# Game Theory Based Aerial Sensor Deployment and Patrol Planning for Counter-Insurgency Operations

***Prashant Channappa Mural* and Rathna GN*****

*Game theory has been widely applied in security and surveillance scenarios to model the strategic interactions between defenders and attackers. Previous research has shown the potential of game theory in improving security outcomes in various scenarios, including airport security, critical infrastructure protection and wildlife conservation. However, the application of game theory in the context of CI/CT operations in India is unexplored. Using drones in Counter-Insurgency and Counter-Terrorism (CI/CT) operations has become increasingly popular due to their ability to gather intelligence and conduct surveillance in areas that are difficult to access by ground forces. However, the effectiveness of these aerial sensors can be limited by the uncertainty in detecting and signalling the presence of terrorist or insurgent activity.*

*We propose a Patrol Planning System based on historical data and real-time patrolling feedback for optimal patrol routes. We also propose a Mathematical model of the uncertainty of aerial sensors and discuss defender strategies in aerial sensor-supported operations. Finally,*

* Lt Col Prashant Channappa Mural is pursuing MTech in Artificial Intelligence from Indian Institute of Science, Bengaluru, India.

** Dr Rathna GN is a Principal Research Scientist at Indian Institute of Science, Bengaluru, India.

*ISSN 0976-1004 (print); 2583-7567 (online)*

*Journal of Defence Studies, Vol. 17, No. 4, October–December 2023, pp. 195–215*

*the article explores the 'security games with signalling' to propose a Stackelberg Security Games model for CI/CT environment supported by aerial sensors. By integrating signalling and sensor uncertainty, game theory can help in designing effective strategies for sensor placement and signalling to minimise the risk of successful attacks by adversaries in CI/CT environments.*

**Keywords:** *Game Theory, Drones, CI/CT operations, Patrol Planning, Machine Learning, Uncertainty Modelling*

## Introduction

In the current methodology of patrolling within Counter-Insurgency and Counter-Terrorism (CI/CT) operations, the backbone of these efforts primarily consists of human patrollers who conduct both fixed and mobile patrols. These dedicated security personnel, often operating with limited resources, play a crucial role in maintaining security and responding to threats but several factors often constrain their effectiveness. Human patrollers face the challenge of covering vast and diverse terrains, and they often rely on predefined patrol routes and schedules, which can become predictable for adversaries. Furthermore, gathering real-time intelligence and maintaining continuous surveillance across these expansive areas can be resource-intensive and sometimes falls short in countering the adaptive strategies employed by insurgent and terrorist groups. In this context, integrating aerial sensors represents a significant leap forward in improving patrolling within CI/CT operations. Aerial sensors, such as drones and surveillance technology, can expand the patrollers' reach, enabling them to cover larger areas more efficiently. These sensors can provide real-time data and surveillance, enhancing situational awareness and allowing for rapid response to emerging threats. By integrating aerial sensors into patrolling strategies, security forces can optimise patrol routes, adapt their approach in real-time, and minimise vulnerabilities and predictability, ultimately bolstering their efforts in safeguarding critical areas in the face of evolving threats.

In India's complex and diverse landscape, counter-terrorism and counter-insurgency operations are a constant challenge. The dynamic and evolving nature of terrorist groups operating within the country demands a nuanced understanding of their behaviour. In addressing the question, 'Do terrorists follow a pattern?' it is evident that these groups may initiate their activities with identifiable patterns, often referred to as their initial strategies against the deployment of security forces. However, it is essential to recognise that these

patterns are not set in stone. As security forces adapt their defences and discern these patterns, terrorist groups, in turn, adjust their strategies to maintain their operational effectiveness. This continuous process of interaction and evolution underscores the need for a comprehensive and adaptable framework for analysing and responding to these changing dynamics, a need fulfilled by the Stackelberg Security Game model. The Stackelberg Security Game Model is a mathematical framework used in game theory to analyse and optimise the strategic interactions between two players: a 'leader' and a 'follower' in security and defence. It is commonly applied to situations where a defender (the leader) makes strategic decisions before an attacker (the follower) makes their move. The model is named after the German economist Heinrich von Stackelberg, who introduced it in the 1930s.

