International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Proposing A Mathematical Model with Two Sets of Population on Rumor Transmission in Social Networks to Reduce the Rumor

Mrs. Dipti Rashmi[1], Prof. (Dr.) Binod Kumar[2], Dr. Prakash C. Mittal[3]

[1]PhD Scholar, Dept. of CS/IT, AISECT University, India
[2]Professor, Dept. of CS/IT, AISECT University, India
[3]Lecturer (Math), Dept. Of SS, UTAS-Muscat, Oman

Abstract

Rumor is an unverified proposition or account concerning individuals, events, or issues of public concern that circulates informally from person to person. By characteristic it lacks official confirmation of being it true or false, or a mixture of both. Rumor can be good if it acts as a "collective problem-solving" mechanism to help groups understand, adapt to, or cope with, the unknown else it can be very harmful or destructive if it is altered badly and wrongly reflecting the motivations and anxieties of the communicators. It can break the harmony of community, society and nation. Intensity of a rumor as being proportional to the importance of the subject to the individual is multiplied by the ambiguity of the situation surrounding the subject [Ralph Rosnow]. Inaccurate or intentionally misleading information framed as scientific, often spread via social media—pose significant dangers to public health, safety, harmony and the integrity of nation. It put public, society and nation in very worst situation. This kind of rumor need to stop or at least minimized up to a level that can harm least. This paper aim is to propose a mathematical model that can reduce the rumor to the least level. It deals with the two sets of population to achieve this goal. It highlights the rumor reproduction rate and how to stabilize that by doing mathematical simulation and result analysis. Researchers can use this paper to design and develop a model or enhance the capability of existing models of this area to stop the rumor intentioned bad.

Keywords: Rumor, Botnet, Endemic, Deepfakes, Stability,Analysis, Simulation, Machine Learning

1. INTRODUCTION

Rumors, defined as unverified and often false information spread among people, having far-reaching impacts. Unconfirmed information is circulated among people, typically through word of mouth or social-media platforms. It often spread rapidly and covers various topics, including gossip about individuals, newsevents, or conspiracy theories. They may contain elements of truth but are more often exaggerated, distorted, or entirely fabricated. It influences public opinion, create panic, and even incite violence. Parallel, repetitive and rapid spread of rumor makes situation worst within the day and sometime within the hour because it is circulated much faster and further than verified, true information. Scientific rumors often leverage emotional, simplistic, or fear-based, "science" language, which people are more likely to share and believe due to confirmation bias (preferring information that fits their existing beliefs. False rumors can have severe financial consequences, such as in 2013 when a fake

tweet caused a temporary $130 billion drop in the stock market. So there is need to take measures to it or at least minimize it to a level that can be least harmful. Bots are automated accounts that produce content, interact with users, and amplify messages at a scale unattainable by humans alone. It often operates in coordinated networks, where multiple bots interact with each other to reinforce specific messages or trends. This behavior creates "echo chambers" that amplify misinformation and polarize communities [10].

This paper aim is to propose a mathematical model that can reduce the rumor to the least level. It highlights the rumor reproduction rate and a way to stabilize that by doing mathematical simulation and result analysis of two sets of population namely normal users and bot users. Researchers can use this paper to design and develop a model or enhance the capability of existing models of this area to stop the rumors intentioned bad. They can use these concepts willing to do research in rumor detection, investigation, controlling, stopping and dumping. This paper is useful for the researchers focused on understanding their creation, dissemination, and mitigation, leveraging disciplines like sociology, psychology, mathematics, and computer science. Key areas include modeling propagation mechanisms, developing AI-driven detection systems, analyzing user psychology, and crafting effective rumor-refutation strategies. This paper provides valuable insights into the design and implementation of crowd sourcing frameworks and highlights the importance of integrating diverse detection methods to enhance social media security. It provides a detailed examination of the role of bots during a significant political event, highlighting their potential to influence public discourse and amplify specific messages. It underscores challenges posed by automated accounts in the digital age and calls for more robust measures to detect and mitigate their impact on political communication. This study's findings contribute to the broader understanding of how automation and social media intersect with politics and public opinion. Additionally, bots can exploit social media algorithms designed to prioritize popular content, thereby increasing the visibility of their messages and influencing what human users see [15-19]. These also include algorithmic approaches to identify unusual patterns of information spread, network analysis to detect clusters of coordinated activity, and the development of digital literacy programs to educate users about the risks of misinformation.

2. Challenges

Challenges in rumor area, specifically within online social networks and digital platforms, are multifaceted, covering detection, propagation modeling, and intervention. Key challenges include dealing with massive data volume and velocity, the rapid evolution of fake news techniques (e.g.,deepfakes), and the difficulty of interpreting "black box" AI detection models. Identifying rumors early in their spread, especially when they are designed to look authentic, remains a significant technical challenge. These challenges involve integrating multimodal fusion (text + images), using Graph Neural Networks (GNNs) for better structural analysis, and incorporating AI-based detection to tackle increasingly sophisticated misinformation. Further advancements in detection methodologies were a wavelet-based model to classify users in online social networks as human, legitimate bots, or malicious bots. This approach utilizes spectral patterns derived from textual content; showcasing the potential of advanced signal processing techniques in bot detection mechanisms of bot propagation are multifaceted. Rapid spread of rumors on social media is facilitated by the platform's design, which encourages sharing and amplification of content, often without thorough verification[5].

New challenges of detecting mimicking attacks, revealing that when the number of active bots matches

or exceeds that of legitimate users, statistical detection become nearly impossible. This insight underscores the complexity of modeling botnet behavior, particularly in environments with high user activity [6]. This phenomenon is particularly concerning during crises or significant events, where misinformation can hinder effective response efforts and exacerbate situations [7]. The evolution of detection techniques like who present SMARTbot, a dynamic analysis framework that integrates machine learning to identify mobile botnet applications. This not only advances detection methodologies but also establishes a mobile botnet dataset that serves as a benchmark for future research [8].

Understanding bot propagation models is crucial for developing effective counter measures. Researchers are employing various techniques to detect and mitigate the influence of bots, including network analysis, machine learning-based detection systems, and the development of policies aimed at improving transparency and accountability on social media platforms [11-12]. Presence of bots complicates the landscape of social media by making it difficult to discern authentic user activity from automated interventions. Advanced bot models utilize machine learning algorithms to enhance their interaction capabilities, making them increasingly indistinguishable from human users These sophisticated bots can adapt to the context of conversations, tailor responses based on user interactions, and even generate original content, further blurring the line between human and automated behavior[21-22]. In related vein, artificial application intelligence in developing chatbots for agricultural discussions, demonstrating how AI can enhance user interaction while also raises questions about the authenticity of user-generated content [20].

