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

An Expected Utility-based Decision Making Model for Analyzing the Behavior of Agents in a Bio Attack

Alolika Mahanty[1], Nithin PS[2]

[1,2]Student, Amity Institute of Defence Technology, Amity University, Noida.

Abstract

The behavior of agents in a bio attack is a critical factor that influences the outcome of such an event. In this paper, we propose an adaptive dynamic model for analyzing the behavior of agents in a bio attack based on expected utility theory. The model incorporates the environmental factors, agent characteristics, decision-making processes, communication networks, feedback mechanisms, and learning and adaptation processes. Specifically, we present a decision-making model based on expected utility theory to assist agents in choosing the best course of action. The model can help agents assess the risks and benefits associated with different options and choose the action that maximizes their expected utility. We also discuss the potential benefits of incorporating feedback mechanisms and learning processes into the model to improve agents' decision-making over time.

Keywords: Agent, Adaptive Dynamic Model, Utility, Bio-Attack

1. Introduction

The threat of a bio attack has become a significant concern for national security in recent years. In such an event, the behavior of agents involved in the response plays a critical role in the outcome. A bio attack involves complex and dynamic situations that require quick and efficient decision-making. To analyze the behavior of agents in a bio attack, an adaptive dynamic model that incorporates various factors such as environmental factors, agent characteristics, decision-making processes, communication networks, feedback mechanisms, and learning and adaptation processes is needed. In this paper, we focus on the decision-making process and propose an expected utility-based decision-making model to help agents choose the best course of action.

2. Defensive approach

The defensive approach is an adaptive dynamic model for analyzing the behavior of agents in a bio attack scenario. The model is based on the assumption that agents are rational and seek to maximize their utility. The model considers the behavior of three types of agents: attackers, defenders, and the public.

Attackers are individuals or organizations that carry out the bio attack. The attackers seek to achieve their objectives, such as causing harm or death to people, animals, or plants, or disrupting social and economic activities. The attackers may have different objectives, such as making a political statement, seeking revenge, or causing chaos.

Defenders are individuals or organizations responsible for protecting the public against a bio attack. The defenders seek to minimize the impact of the attack and protect the public from harm. The defenders may have different objectives, such as preventing the spread of the biological agent, treating the affected individuals, or restoring social and economic activities.

The public is the group of individuals affected by the bio attack. The public includes individuals who are directly affected, such as those who become ill or die, and those who are indirectly affected, such as those who suffer economic losses or psychological trauma. The behavior of the public can be influenced by various factors, such as the severity of the attack, the response of the authorities, and the perception of risk.

The defensive approach model considers the behavior of these three types of agents and how they interact with each other. The model is adaptive and dynamic, meaning that it takes into account the changing nature of the attack and the response of the agents.

The model consists of four stages: planning, detection, response, and recovery. In the planning stage, the defenders develop strategies and plans to prevent or mitigate the impact of a bio attack. The planning stage includes identifying the potential threats, assessing the vulnerabilities, and developing response plans.

In the detection stage, the defenders use various methods to detect the bio attack, such as surveillance systems, laboratory testing, or public health reports. The detection stage is critical because it allows the defenders to respond quickly and prevent the spread of the biological agent.
In the response stage, the defenders implement the response plans developed in the planning stage. The response stage includes various activities, such as quarantine, isolation, treatment, and decontamination. The response stage is crucial because it determines the effectiveness of the defenders' efforts to mitigate the impact of the bio attack.

In the recovery stage, the defenders focus on restoring normal social and economic activities after the bio attack. The recovery stage includes activities such as clean up and decontamination, restoration of critical infrastructure, and support for affected individuals and businesses.

The defensive approach model considers the behavior of the agents in each stage of the response and how they interact with each other. The model takes into account the rationality of the agents and how they seek to maximize their utility. For example, attackers may seek to modify their behavior based on the response of the defenders, such as changing the location or timing of the attack. Defenders may modify their behavior based on the perceived threat, such as increasing surveillance or deploying additional resources. The public may modify their behavior based on the severity of the attack, such as avoiding public places or seeking medical attention.

The defensive approach model is flexible and can be adapted to different scenarios and contexts. The model can incorporate various factors, such as the nature of the biological agent, the location and timing of the attack, the response of the authorities, and the perception of risk by the public. The model can also be used to evaluate the effectiveness of different strategies and interventions.

3. Methodology

The proposed model for analyzing the behavior of agents in a bio attack incorporates six components: environmental factors, agent characteristics, decision-making processes, communication networks, feedback mechanisms, and learning and adaptation processes. Environmental factors include the type of bio agent, the location of the attack, the weather, and other relevant factors that could impact the behavior of the agents. Agent characteristics include the characteristics of the agents themselves, such as their level of training, their mental state, their level of preparedness, and their previous experience with similar situations. Decision-making processes include the processes by which agents make decisions about how to respond to the attack, including factors such as risk assessment, cost-benefit analysis, and information processing. Communication networks include the communication networks that agents use to share information and coordinate their actions, including formal communication channels, social media, and informal networks. Feedback mechanisms include the feedback mechanisms that agents use to evaluate the success of their actions and adjust their behavior accordingly, including situational awareness, performance metrics, and self-assessment. Learning and adaptation include the ability of agents to learn from their experiences and adapt their behavior in response to changing conditions, including changes in the environment, new information, and feedback from others.