In the context of security and defence, the Stackelberg Security Game Model can address issues such as resource allocation, patrolling, and surveillance. The leader, typically representing the defender or security forces, commits to a strategy first, knowing that the follower (representing an adversary or attacker) will respond strategically based on the leader's actions. The objective is to find the leader's strategy that maximises their security while considering the follower's potential counter-strategies. This model is beneficial for situations where security decisions can influence the behaviour of adversaries. By modelling these interactions mathematically, the Stackelberg Security Game Model provides a structured approach to making decisions that can optimise security measures, deter adversaries, and adapt to changing threats. In the context of CI/CT operations, while terrorists may initially follow patterns in their strategies, it would be naive to assume that they will continue to do so as security forces adapt and discern these patterns. The continual evolution of the interaction between both parties underscores the need for a sophisticated and adaptable framework, such as the Stackelberg Security Game model, to analyse and respond to the changing dynamics effectively. This approach considers the evolving strategies of both terrorist groups and security forces, making it a valuable tool for counter-terrorism and counter-insurgency efforts in the Indian context.

In the realm of Counter-Insurgency and Counter-Terrorism (CI/CT) operations, integrating advanced technologies, such as drones and human patrollers, is increasingly crucial for maintaining security and outmanoeuvering adaptive adversaries. We propose a Stackelberg security game with a signalling model to effectively employ aerial sensors capable of signalling the attacker. Signalling is incorporated to drive the attacker's decision-making to compel him to behave in a certain way. This model represents

a groundbreaking approach that leverages the principles of game theory to enhance the coordination and efficacy of drone and human patroller teams in CI/CT operations. In this framework, aerial sensors, including drones, are not limited to mere data collection; instead, they become strategic assets capable of signalling information that can influence the actions of both sides. By employing game theory, security forces can develop a dynamic strategy that accounts for the human patrollers' signalling and counter-signalling actions and the adversaries' adaptability. We also propose optimising resource allocation, patrols, and surveillance activities by considering the interplay of signals, responses, and strategic decisions. It provides a structured approach to security management, which adapts to the constantly changing CI/CT environment, ultimately offering security forces a competitive edge in countering threats and safeguarding critical areas effectively.

Brown, Carlyle and Wood introduced the Stackelberg security game with signalling, which has since been used to improve security outcomes in various scenarios. Signalling aims to inform the adversary about the defender's actions or intentions. In aerial sensor deployment, signalling can indicate the presence of sensors and patrollers. Signalling can deter adversaries from attacking, increase the probability of detecting an attack, and inform the defender of the adversary's intentions. We will use this model to strategically deploy aerial sensors, human patrollers, and warning signals to ward off adversaries. This article is structured as follows:

1. Reviewing previous research on game theoretic applications in security and surveillance scenarios.
2. Presenting a conceptual framework for employing game theory in aerial sensor deployment for CI/CT operations.
3. Discussing this approach's potential challenges and limitations and suggest future research directions.

## Previous Research

Previous research has demonstrated the potential of game theory in various security and surveillance scenarios. Alderson et al. used game theory to solve defender-attacker-defender models for infrastructure defence.[1] Basilico, De Nittis and Gatti proposed a security game model for environmental protection in the presence of an alarm system.[2] The model was used to improve conservation outcomes in a wildlife conservation scenario. In a subsequent study, Basilico et al. proposed a security game that combined patrolling and alarm-triggered responses under spatial and detection uncertainties.[3] The

model was used to improve security outcomes in a maritime environment. In the context of CI/CT operations, game theory has been used to analyse the behaviour of terrorists and predict their actions. For example, Enders and Sandler used game theory to model the behaviour of terrorists in terms of target selection, the timing of attacks, and the type of weapons used.[4] The study found that terrorists are more likely to attack targets of high symbolic value, such as political or religious institutions. In a recent study, Singh et al. used game theory to analyse the strategic interactions between drones and ground forces in the CI/ CT operations context.[5] The study proposed a game theoretic model that can optimise the coordination between drones and ground forces for maximum efficiency in coverage, response time, and resource allocation.

Other studies have used game theory to improve security outcomes in various contexts. For example, Tambe et al. proposed a security game for allocating police resources to protect ports from potential terrorist attacks.[6] The model was used to allocate police resources dynamically based on the changing threat environment. In a subsequent study, Pita et al. proposed a security game that combined static and dynamic patrolling strategies to improve security outcomes in a transit system.[7] Overall, previous research has demonstrated the potential of game theory to improve security outcomes in various contexts. However, there is a need for further research to explore the application of game theory in deploying aerial sensors for CI/ CT operations in India, given this approach's unique challenges and limitations in this context.