3. Proposed Model

3.1 Proposed Model: Analysis

Foundational works in this area is the study that presents a bot detection model utilizing users' in-game action sequences. This model leverages big data analysis to identify patterns indicative of bot activity, highlighting the importance of user behavior analysis in distinguishing between human and bot interactions[3]. A network failure model for detecting bot hosts, emphasizing a method that operates independently of aggregated network information, thus providing a scalable solution for bot detection across various network sizes was proposed[4]. Bot models are employed for variety of purposes, ranging from benign activities such as customer service and information dissemination to more malicious intentions like spreading misinformation, manipulating public opinion, and even orchestrating cyber-attacks[9]. One significant aspect of bot propagation is the use of network effects. By analyzing the structure and behavior of bot networks, researchers can identify patterns and signals indicative of bot activity, thus contributing to more robust defenses against their potentially harmful effects .The scale and speed at which bots operate make them powerful tools for shaping discourse, particularly during critical events such as elections, pandemics, and social movements. Mazzariello in 2008 introduced a network traffic analysis architecture designed to detect botnets by focusing on behavioral models of network users. This foundational work emphasizes the importance of understanding user behavior to identify botnet-related activities effectively[1]. Following this a real-time detection method for fast-flux botnets, highlighting the temporal aspect of detection, which requires a few days to draw reliable conclusions about web services potentially hosted by such botnets[2]. Then correlation-based approach came that utilizes network communication histogram analysis to detect HTTP bots. Their model achieves high accuracy and low false positive rates, demonstrating the effectiveness of behavior-based detection strategies [13]. Emergence of new botnet types were addressed by SoCellBot, a cellular botnet

leveraging online social networks for recruitment and communication. This study highlights the need for adaptive models that account for the evolving landscape of botnet strategies[14].

Bots can be programmed to post content, like and share posts, follow users, and engage in conversations, thereby creating an illusion of consensus and amplifying specific narratives. bots can be used for benign purposes, such as customer service or information dissemination, they are frequently deployed to manipulate public opinion, spread disinformation, and create the illusion of consensus. The potential of crowd sourcing as a powerful tool for detecting bot accounts on social networks combines the strengths of human judgment with automated detection systems. In a more recent contribution, a multi-feature behavior approximation model aimed at enhancing botnet detection and reducing financial fraud was developed. This model reflects a growing trend towards integrating multiple behavioral features to improve detection efficacy[23]. A game-theoretic approach, proposing a zero-sum one-sided partially observable stochastic game model to address botnet propagation in IoT environments. It focus on deception strategies for defenders illustrates a novel angle in the ongoing battle against botnets[24].

Finally, a smart detection system utilizing a Random Forest Classifier and Principal Component Analysis (PCA) to identify behavioral botnet attacks. This approach emphasizes the importance of robust datasets in developing effective detection models[25]. Then challenge of distinguishing between human users and bots is further examined by investigating the factors influencing individuals' abilities to detect social bots on platforms like Twitter. This results highlight how difficult it is to detect bots and how various users' abilities to spot dishonest people vary. This complexity is compounded by the adversarial tactics employed by bots by introducing a node injection-based attack method that aims to evade detection by existing models[26-27]. Most recently, DBoTPM, a deep neural network-based model for botnet prediction, which addresses the challenges posed by botnet attacks on IoT system, signifies a shift towards leveraging advanced machine learning techniques to enhance predictive capabilities in botnet detection [28].

3.2 Proposed Model: Description & Formulation

We are proposing a mathematical model with the formulation of two population sizes of human first one consisting population of normal social media users and the second one is botnet users. Normal social media users encompass a broad spectrum of individuals who use social media platforms for various purposes, such as staying connected with friends and family, sharing personal updates, consuming news and entertainment, networking professionally, promoting businesses or personal brands, and engaging with communities of shared interests. Bots are computer programs that mimic or communicate with human users by doing automated tasks over the Internet. The propagation of bot models, or the strategies and mechanisms by which these bots spread and amplify information, presents complex challenges and opportunities for understanding digital communication dynamics. Bot users ranges from individuals running small-scale automated scripts to organizations or malicious actors deploying sophisticated bot networks for various purposes, including marketing, political manipulation, or spreading malicious content. Social media platforms continually develop measures to detect and mitigate the impact of bot activity on their platforms.

The basic reproductive number R_0 and equilibrium points for the model are defined. The rumor - free equilibrium is proved to be globally stable when $R_0 < 1$, which means the rumor, will die out and when $R_0 > 1$, the endemic equilibrium is globally stable. Extensive numerical simulations are carried out in MATLAB to establish the analytical results. In social networks, we categorize the normal human population into three groups $S_x I_x R_x$ (Susceptible-Infected-Recovered) and the rumor-transmitting human

population into two classes S_y I_y (Susceptible-Infected) .Figure 1 illustrates the model's schematic flow, while Table-1 lists the state variables and related parameters.

S_x**(t)** : Susceptible proportions of x-humans in time t Designate the unaware group of people subjected to bot rumors. The term "unaware" refers to people who are probably well-informed and disregard any rumors.
$I_x(t)$: Infectious proportions of x-humans in time t Designate the group of persons who have heard the rumor but haven't started spreading it yet. They may be in a stage where they are processing the knowledge in their brains and are unable to communicate it to others at this time.
R_x **(t):** Recovered proportions of x-humans in time t This category represents individuals who are committed to reducing the spread and impact of propaganda and bot rumors by combating misinformation with factual information or by simply choosing to no longer spread the bot.
$S_y(t)$: Susceptible proportions of y-humans in time t Designate the group of people who have not only heard the rumor but are also actively and ignorantly spreading it to others. Since they are deliberately disseminating false information, they have turned into "infectious." The term "misinformation" describes the dissemination of false information, typically without the aim to mislead. It can occur due, to errors, misunderstandings or misinterpretations of facts.
$I_y(t)$**:** Infectious proportions of y-humans in time t Designate the group of malicious bots. They are persons who engage in dishonest behavior with the objective of misleading and exploiting others for monetary gain or other negative goals by purposefully spreading "disinformation." Disinformation is defined as purposefully inaccurate or misleading information that is produced and spread with the express objective of misleading or deceiving other people. Often there is a deliberate attempt to spread false and misleading information out of political or ideological motives. Bots aim to use available information to achieve their goals, which may include sowing confusion, destroying trust, or driving a specific policy face.
$\bar{S}_x$ **(t)** : Susceptible x- humans in time t
$\bar{I}_x$ **(t)** : Infectious x- humans in time t
$\bar{R}_x$ **(t)** : Recovered x- humans in time t
$\bar{S}_y$ **(t)** : Susceptible y- humans in time t
$\overline{I_y}$**(t):** Infectious y- humans in time t
N_x **(t) :** Total x-human population in time t
N_y**(t)** : Total y-human population in time t
B_x **:** Birth rate and immigration rate of x- humans
B_y **:** Birth rate and immigration rate of y- humans
β_x **SI:** Transmission probability of rumor from x-susceptible humans to x- infected humans
β_y **SI:** Transmission probability of rumor from y-susceptible humans to y- infected humans
η : Rate of rumor transmission from x-Infected to x-recovered humans.
δ**:** Rate of rumor transmission from x-recovered to x-susceptible humans.
μ_h**:** Natural death rate of x- humans.