4. Environmental Factors

Environmental factors play a crucial role in shaping the behavior of agents in a bio attack. These factors can include the type of bio agent, the location of the attack, the weather, and other relevant factors that could impact the behavior of the agents. For example, if the bio agent is highly contagious, agents may be more likely to prioritize evacuation and isolation of affected individuals over containment and mitigation. Similarly, the location of the attack can affect the behavior of agents. For example, if the attack occurs in a densely populated urban area, agents may need to prioritize evacuation and containment to prevent the spread of the bio agent.

5. Agent Characteristics

The characteristics of the agents involved in a bio attack can also have a significant impact on their behavior. These characteristics can include their level of training, their mental state, their level of preparedness, and their previous experience with similar situations. For example, agents who have undergone extensive training in responding to bio-terrorism attacks may be better equipped to make effective decisions and respond to changing circumstances. Similarly, agents who are mentally prepared and have experience in high-stress situations may be more resilient and better able to adapt to the demands of a bio attack.

6. Decision-Making Processes

The decision-making processes of agents in a bio attack are critical to the success of their response efforts. These processes can include risk assessment, cost-benefit analysis, and information processing. For example, agents may need to weigh the risks associated with different response options, such as evacuation or containment, and assess the potential costs and benefits of each. They may also need to process large amounts of information quickly and accurately in order to make informed decisions and respond effectively to changing circumstances.

7. Communication Networks

Effective communication networks are essential for coordinating the response efforts of agents in a bio attack. These networks can include formal communication channels, such as radio and telephone systems, as well as informal networks, such as social media and personal contacts. For example, agents may need to quickly communicate information about the location and spread of the bio agent, as well as updates on the status of response efforts, to other agents and stakeholders.

8. Feedback Mechanisms

Feedback mechanisms are important for evaluating the success of response efforts and adjusting behavior accordingly. These mechanisms can include situational awareness, performance metrics, and self-assessment. For example, agents may need to monitor the spread of the bio agent and assess the effectiveness of their response efforts in containing it. They may also need to evaluate their own performance and identify areas for improvement in order to adapt their behavior to changing circumstances.

9. Learning and Adaptation

The ability of agents to learn from their experiences and adapt their behavior in response to changing conditions is critical for effectively responding to a bio attack. This can involve adjusting response strategies, improving decision-making processes, and developing new skills and knowledge. For example, agents may need to develop new strategies for responding to different types of bio agents or learn new techniques for quickly processing and analyzing large amounts of information.

10. Expected Utility-based Decision-making Model

Expected utility theory is a decision-making model that assumes that agents will choose the action that maximizes their expected utility. The expected utility of an action is the sum of the utilities associated with each possible outcome of the action, weighted by the probability of each outcome. The formula for expected utility is:

$$EU(A) = \sum[U(Si) \times P(Si|A)] \quad (1)$$

Where:
EU(A) is the expected utility of action A
U(Si) is the utility of outcome Si
P(Si|A) is the probability of outcome Si given that action A is taken

In the context of a bio attack, the decision-making model could be used to help agents choose the best course of action based on their assessment of the risks and benefits associated with each option. For example, an agent might choose to evacuate a contaminated area if the expected utility of that action is higher than the expected utility of remaining in the area and attempting to contain the outbreak.

11. Conclusion

The proposed expected utility-based decision-making model can be used to analyze the behavior of agents in a bio attack and help them choose the best course of action. By incorporating feedback mechanisms and learning processes, the model can be further improved over time to enhance agents' decision-making. The model can also be used to simulate different scenarios and test response strategies to improve the performance and effectiveness of agents in a bio attack.

12. Reference

1. P. G. Esteban and D. R. Insua, "A Model for an Affective Non-Expensive Utility-Based Decision Agent," in IEEE Transactions on Affective Computing, vol. 10, no. 4, pp. 498-509, 1 Oct.-Dec. 2019, doi: 10.1109/TAFFC.2017.2737979.
2. Ji-Wen Hu, Quan-Jun Yin, Lei Feng and Ya- Bing Zha, "Modeling risk propensity in decision making behavior for CGF agent," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, 2010, pp. 590-594, doi: 10.1109/ICCSIT.2010.5563832.
3. P. G. Esteban and D. R. Insua, "A Model for an Affective Non-Expensive Utility-Based Decision Agent," in IEEE Transactions on Affective Computing, vol. 10, no. 4, pp. 498-509, 1 Oct.-Dec. 2019, doi: 10.1109/TAFFC.2017.2737979.
4. Abrams, P., and Matsuda, H. (1993). Effects of adaptive predatory and anti-predator behaviour in a two-prey-one-predator system. Evol. Ecol. 7, 312–326. doi: 10.1007/BF01237749
5. Wallace R, Geller A, Ogawa VA, editors. Assessing the Use of Agent-Based Models for Tobacco Regulation. Washington (DC): National Academies Press (US); 2015 Jul 17. Appendix A. Available from: https://www.ncbi.nlm.nih.gov/books/NBK305917/