## Patrol Planning with Aerial Sensors

Using computational tools can aid in improving patrol planning and making it more efficient. Xu et al. propose a novel Sensor-Empowered security Game (SEG) model that captures the joint allocation of human patrollers and mobile sensors, which can notify nearby patrollers of potential threats.[8] The paper also highlights the natural functionality of strategic signalling in mobile sensors and presents a scalable algorithm for solving SEGs.

### Conceptual Framework for Aerial Sensor Deployment in CI/CT Operations

The application of game theory in deploying aerial sensors for CI/CT operations involves several factors that must be considered. The following framework provides a broad overview of the primary considerations.

- **Objective:** The primary aim of aerial sensor deployment is to maximise security outcomes while minimising the risk of successful attacks by adversaries. The deployment of sensors must be optimised to provide adequate surveillance and intelligence.
- **Sensor placement:** Sensor placement is a critical factor in the success of aerial sensor deployment. We must place sensors in areas where they can provide maximum coverage and intelligence while minimising the risk of detection by adversaries.
- **Signalling:** Signalling is an essential component of security games with signalling. In aerial sensor deployment, we use signalling to indicate the presence of sensors and patrollers. Signalling can deter adversaries from attacking, increase the probability of detecting an attack, and inform the defender of the adversary's intentions. We must design a signalling strategy to maximise the effectiveness of security forces.
- **Human patrolling:** Human patrolling is an essential complement to aerial sensor deployment. Patrolling can provide additional intelligence and surveillance in areas that are difficult to access by aerial sensors.
- **Technology integration:** Technology integration is a critical factor in the success of aerial sensor deployment. We must optimise integrating different sensor technologies and platforms to provide adequate surveillance and intelligence.
- **Resource constraints:** Resource constraints are a significant factor that must be considered in deploying aerial sensors for CI/CT operations. The deployment of sensors must be optimised to maximise security outcomes while operating within the constraints of available resources. Game theory can be used to optimise the use of available resources.

**Patrol Planning**

Here is a step-by-step method for patrol planning using aerial sensors and game theory in the context of counter-insurgency operations:

- *Identify the area of interest and the operation's objectives*: Before deploying any aerial sensors, it is important to determine the area of interest and the operation's objectives. This will help determine the type and number of sensors required for the mission.
- *Determine the capabilities of the sensors*: Aerial sensors can be equipped with various capabilities, such as high-resolution cameras, thermal imaging, and night vision. Depending on the operation's objectives, the sensor type and capabilities must be selected.

- *Collect and analyse data*: Sensors will collect data from the designated area, which will be analysed using game theory algorithms to determine the area used by insurgents. The identification of a terrorist from a civilian can be made at this stage *by the patrol commander* based on the modus operandi of insurgents. We may also add a function to effectively differentiate between friend (own patrols) and foe (terrorists) at this stage.
- *Optimize patrol routes*: Using the data collected and analysed, the algorithm will optimise the patrol routes for the security personnel. The routes will cover the area used by insurgents and ensure the person can reach the location quickly.
- *Deploy the sensors and personnel*: Once the patrol routes are optimised, aerial sensors and security personnel can be deployed. Aerial sensors will continue collecting data while security personnel patrol the designated areas.
- *Continuously update patrol plan*: As more data is collected, the patrol plan will need to be updated to reflect any changes in the areas of interest or insurgent activity.
- *Evaluate the effectiveness of the plan*: The effectiveness of the patrol plan can be evaluated based on the number of insurgent activities detected and prevented. The patrol plan can be adjusted if necessary to improve its effectiveness.

Using aerial sensors and game theory algorithms, the patrol plan can be optimised to detect and prevent insurgent activities effectively and efficiently.

**Machine Learning-based Patrol Planning**

To plan patrols in a counter-insurgency operation, historical data is crucial to understand the patterns and behaviour of the insurgents. This historical data can be used to train a machine learning (ML) model to predict the likelihood of an attack occurring in a particular area. The ML model can be combined with game theory to create a Stackelberg Security Game between the security forces and insurgents. The security forces plan their patrols based on the ML model's predictions, while the insurgents react to the security forces' movements.