μ_z: Death rate of humans due to xy- rumor.
μ_y: Natural death rate of rumor.

Table-1: State variables and related parameters

3.4 Proposed Model: Basic assumptions

We assume that normal humans (x) enter the susceptible class through a constant birth rate and immigration rate B_x. When a rumor enters into a Susceptible group of human, he/she moves to the infected class with the transmission probability β_x, where β_x is the sum of the transmission probability of rumor from human to human in social network. After some time, the infectious humans recover and move to the Recovered class with a constant rate η. The recovered humans have awareness about the rumor and so after some period of time, they return to the Susceptible class with constant rate δ. Humans leave the population through a natural death rate μ_h, and through a per capita rumor-induced death rate μ_z. In rumor transmitting humans(y), we assumed that the rumor enters the Susceptible class through a constant birth rate and immigration rate B_y. The constant transmission probability of rumor from susceptible human to infected human is β_y. Rumors leave the social network at a constant rate of μ_y.

3.3. Proposed Model: Equations for Humans population

Based on our assumptions and the flow of transmission of rumor in normal human population (x) in social netwoks and rumor propagating bot users (y) in social networks, we have the following system of equations and diagram.

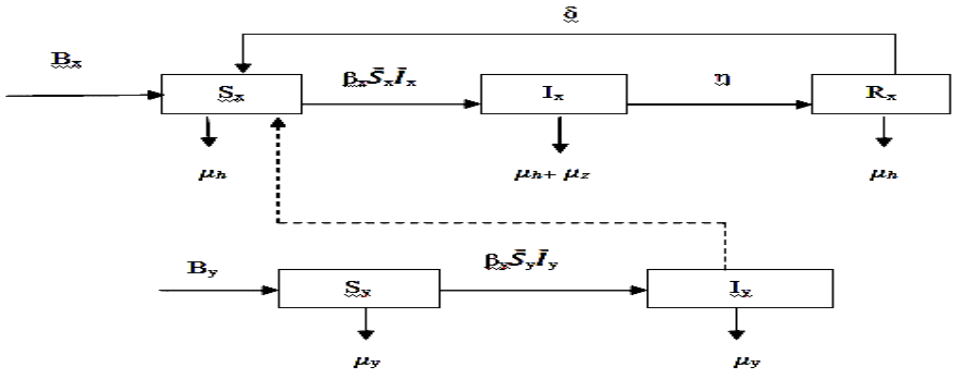

Fig.-1: Schematic diagram of rumor transmission in two population models.

$$\frac{d\bar{S}_x}{dt} = B_x N_x - \beta_x \bar{S}_x(\bar{I}_x + \bar{I}_y) - \mu_n \bar{S}_x + \delta\bar{R}_x$$

$$\frac{d\bar{I}_H}{dt} = \beta_x \bar{S}_x(\bar{I}_x + \bar{I}_y) - (\mu_n + \mu_z + \eta - \theta)\bar{I}_x \quad (1)$$

$$\frac{d\bar{R}_x}{dt} = \eta\bar{I}_x - (\mu_n + \delta)\bar{R}_x$$

Similarly, for the flow of transmission of rumor by bot users, we have equations as:

$$\frac{d\bar{S}_y}{dt} = B_y N_Y - \beta_y \bar{S}_y \bar{I}_y - \mu_y \bar{S}_y$$

$$\frac{d\bar{I}_y}{dt} = \beta_y \bar{S}_y \bar{I}_y - \mu_y \bar{I}_y \quad (2)$$

With these two conditions $\bar{S}_x + \bar{I}_x + \bar{R}_x = N_x$ and $\bar{S}_y + \bar{I}_y = N_y$
Without loss of generality, we can write with the proportions

$$S_x = \frac{\bar{S}_x}{N_x}, I_x = \frac{\bar{I}_x}{N_x}, R_x = \frac{\bar{R}_x}{N_x}, S_y = \frac{\bar{S}_y}{N_y}, I_y = \frac{\bar{I}_y}{N_y}$$

Since $R_x = 1 - S_x - I_x$ and $S_y = 1 - I_y$, the above two systems (1) and (2) can be reduced to the following equivalent system:

$$\begin{aligned} \frac{dS_x}{dt} &= B_x - \beta_x S_x (I_x + I_y) - \mu_n S_x + \delta(1 - S_x - I_x) \\ \frac{dI_x}{dt} &= \beta_x + S_x + (I_x + I_y) - (\mu_n + \mu_z + \eta - \theta) I_x \\ \frac{dI_y}{dt} &= \beta_y (1 - I_y) I_y - \mu_y I_y \end{aligned} \quad (3)$$

The feasible region for the system (3) is as follows:
$\Gamma = \{(S_x, I_x, I_y) \in R^3: S_x > 0, I_x \geq 0, I_y \geq 0, S_x + I_x \leq 1, I_y \leq 1\}$.

