	20.6076	26.5095	32.4114
4	3.8586	11.7172	19.5759	27.4345	35.2932	43.1518
5	4.8102	14.6204	24.4307	34.2409	44.0512	53.8614
6	5.7565	17.5130	29.2695	41.0260	52.7825	64.5390
7	6.6974	20.3948	34.0922	47.7896	61.4870	75.1844
8	7.6329	23.2658	38.8987	54.5331	70.1646	85.7975
9	8.5630	26.1261	43.6892	61.2522	78.8153	96.3784
10	9.4878	28.9757	48.4636	67.9514	87.4393	106.9272

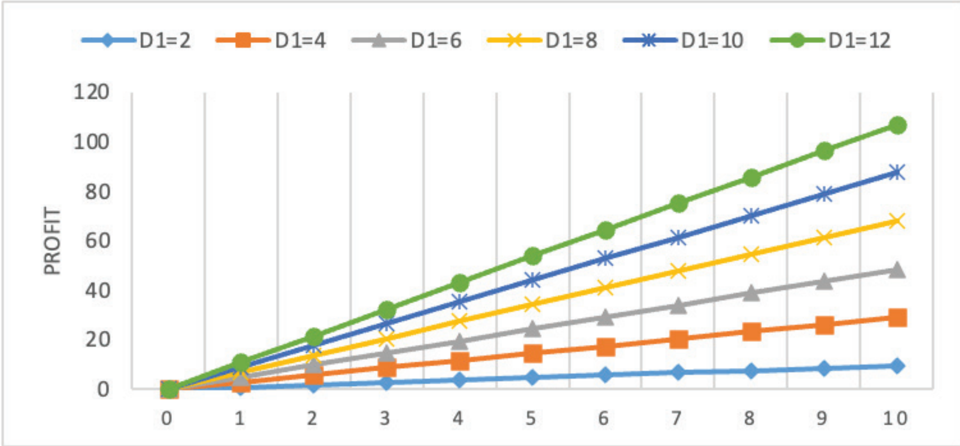

Figure 7. Honeynet Profit Analysis.

= 0.015, m_{s_1} = 0.016 of the system, by introducing the set of parametric variation of the failure rates from the resulting expression, we calculated the sensitivity as shown in Table 5 and the corresponding value in Figure 5

COST (Revenue fixed)

The service cost (D_2) is varied and revenue (D_1) fixed as 0.1, 0.2..., 0.6 for time interval, as q = 0, 1...10 in equation (83).

$$E_p(q) = D_1\int_0^q H_{up}(q)dq - D_2 q \tag{82}$$

$$E_p(q) = D_1\begin{Bmatrix} 0.000369e^{-1.04200q} + 0.000434e^{-1.04300q} + 0.000529e^{-1.05300q} + \\ 0.000518e^{-1.05500q} - 0.008282e^{-2.78291q} + 0.007873e^{-1.17509q} + \\ 5.033668e^{-1.11551q} - 355.528670e^{-0.00277q} + 355.5272 \end{Bmatrix} - D_2(q) \tag{83}$$

The revenue (D_1) is fixed and service cost (D_2) is varied as 0.1, 0.2…, 0.6 for time interval, as q = 0, 1…10 in equation (83).

COST (Service cost fixed)

The service cost (D_2) is fixed and revenue (D_1) varied as 0.1, 0.2..., 0.6 for time interval, as q = 0, 1...10 in equation (83).

RESULTS AND DISCUSSION

The objective of this section is to express numerical experiment so as to see effect of the parameters on the performance of each and every honeynet subsystem. The findings in terms of honeynet availability were briefed in the figure (3) through figure (7) and table (1) through table (5) above. The following figures have shown the simulations of availability with respect time (t) of honeynet system and it was observed that system availability decreases with increase in time (t), on the other hand the honeynet system reliability analysis shows from their respective figures above that as the time increases reliability decreases. However, in another dimension the average time to honeynet system failure (MTTF) were analyzed based on different failure rate by varying it from 0.001,.., 0.009 fixing 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. MTTF honeynet system decreases with increase in failure rate in all the cases, MTTF Sensitivity was checked in this article to determine how the honeynet 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 honeynet 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 honeynet system require optimal maintenance action in order to avoid huge downfall and adequate the life span of the network.

CONCLUSION

In this research, 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 tranfer 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 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

[1] Paryathia P, Chintab A, Patnala CM. A Honey Pot Implementation for Security Enhancement in IOT System using AES and Key management. Turk J Comput Math Educ 2021;12:5206−5214. [CrossRef]

[2] Naik N, Jenkins P, Savage N. A computational intelligence enabled honeypot for chasing ghosts in the wires. Complex Intell Syst 2021;7:477−494. [CrossRef]

[3] Kondra JR, Bharti SK, Mishra SK, Babu KS. Honeypot-Based Intrusion Detection System: A Performance Analysis. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom); 2016. p. 2347−2351

[4] Agrawal N, Tapaswi S. The performance analysis of honeypot based intrusion detection system for wireless network. Int J Wirel Inf Netw 2017;24:14−21. [CrossRef]

[5] Kasongo SM, Sun Y. Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. J Big Data 2020;7:1−20. [CrossRef]

[6] Disha RA, Waheed S. Performance analysis of machine learning models for intrusion detection system using gini impurity-based weighted random forest (GIWRF) feature selection technique. Cybersecurity 2022;5:1. [CrossRef]

[7] Alazzam H, Sharieh A, Sabri KE. A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. Expert Syst Appl 2020;148:113−249. [CrossRef]

[8] Belgrana FZ, Benamrane N, Hamaida MA. Network Intrusion Detection System using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing features. In: 2020 IEEE International Conference on Internet of Things and Intelligence System; 2020. p. 23−29. [CrossRef]