Gholami et al. present a data-driven predictive model for wildlife protection that accounts for imperfect crime information and uncertainty in wildlife data, which can serve as a valuable reference for developing patrol planning algorithms in the context of CI/CT operations.[9] The study by Xu

et al. presents an end-to-end approach for anti-poaching patrol planning, which can be applied to other security domains such as critical infrastructure and counter-terrorism.[10] The study addresses the challenge of uncertainty in historical data and proposes a data-driven approach that accounts for predictive uncertainty to improve the robustness of patrol plans. The proposed methodology was successfully applied in real-world scenarios and resulted in a significant increase in poaching detection. The study uses these studies to highlight the potential of ML and data-driven approaches in enhancing the effectiveness of patrols for protecting critical assets and combating security threats.

In addition to the ML model, other features such as geographical information system (GIS) data, terrain, demography, and the sentiment of the local population can be incorporated into the patrol planning process. These features can be used to identify high-risk areas and to plan patrol routes that cover these areas. The patrol plan generated using the ML model and the game theoretic approach can be continuously updated based on historical and real-time patrol data. This allows the algorithm to learn from its performance and adjust its optimal strategy. Therefore, combining ML and game theory allows for a more efficient and effective patrol planning process to adapt to real-time changing circumstances. By incorporating historical data, real-time data, and relevant features, this approach can help prevent insurgent attacks and save lives.

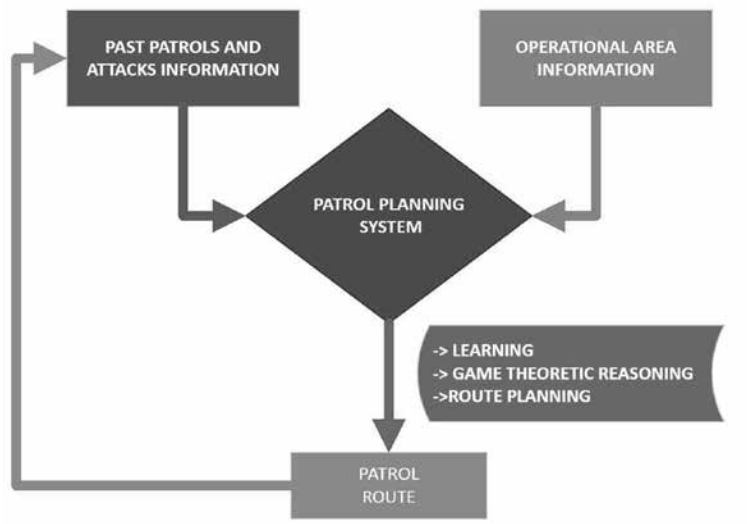


**Figure 1** Proposed Patrol Planning System

**Patrol Planning Algorithm**

The following steps outline broad guidelines for CI/CT patrolling algorithm:

1. *Collect and input the past and terrain data:*
   - Past patrolling and terrorist attack information
   - Inputs from past patrol commanders
   - Geospatial information (feasible routes filtering)
   - Information on key infrastructure, population centers, and areas of strategic importance
2. *Generate an optimized patrol route by*:
   - Using game theoretical reasoning to identify the area most vulnerable to attack and prioritise patrolling in these areas.
   - Considering the time and distance required to complete the patrol route.
   - Ensuring that patrol routes are varied and unpredictable to prevent potential attackers from predicting patrol patterns.
   - Incorporating data collected by patrollers into the algorithm to improve the route over time.
3. *Deploy patrollers*:
   - Assigning patrollers to specific routes and providing them with necessary equipment and resources.
   - Ensuring patrollers are well-trained and equipped to handle potential threats.
   - Monitoring the progress of patrollers in real-time using GPS or other tracking technologies.
4. *Data Collection and Analysis:*
   - Collecting data from patrollers on any potential security threats, including suspicious activities or individuals, unauthorised entry into restricted areas, and other security breaches.
   - Feeding collected data back into the patrol planning algorithm to optimise future patrol routes and improve overall effectiveness.
5. *Continuous improvement:*
   - Regularly reviewing and analysing the effectiveness of patrol routes and adjusting the algorithm as necessary to improve results.
   - Incorporating new data and information as it becomes available to enhance patrol planning and deployment strategies.

In the context of CI/CT operations, game theory-based aerial sensor deployment can be utilised to create a proactive patrol plan. But when integrated with AI/ML models, it can provide a significant advantage in

promptly identifying and responding to potential threats by analysing historical data and designing proactive patrols. Additionally, by using unmanned aerial vehicles (UAVs) equipped with sensors, the patrol plan can be designed to cover a larger area than what is possible with ground patrols alone. This technology can help track insurgents' movements and detect activities of interest. The use of aerial technology in patrol planning can enhance the effectiveness and efficiency of CI/CT operations.