4. Model Stability

In this section, we are finding the equilibrium states and basic reproduction number of the model. We have demonstrated the global and local stability of our model for both endemic and rumor-free equilibrium points. We may identify equilibrium states by setting the right-hand side of all system (3) model equations to zero. This yields two equilibrium states:
(i) Bot free equilibrium state: $E_0 = (1, 0, 0)$
(ii) Endemic equilibrium state: $E_1 = (S_x^*, I_x^*, I_y^*)$
It is anticipated that the system under modeling would exhibit several types of behavior throughout time. We may forecast the long-term behavior of the system and categorize it into a limited number of options by using the equilibrium points and the conditions for their existence, which provide us mathematical conditions.
Endemic Equilibrium points of the system (3): From the third equation of the system (3) by equating to zero, we get:

$$I_y = \frac{\beta_y I_x}{\mu_y + \beta_y I_x}$$

Similarly, from the first and the second of the system (3) by equating to zero and solving it, we get:

$$S_x = \frac{A - BI_x}{C}, where\ A = B_x + \delta, B = \mu_n + \mu_z + \eta + \delta - \theta, C = \mu + \delta$$

Putting the values of I_y and S_x in second equation of system(3), we get:

$$B\beta_x\beta_y I_x^2 + [CD\beta_y - A\beta_x\beta_y + B\beta_x(\mu_y + \beta_y)]I_x + CD\mu_y - A\beta_x(\mu_y + \beta_y) = 0$$

Since all the parametric values are positive, so we consider only positive root of above equation and endemic equilibriums
$E_1 = (S_x^*, I_x^*, I_y^*)$ are as follows:

$$I_x^* = \frac{CD\beta_y - A\beta_x\beta_y + B\beta_x(\mu_y + \beta_y) + \sqrt{(CD\beta_y - A\beta_x\beta_y + B\beta_x(\mu_y + \beta_y))^2 - 4B\beta_x\beta_y(CD\mu_y - A\beta_x(\mu_y + \beta_y))}}{2B\beta_x\beta_y},$$

$I_y^* = \frac{\beta_y I_x^*}{\mu_y + \beta_y I_x^*}$, and $S_x^* = \frac{(\mu_n + \mu_z + \eta - \theta) I_x^*}{\beta_x (I_x^* + I_y^*)}$.

4.1 Basic reproduction number

The average number of secondary infectious cases caused by a single infection in the entire susceptible population is the basic reproduction number for any epidemic model. The fundamental reproduction number is calculated by $R_0 = \rho(FV^{-1})$, where ρ is spectral radius of the matrix FV^{-1} and F & V are the matrices of new infection terms and the remaining transmission terms respectively.

For the systems (1) & (2), the matrices F and V are as follows:

$$F = \begin{bmatrix} \beta_x & \beta_x \\ \beta_y & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} \mu_n + \mu_z + \eta - \theta & 0 \\ 0 & \mu_y \end{bmatrix}.$$

Hence, the basic reproduction number of the above model is:

$$R_0 = \frac{\beta_x \mu_n^2 + \sqrt{\mu_y \beta_x^2 + 4(\mu_n + \mu_z + \eta - \theta)\beta_y^2}}{2\mu_y^2(\mu_n + \mu_z + \eta - \theta)}$$

4.2 Theorem-1: The System (3) is locally asymptotically stable for bot free equilibrium, when $R_0 < 1$.

Proof: Jacobian matrix of the system (3) is as follows:

$$J = \begin{bmatrix} -(\mu_n + \delta) & -(\beta_x + \delta) & -\beta_x \\ 0 & \beta_x - (\mu_n + \mu_z + \eta - \theta) & \beta_x \\ 0 & \beta_y & -\mu_y \end{bmatrix}$$

The eigen values of Jacobian matrix J are as follows:

$$\lambda_1 = -(\mu + \delta)$$

$$\lambda_2 = -\frac{(\mu_n + \mu_z + \eta - \theta + \mu_y - \beta_x)}{2} - \frac{\sqrt{(\mu_n + \mu_z + \eta - \theta - \mu_y - \beta_x)^2 + 4\beta_x\beta_y}}{2}$$

$$\lambda_3 = -\frac{(\mu_n + \mu_z + \eta - \theta + \mu_y - \beta_x)}{2} + \frac{\sqrt{(\mu_n + \mu_z + \eta - \theta - \mu_y - \beta_x)^2 + 4\beta_x\beta_y}}{2}$$

Eigen values λ_1 and λ_2 have negative real value and we can easily verify that the eigen value $\lambda_3 < 0$, when $R_0 < 1$.

Hence, all eigen values of Jacobian matrix J are negative when $R_0 < 1$.

This proves that our the system is locally asymptotically stable when $R_0 < 1$.

4.3 Theorem- 2: The unique endemic equilibrium point E_1 is globally asymptotically stable if $R_0 > 1$.

Proof: We will prove the global stability of endemic equilibrium E_1 using geometric approach [29]. The sufficient conditions for the global stability are shown in the hypotheses (H1) and (H2) with the Bendixson criteria [30].

For the general solution $(S_x(t), I_x(t), I_y(t))$ of system (3),the Jacobian matrix is:

$$J = \begin{bmatrix} -\beta_x(I_x + I_y) - \mu_n - \delta & -\beta_x S_x - \delta & -\beta_x S_x \\ \beta_x(I_x + I_y) & \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) & \beta_x S_x \\ 0 & \beta_y(1 - I_y) & -\beta_y I_y - \mu_y \end{bmatrix}$$

The matrix $J^{[2]}$, the second additive compound matrix of the Jacobian for n=3, is defined as:

$$J^{[2]} = \begin{bmatrix} j_{11} + j_{22} & j_{23} & -j_{13} \\ j_{32} & j_{11} + j_{33} & j_{12} \\ -j_{31} & j_{21} & j_{22} + j_{33} \end{bmatrix}$$

So, its second additive compound matrix $J^{[2]}$ is

$$J^{[2]} = \begin{bmatrix} x & \beta_x S_x & \beta_x S_x \\ \beta_y(1 - I_y) & y & -\beta_x S_x - \delta \\ 0 & \beta_x(I_x + I_y) & \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) - \beta_y I_y - \mu_y \end{bmatrix},$$

Where $x = -\beta_x(I_x + I_y) - \mu_n - \delta + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta)$ and

$$y = -\beta_x(I_x + I_y) - \mu_n - \delta - \beta_y I_y - \mu_y$$

Let the function $P = (S_x, I_x, I_y)$ be defined as

$$P = (S_x, I_x, I_y) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{I_x}{I_y} & 0 \\ 0 & 0 & \frac{I_x}{I_y} \end{bmatrix} = diag\{1, \frac{I_x}{I_y}, \frac{I_x}{I_y}\}$$

$$\text{Then, } P_f P^{-1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \frac{I_x'}{I_x} - \frac{I_y'}{I_y} & 0 \\ 0 & 0 & \frac{I_x'}{I_x} - \frac{I_y'}{I_y} \end{bmatrix} \quad (4)$$

where P_f is the matrix obtained by replacing each elements of P by its derivative in the direction of f.