[9] Mauro DM, Galatro G, Liotta A. Experimental review of neural-based approaches for network intrusion management. IEEE Trans Netw Serv Manag 2020;17:2480−2495. [CrossRef]

[10] Kelly C, Pitropakis N, Mylonas A, McKeown S, Buchanan WJ. A comparative analysis of honeypots on different cloud platforms. Sensors. 2021;21:2433. [CrossRef]

[11] Sethia V, Jeyasekar A. Malware Capturing and Analysis using Dionaea Honeypot. In: 2019 International Carnahan Conference on Security Technology; 2019 Oct 1-3; Chennai, India. p. 1−4. [CrossRef]

[12] Lee J, Pak J, Lee M. Network Intrusion Detection System using Feature Extraction Based on Deep Sparse Autoencoder. In: 2020 International Conference on Information and Communication Technology Convergence; 2020. p. 1282−1287. [CrossRef]

[13] Gu J, Lu S. An effective intrusion detection approach using SVM with naive bayes feature embedding. Comput Secur 2021;103:102−158. [CrossRef]

[14] Isa MS, Yusuf I, Ali UA, Suleiman K, Yusuf B, Ismail AL. Reliability analysis of multi-workstation computer network configured as series-parallel system via gumbel - hougaard family copula. Int J Oper Res 2022;19:13−26.

[15] Isa MS, Abubakar MI, Ibrahim KH, Yusuf I, Tukur I. Performance analysis of complex series parallel computer network with transparent bridge using copula distribution. Int J Reliab Risk Saf Theory Appl 2021;4:47−59. [CrossRef]
[16] Xie L, Lundteigen MA, Liu YL. Common Cause Failures and Cascading Failures in Technical Systems, Similarities, Differences and Barriers. In Haugen S, Barros A, Gulijk C, Kongsvik T, Vinnem JE, (editors). Safety and Reliability - Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway. [CrossRef]
[17] Xie L, Lundteigen MA, Liu YL. Performance analysis of safety instrumented systems against cascading failures during prolonged demands. Reliab Eng Syst Saf 2021;216. [CrossRef]
[18] Yusuf I, Ismail AL, Singh VV, Ali UA, Sufi NA. Performance analysis of multi computer system consisting of three subsystems in series configuration using copula repair policy. SN Comput Sci 2020;1:241. [CrossRef]
[19] Colledani M, Tolio T, Yemane A. Production Quality Improvement During manufacturing systems ramp-up. J Manuf Sci Technol 2019;23. [CrossRef]
[20] Althubiti SA, Jones EM, Roy K. LSTM for Anomaly-Based Network Intrusion Detection. In: 28th International Telecommunication Networks and Applications Conference; 2018. [CrossRef]
[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]
[22] Albahar M, Alharbi A, Alsuwat M, Aljuaid H. A hybrid model based on radial basis function neural network for intrusion detection. Int J Adv Comput Sci Appl 2020;11:781−791. [CrossRef]
[23] Arqub OA, Singh J, Alhodaly M. Adaptation of kernel functions-based approach with Atangana-Baleanu-Caputo distributed order derivative for solutions of fuzzy fractional Volterra and Fredholm integrodifferential equations. Math Meth Appl Sci 2021;46:7228. [CrossRef]
[24] Hammour ZA, Arqub OA, Momani S, Nabil S. Optimization Solution of Troesch's and Bratu's Problems of Ordinary Type Using Novel Continuous Genetic Algorithm. Discret Dyn Nat Soc 2014;2014:401696. [CrossRef]
[25] Arqub OA, Hammour ZA. Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm. Inf Sci 2014;279:396−415. [CrossRef]
[26] Arqub OA, Singh J, Banan M, Alhodaly M. Reproducing kernel approach for numerical solutions of fuzzy fractional initial value problems under the Mittag-Leffler kernel differential operator. Math Meth Appl Sci 2021;46:7965−7986. [CrossRef]
[27] Kenan E, Mustafa CK, Boru B. Comparison of gesture classification methods with contact and non-contact sensors for human-computer interaction. Sigma J Eng Nat Sci 2021;40:219−226.
[28] Şekerci AZ, Aydın N. A stochastic model for facility locations using the priority of fuzzy AHP. Sigma J Eng Nat Sci 2022;40:649−662. [CrossRef]
[29] Aydın Er B, Şişman A, Ardalı Y. Applicability of radial-based artificial neural networks (RBNN) on coliform calculation: A case of study. Sigma J Eng Nat Sci 2022;40:724−731. [CrossRef]
[30] Tolga B, Ali FG. BLEVE risk effect estimation using the Levenberg-Marquardt algorithm in an artificial neural network model. Sigma J Eng Nat Sci 2022;40:877−893.
[31] Bakar O, Murat B. Applicability of radial-based artificial neural networks (RBNN) on coliform calculation: A case of study. Sigma J Eng Nat Sci 2021;40:235−242.
[32] Adem Y. Intuitionistic fuzzy hypersoft topology and its applications to multi-criteria decision-making. Sigma J Eng Nat Sci 2023;41:106−118.
[33] Maryam B, Rashid R, Karim S. On codes over product of finite chain rings. Sigma J Eng Nat Sci 2023;41:145−155.
[34] Isa MS, Yusuf I, Ali UA, Jinbiao W. Series-parallel computer system performance evaluation with human operator using gumbel hougaard family copula. In: Computational Intelligence in Sustainable Reliability Engineering. 2023. p. 109−127. [CrossRef]
[35] Yusuf I, Ismail AL, Sufi NA, Ambursa FU, Sanusi A, Isa MS. Reliability Analysis of Distributed System for Enhancing Data Replication using Gumbel Hougaard Family Copula Approach Joint Probability Distribution. J Ind Eng Int 2021;17:59−78.