$$P_f J^2 P^{-1} = \begin{bmatrix} x & \beta_x S_x \frac{I_y}{I_x} & \beta_x S_x \frac{I_y}{I_x} \\ \beta_y(1 - I_y)\frac{I_y}{I_x} & y & -\beta_x S_x - \delta \\ 0 & \beta_x(I_x + I_y) & \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) - \beta_y I_y - \mu_y \end{bmatrix}$$

Where $x = -\beta_x(I_x + I_y) - \mu_n - \delta + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta)$ and

$$y = -\beta_x(I_x + I_y) - \mu_n - \delta - \beta_y I_y - \mu_y$$

$$B = P_f P^{-1} + P_f J^2 P^{-1} = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

Where, $B_{11} = [-\beta_x(I_x + I_y) - \mu_n - \delta + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta)]$,

$$B_{12} = [\beta_x S_x \frac{I_y}{I_x} \quad \beta_x S_x \frac{I_y}{I_x}],$$

$$B_{21} = \begin{bmatrix} \beta_y (1 - I_y) \frac{I_x}{I_y} \\ 0 \end{bmatrix} \text{ and}$$

$$B_{22} = \begin{bmatrix} y + \frac{I_x'}{I_x} - \frac{I_y'}{I_y} & -\beta_x S_x - \delta \\ \beta_x (I_x + I_y) & \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) - \beta_y I_y - \mu_y + \frac{I_x'}{I_x} - \frac{I_y'}{I_y} \end{bmatrix}$$

Where, y = $-\beta_x (I_x + I_y) - \mu_n - \delta + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) - \beta_y I_y - \mu_y$

Now, for a vector (u, v, w) in $\boldsymbol{R}3$, we select a norm as $|(u, v, w)| = max\{|u|, |v + w|\}$ and denote $\mu(B)$ the Lozinskii measure for this norm.

From (4), it follows that $(B) \leq \sup\{k1, k2\}$ (5)
where $\boldsymbol{k_1}$ and $\boldsymbol{k_2}$ are defined as follows:
$\boldsymbol{k_1} = \boldsymbol{B_{11}} + |\boldsymbol{B_{12}}|$and $\boldsymbol{k_2} = \boldsymbol{\mu_1}(\boldsymbol{B_{22}}) + |\boldsymbol{B_{21}}|$, where $|\boldsymbol{B_{12}}|$ and $|\boldsymbol{B_{21}}|$ are matrix norms with respect to the vector norm $L1$ and $\boldsymbol{\mu_1}$denotes the Lozinskii measure with respect to the vector Norm $\boldsymbol{L^1}$. So, we have:

$$\boldsymbol{k_1} = \boldsymbol{B_{11}} + |\boldsymbol{B_{12}}| = -\beta_x (I_x + I_y) - \mu_n - \delta + S_x - (\mu_n + \mu_z + \eta - \theta) + \sup\left\{\beta_x S_x \frac{I_y}{I_x}, \beta_x S_x \frac{I_y}{I_x}\right\}$$

$$\boldsymbol{k_1} = -\beta_x (I_x + I_y) - \mu_n - \delta + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) + \beta_x S_x \frac{I_y}{I_x} \quad (6)$$

Similarly, $\boldsymbol{k_2} = \boldsymbol{\mu_1}(\boldsymbol{B_{22}}) + |\boldsymbol{B_{21}}| =$

$$(1 - I_y) \frac{I_y}{I_x} + \beta_x S_x - (\mu_n + \mu_z + \eta - \theta) - \beta_y I_y - \mu_y + \frac{I_x'}{I_x} - \frac{I_y'}{I_y} \quad (7)$$

From second and third equations of system (3), we can rewrite as:

$$\frac{I_x'}{I_x} + (\mu_n + \mu_z + \eta - \theta) = \beta_x S_x + \beta_x S_x \frac{I_y}{I_x} \quad (8)$$

$$\frac{I_y'}{I_y} + \mu_y = \beta_y (1 - I_y) \frac{I_x}{I_y} \quad (9)$$

Putting (8) and (9) in (7) and (6) respectively, we get:

$$\boldsymbol{k_1} = -\beta_x (I_x + I_y) + \frac{I_x'}{I_x} - (\mu_n + \delta) \leq \frac{I_x'}{I_x} - (\mu_n + \delta)$$

$$\boldsymbol{k_2} = -\beta_y I_y + \frac{I_x'}{I_x} - (\mu_n + \delta) \leq \frac{I_x'}{I_x} - (\mu_n + \delta)$$

Hence, from (5)

$\mu(\mathbf{B}) \leq \frac{I_x'}{I_x} - (\mu_n + \delta)$ and so, $\frac{1}{t}\int_0^t \mu(\mathbf{B})\mathbf{ds} \leq \frac{1}{t}\log_e \frac{I_x'}{I_x} - (\mu_n + \delta)$.

So, $\bar{q_2} < 0$, and hence the Bendixson criteria is also satisfied, which thus proves the global stability of the endemic equilibrium.

5. Proposed Model: Numerical Simulation and Parametric Values Effectiveness

In this section, using Runge-kutta-Fehlberg method of order 4 & 5 in MATLAB, we numerically simulating our system with parametric values as given in Table 2 when $R_0 < 1$ & Table 3, when $R_0 > 1$ and establish the stability of models by taking different examples.

Parameter	Value	Parameter	Value
β_x	0.0004	η	0.2
β_y	0.0003	θ	0.1
δ	0.9	μ_n	0.6
B_x	0.8	μ_y	0.4
B_y	0.7	μ_z	0.3

Table-2: Parametric values for the model when $R_0 < 1$.

Parameter	Value	Parameter	Value
β_x	0.7	η	0.5
β_y	0.9	θ	0.1
δ	0.6	μ_n	0.4
B_x	0.8	μ_y	0.8
B_y	0.7	μ_z	0.9

Table-3: Parametric values for the model when $R_0 > 1$.

Example- 1: Consider the system (1) with initial conditions S_x=9999, I_x=1000, R_x=100, S_y=4999, I_y=100 and the parametric values as shown in Table-2. The simulation results are shown in figure 1, which illustrates the behavior of Susceptible, Infected, Recovered classes for human population and Susceptible, Infected classes for bot population. These are initially positive in the region of admissible values and asymptotically approach to the rumor free equilibrium for $R_0 = 0.0022 < 1$

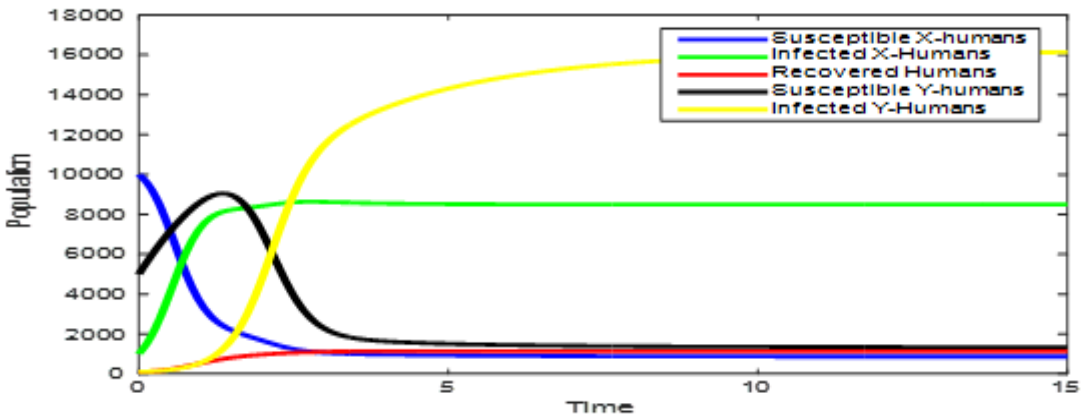

Fig.-2: Comparison of all classes for normal humans(x-humans) and bot users(y-humans).

Example-2: Consider the system (1) with initial conditions Sx=9999, Ix=100, Rx=100, Sy=999, Iy=100 and the parametric values as shown in Table-2. We simulate between infected humans versus recovered

humans when η=0.2, η=0.25, η=0.35, η=0.45, η=0.6, then the basic reproduction numbers are R_0= 0.0022, R_0 =0.0021, R_0=0.0020, R_0= 0.0019 and R_0=0.0018 respectively as shown in figure 3. From figure 3, we observe that the nature of trajectory tends to rumor-free equilibrium point in infected-recovered phase plane, which shows the global stability of bot -free equilibrium point.

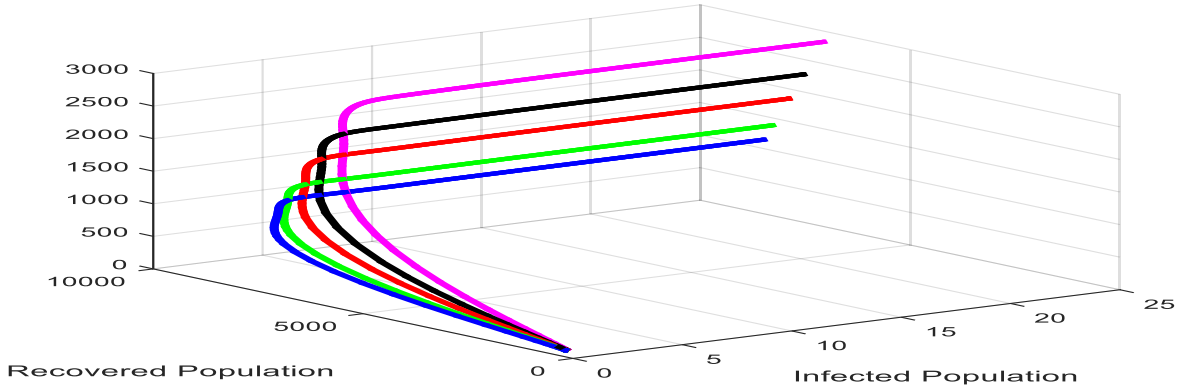

Fig.-3: Infected-recovered phase plane when R_0 < 1.

Example-3: To show the global stability of endemic equilibrium point, when $\boldsymbol{R_0}$ >1, we consider the global dynamics of the infected x-human-infected y-humans plane and try to understand the nature of the trajectory towards the endemic equilibrium point when $\boldsymbol{R_0}$= 1.0270. Consider the system (1) with three initial conditions of different Susceptible humans Sx = 9899, Sx= 9099, Sx = 8099 and Ix = 50, Rx= 10, Sy =999, Iy = 50 and with parametric values as shown in Table 3.

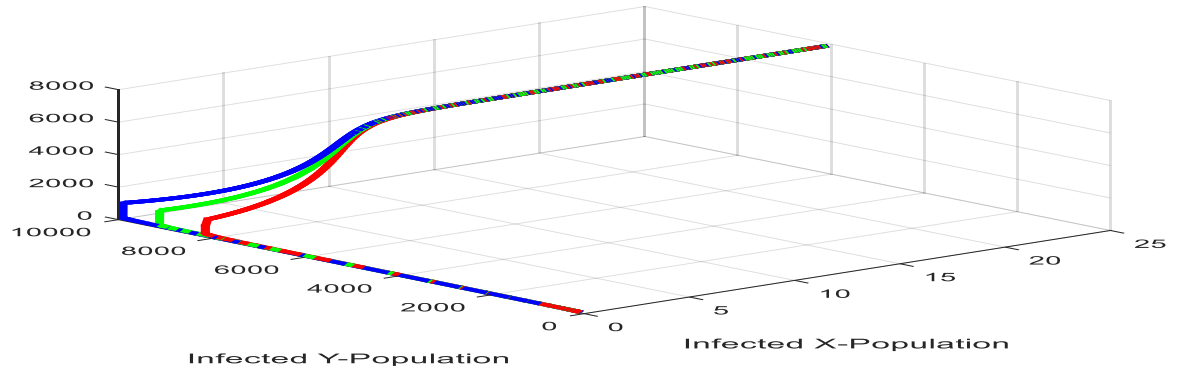

Fig.-4: Infected X-human- infected Y-humans plane when $\boldsymbol{R_0}$ > 1.

Example-4: To compare the numbers of recovered humans with the numbers of infected human when R_0>1, we consider the system (1) with initial conditions Sx=9999, Ix=50, Rx=10, Sy=999, Iy=50 and the parametric values of Table-3. The simulation result is shown in fig.-4. From fig.-4, it is clear that number of recovered human increases for short time period and again becomes susceptible human. Hence the total recovered humans become susceptible and finally total numbers of susceptible humans get infected with bot and the total number of infected human increase to Ix=9999 when R_0= 1.0270>1. From the peak, the infected class decreases because there are no susceptible humans to be infected.

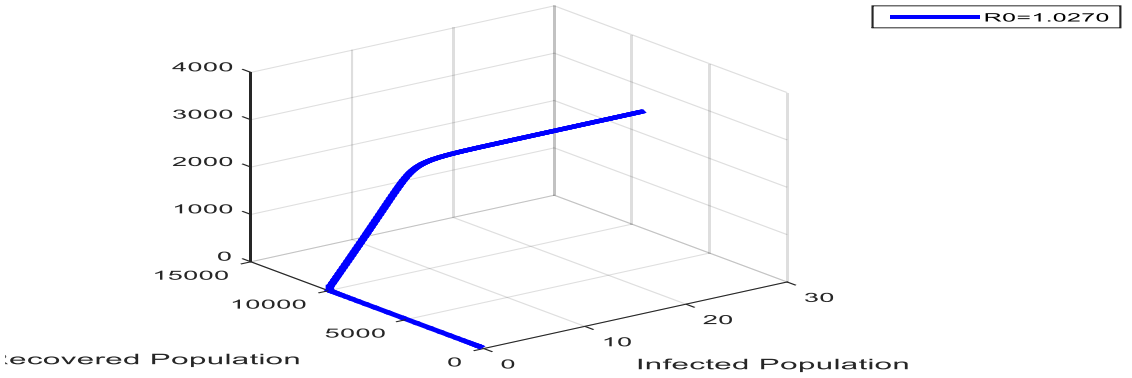

Fig.-5: Comparison between infected and recovered human population when R_0 >1.

Example-5: Consider the system (1) with initial condition Sx = 9999, Ix= 100, Rx = 100, Sy = 999, Iy=100 and the parametric values as shown in Table 2. Figure 5 shows the efficacy of personal protection from the bots, for different values of βx.

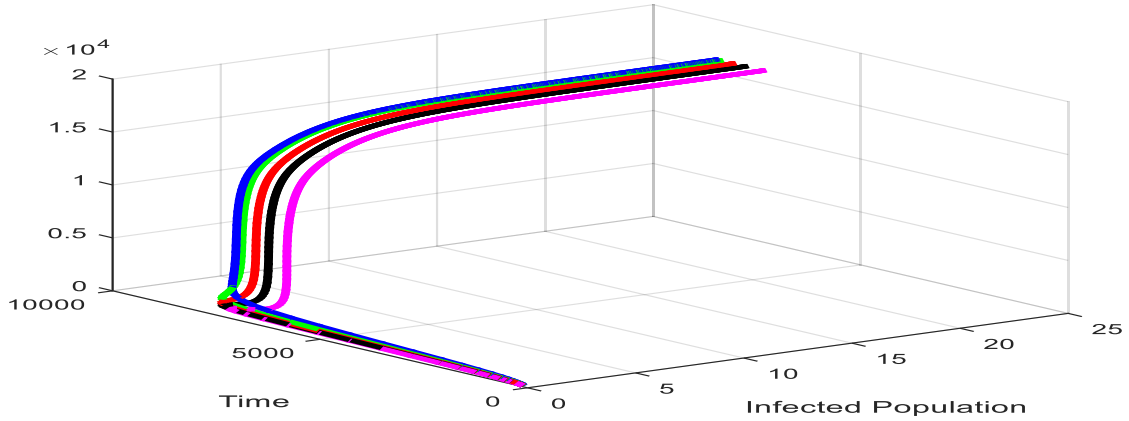

Fig.-6: Efficacy of personal protection of infected humans from bots.

6. Result Analysis

Fig.-2, simulation illustrates the dynamic interactions between normal human users and bot users across five population classes over the time: Susceptible X-humans, Infected X-humans, Recovered Humans, Susceptible Y-humans, and Infected Y-humans. **Fig.-2** graph shows that the susceptible X-human population (green) stabilizes after an initial decline. The infected X-human population (blue) rises quickly and then sharply declines as the population either recovers or transitions to other states. Recovered humans (black) peak early, indicating successful recovery before declining due to the dominating influence of Y-human infection. Susceptible Y-humans (red) start low and remain relatively low throughout, indicating limited replenishment. The infected Y-human population (yellow) exhibits exponential growth, eventually dominating the system and surpassing all other groups. This behavior highlights the aggressive and sustained infection potential of bot users (Y-humans) in comparison to normal users (X-humans), suggesting that once bot infection is introduced, it rapidly overtakes the population unless effective containment or recovery strategies are implemented.

Fig.-3, illustrates the infected-recovered phase plane for various simulations when $R_0 < 1$ (basic reproduction number less than 1). The infected-recovered phase plane shows that the number of infected individuals decreases over time, approaching zero. Meanwhile, the recovered population gradually increases and stabilizes. This behavior indicates that when the basic reproduction number is <1, the bot infection fails to spread widely and eventually dies out. The system converges to a bot infection -free

equilibrium, validating the theoretical prediction that an epidemic cannot sustain itself when $R_0 < 1$.

Fig.-4, clearly demonstrates the influence of the basic reproduction number on the dynamics of infection and recovery in a population. When R_0 >1 the bot infection cannot sustain itself in the population. The infected population decreases over time, leading to a stable endemic equilibrium where the bot infection dies out, as shown in **Fig.-3**. The bot infection spreads rapidly. Initially, the number of recovered individuals increases, but after reaching a peak in the infected population, the bot infection declines due to the depletion of susceptible individuals. **Fig.-4** & **Fig.-5** illustrate this behavior, where bot infection and recovery from bots are directly influenced by the initial number of susceptible individuals and parameter values.

These simulations confirm that a higher leads to a greater peak in infections and faster spread, emphasizing the importance of controlling through intervention strategies such as increasing recovery rate or reducing transmission**.**

Fig.-5, demonstrates the dynamics between bot infected and recovered populations over time when the basic reproduction number (R_0) is slightly > 1 (R_0 = 1.0270). Initially, the number of bot infected individuals rises as the bots spreads. However, due to the recovery process, the number of bot infected individuals eventually declines while the recovered population increases steadily. This indicates that although the bot infection initially spreads (since R_0>1), it eventually stabilizes as more individuals recover, reducing the susceptible pool and slowing transmission. This behavior aligns with epidemic models where R_0 slightly above 1 leads to a manageable outbreak that eventually dies out.

Fig.-6, a 3D plot, illustrates the impact of varying levels of personal protection on the bot infected human population over time. The distinct curves likely represent different protection efficacy rates. As the level of personal protection increases, the infected population is shown to decline more rapidly and peak at lower values. This suggests that personal protection measures (such as cyber security protocols) significantly reduce the spread bots. The graph clearly emphasizes the importance and effectiveness of personal protection strategies in controlling bot propagation dynamics.

7. Summary

Rumor is an unverified piece of information circulating among people, especially without solid evidence and has severe negative impacts on individuals, organizations, and society. It thrives in environments of ambiguity and anxiety, eroding trust, damaging reputations, and creating toxic environments. So there is a need to stop it or ate lest minimize its impact up to level zero. Several models have been deign to control and minimize its impact but are failing in this. This paper after doing study and analysis is proposing a mathematical model with two sets of population named bot users and normal users respectively, and a set of mathematical equations to control the rumors. For this model stability and reliability it's simulating and varying the result using MATLAB and simulation.

References:

1. Claudio Mazzariello; "IRC Traffic Analysis for Botnet Detection", 2008 THE FOURTH NTERNATIONAL CONFERENCE ON INFORMATION**.**
2. Ching-Hsiang Hsu; Chun-Ying Huang etl, "Fast-Flux Bot Detection in Real Time",2010.
3. Jina Lee etl; "I Know What The BOTs Did Yesterday: Full Action Sequence Analysis Using Naïve Bayesian Algorithm", 2013 12TH ANNUAL WORKSHOP ON NETWORK AND SYSTEMS SUPPORT

4. Chun-Ying Huang; "Effective Bot Host Detection Based on Network Failure Models", COM. NET. 2013.
5. Friggeri, A., Adamic, L. A., Eckles, D., & Cheng, J. (2014). Rumor Cascades. In Proceedings of the Eighth International Conference on Weblogs and Social Media (ICWSM 2014).
6. Shui Yu; Song Guo; Ivan Stojmenovic; "Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace", IEEE TRANSACTIONS ON COMPUTERS, 2015
7. Starbird, K. etl. (2016). Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston Marathon bombing. iConference 2016 Proceedings.
8. Ahmad Karim etl, "SMARTbot: A Behavioral Analysis Framework Augmented With Machine Learning To Identify Mobile Botnet Applications", PLOS ONE, 2016.
9. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. Communications of the ACM, 59(7), 96–104. https://doi.org/10.1145/2818717
10. Bessi etl, Social bots distort the 2016 US Presidential election online discussion. First Monday, 21(11).
11. Cresci, S. etl. M. (2017). The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. Proceedings of the 26th International Conference on World Wide Web Companion, 963-972.
12. Varol, O. etl., A. (2017). Online human-bot interactions: Detection, estimation, and characterization. Proceedings of the International AAAI Conference on Web and Social Media (ICWSM).
13. Meisam Eslahi etl, "Correlation-based HTTP Botnet Detection Using Network Communication Histogram Analysis", 2017 IEEE CONFERENCE ON APPLICATION, INFORMATION AND ..., 2017.
14. Mohammad R. Faghani; Uyen T. Nguyen; "Mobile Botnets Meet Social Networks: Design and Analysis of A New Type of Botnet", INTERNATIONAL JOURNAL OF INFORMATION SECURITY, 2018.
15. Sylvio Barbon Junior etl.,"Detection of Human, Legitimate Bot, and Malicious Bot in Online Social Networks Based on Wavelets", ACM TRANSACTIONS ON MULTIMEDIA COMPUTING, COMMUNICATIONS, 2018.
16. Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2018). The spread of fake news by social bots. Nature Communications, 9(1), 1-9.
17. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559
18. Zhang, Xinyu, et al. "A Survey of Bot Detection Techniques." ACM Computing Surveys (CSUR) 53.5 (2020): 1-39.
19. Kollanyi, Bence, Philip N. Howard, and Samuel C. Woolley. "Bots and automation over Twitter during the first US presidential debate." Political Communication 35.4 (2018): 588-591.
20. Jayalath Ekanayake; Saputhanthri Luckshitha; "E-AGRO: Intelligent Chat-Bot. IoT and Artificial Intelligence to Enhance Farming Industry", 2020.
21. Alejandro Acien; Aythami Morales; Julian Fierrez; Ruben Vera-Rodriguez; "BeCAPTCHA-Mouse: Synthetic Mouse Trajectories and Improved Bot Detection", ARXIV-CS.CV, 2020.
22. Ferrara, E. (2020). What types of COVID-19 conspiracies are populated by Twitter bots?
23. M. D. Amala Dhaya etl. "Multi Feature Behavior Approximation Model Based Efficient Botnet Detection to Mitigate Financial Frauds", JOURNAL OF AMBIENT INTELLIGENCE AND

HUMANIZED COMPUTING, 2021
24. Olivier Tsemogne; Y. Hayel; C. Kamhoua; G. Deugoue; "Game-Theoretic Modeling of Cyber Deception Against Epidemic Botnets in Internet of Things", IEEE INTERNET OF THINGS JOURNAL, 2021.
25. O. Taylor etl.; "A Smart System for Detecting Behavioural Botnet Attacks Using Random Forest Classifier with Principal Component Analysis", EUROPEAN JOURNAL OF ARTIFICIAL INTELLIGENCE AND MACHINE , 2022.
26. Ryan Kenny; Baruch Fischhoff; Alex Davis; Kathleen M Carley; Casey Canfield; "Duped By Bots: Why Some Are Better Than Others at Detecting Fake Social Media Personas", HUMAN FACTORS, 2022.
27. Lanjun Wang; Xinran Qiao; Yanwei Xie; Weizhi Nie; Yongdong Zhang; Anan Liu; "My Brother Helps Me: Node Injection Based Adversarial Attack on Social Bot Detection", ARXIV-CS.CR, 2023.
28. Mohd Anul Haq; "DBoTPM: A Deep Neural Network-Based Botnet Prediction Model", ELECTRONICS, 2023.
29. Li M Y etl., 1996, “A geometric approach to global-stability problem”, SIMS J Math Anal 27, pp. 1070-83
30. Mahato, B., & Mishra, B. K. (2018). Global stability analysis on the transmission dynamics of Zika virus. International Journal of Applied Engineering Research, 13(15), 12296–12303.