**Practical Challenges**

In CI/ CT operations context, several practical challenges must be addressed while coordinating aerial sensors and patrols. One practical constraint is the need to consider mountaintops as key points in the patrol route. This is because patrollers may be required to go downhill for a short distance before backtracking, which can be annoying and discourage them from following the suggested patrol route. To address this problem, mountaintops are considered key attack points (KAPs) when building a street map. This ensures that patrollers are not forced to take the short downhill unless necessary. Another practical constraint is the limit on working time and walking distance. Patrollers must record their observations, including human activity and tell-tale signs. If they walk along the same ridgeline twice daily, they only need to record the signs once. Therefore, the total working time and distance must be considered when designing patrol routes.

Furthermore, not all terrain features should be treated equally. Some terrain features, such as ridgelines, should be given priority in the patrol route design. The importance given to terrain features should depend on the cost of alternative routes and how much easier they are compared to other routes. In a hilly region with significant elevation changes, patrollers prefer terrain features as they are much easier to walk along than an alternative route. In contrast, if the elevation change in the region is small, the effort of taking a ridgeline for a unit distance is comparable to that of taking an alternative route. Secondary derivatives can be used to differentiate between these cases to check how vital the ridgeline is.

Lastly, additional factors such as slope must be considered when evaluating the walking effort. While the distance measure introduced previously considers elevation change and terrain features, other factors, such as slope, contribute to the walking effort. Therefore, walking along the hillside of a steep slope should be penalised more than walking on flat terrain. This can be achieved by assigning a higher penalty factor for a higher slope.

**Things to Remember for Technical Team Designing the Algorithm**

The technical team designing the algorithm for optimal patrolling strategy should/must remember several practical aspects mentioned earlier.

- It is crucial to have first-hand immersion in the security environment of concern to understand the context and accelerate the development process.
- The employment of aerial sensors should be seen in the backdrop of various electronic and physical threats to drones to ensure their reliability in the operational environment.
- The identification of a friend or foe by the aerial sensor is a crucial aspect that needs to be coordinated with the operational commanders coordinating the CI/ CT operations.
- The team should/must consider intentionally going for patrols in the relevant area to familiarise themselves with the terrain and better understand the importance of factors such as ridgelines and elevation changes.
- Visualising the solution is essential for effective communication and technology adaptation. The team should/must visualise the game-theoretic strategy generated by the algorithm and provide visualising information for human planners, including difficulty level for patrol, probability of finding insurgents/terrorists and elevation changes along the route. This information can help planners understand the strategy and assign patrol routes to the right team of patrollers.

Finally, the team should/ must aim to minimise the need for extra equipment/effort by integrating patrol routes into existing software used for data collection in patrolling areas.

By keeping these lessons in mind, the technical team can develop a practical algorithm for optimal patrolling strategy in CI/CT operations.

## Game Modelling

The Stackelberg security games with a signalling model involve the following stages:

- **Stage 1.** Defender chooses security investments.
- **Stage 2.** The adversary observes the defender's investments and decides whether to attack.
- **Stage 3.** Nature determines whether the attack is successful.

- **Stage 4** (Optional). The signalling stage is an optional fourth stage. During the signalling stage, the defender can choose to signal the adversary about the presence of security investments. Signalling aims to deter the adversary from attacking or increase the probability of detecting an attack.

**Stackelberg Security Game Modelling**

A Stackelberg security games model has two types of players: the leader and the followers. The leader (defender) acts first and selects a strategy, which the followers (adversaries) observe. The followers then choose their strategies in response to the leader's plan. The defender's goal is to optimise their approach given the adversaries' reaction, while the adversaries' goal is to optimise their strategy given the defender's response. In CI/CT operations, the defender could be the security force responsible for protecting their area of responsibility from any terror attacks. At the same time, the adversaries could be terrorists who seek to disrupt or damage the area's security. We propose the following steps to fit a Stackelberg security games model to the CI/CT problem:

- *Identify the objectives of the defender and the adversaries*: The defender's goal could be to minimise the probability of an attack on the critical infrastructure, while the adversary's objective could be to maximise the expected payoff from their attack.
- *Define the strategies available to the defender and the adversaries*: The defender could select a strategy that involves deploying security resources (for example, surveillance equipment and personnel) to protect the infrastructure. The adversaries could choose a plan to attack the infrastructure at a particular time and location.
- *Estimate the probabilities of different outcomes*: The probabilities of various outcomes (for example, successful attack, unsuccessful attack, successful defence) can be estimated using historical data, expert opinion, or simulation.
- *Determine the best response strategies*: The defender can use optimisation techniques to determine the best response strategies given the responses of the adversaries. The adversaries can similarly determine the best attack strategies given the defender's responses.
- *Analyse the equilibrium*: The game combines strategies where neither the defender nor the adversaries can improve their outcomes by unilaterally changing their strategy. The equilibrium can be analysed using

mathematical techniques such as linear programming, mixed-integer programming, or game theory algorithms.

Fitting a Stackelberg security games model to the CI/CT problem can help security forces optimise resource deployment and anticipate potential attackers' actions.

**Stackelberg Security Game with Signalling Model**

The security forces act as the defenders in a security game played in a CI/CT environment against terrorists operating as attackers. Let us assume that the defender can allocate k teams of security personnel and l surveillance systems, such as CCTV cameras and drones, to various locations in the CI/CT environment, which a graph can represent. The defender's objective is to protect critical areas and prevent terrorist attacks, while the attacker aims to carry out successful attacks. The defender/attacker (d/a) utility is represented by U± (i) when the defender successfully protects/fails to protect (±) the targeted location i. By convention, the utility is positive if the defender protects and negative if the defender fails. The utility is also negative if the attacker succeeds in the attack and positive if the attacker fails.

Surveillance systems like CCTV cameras and drones can help detect and deter terrorist attacks. They can monitor critical locations and notify nearby security personnel to respond and prevent the attacker. Based on the presence or absence of security personnel or surveillance systems and the strength of the signal they emit, the attacker can encounter *different signalling states* as follows:

(a) Immediate capture by security personnel;
(b) Nothing (state n);
(c) A surveillance system with a weak signal (state $\sigma 0$);
(d) A surveillance system with a strong signal (state $\sigma 1$).

The final set of signalling states an attacker may encounter is $\Omega = \{n, \sigma 0, \sigma 1\}$. The defender's task is to allocate available resources, including security personnel and surveillance systems, to various locations in the operational environment to minimise the probability of a successful terrorist attack. The attacker's task is to choose the place to attack based on the information available about the defender's resource allocation and signalling state. The game can be solved using a Stackelberg equilibrium, where the defender acts as the leader, and the attacker acts as the follower.

**Modelling Uncertainty in CI/CT Operations**

Uncertainty is inherent in any CI/CT operation and can pose significant challenges to security personnel. Uncertainty can arise from various sources, including limitations in sensor capability and observational uncertainty. There are two prominent types of uncertainties, which are as follows:

- *Detectional Uncertainty:* One prominent uncertainty is detection uncertainty, where the sensor's capability is limited, leading to incorrect detection due to the inaccuracy of image detection techniques.[11] Inaccurate detections, either false negatives or false positives, can significantly impact the success of an operation. In this context, false negatives are more critical since they can go undetected and compromise the operation's effectiveness. Therefore, modelling and quantifying any sensor's false negative rate ($\gamma$) in CI/CT operations is essential.
- *Observational uncertainty:* This is another type that might affect the credibility of information in an operation. It arises when the actual signalling state of a target differs from the observer's perception. For example, an observer may be unable to detect a particular signal due to signal masking or other environmental factors. Observational uncertainty can arise in CI/CT operations when security personnel use signalling schemes that are not detectable by the terrorist. To quantify observational uncertainty, we can use an uncertainty matrix $\Pi$ that contains the conditional probability $Pr[\hat{\omega}|\omega]$ (read as 'probability of an attacker observing the state $\hat{\omega}$ given that the drone signalled $\omega$) for all $\hat{\omega}, \omega \in \Omega$. Here, $\hat{\omega}$ denotes the observed signalling state of the attacker, and $\omega$ denotes the actual signalling state based on the defender signalling scheme.

The article by Bondi et al. proposes a novel game model for integrating signalling and sensor uncertainty in the context of security games with drones.[12] The authors show that ignoring real-world uncertainties can lead to significant losses for defenders, even with carefully planned strategies. However, they demonstrate that defenders can perform well by exploiting uncertain real-time information through a signalling scheme designed to mislead the attacker. The proposed algorithm and experimental results from their ongoing deployment of a conservation drone system in South Africa provide valuable insights for handling uncertainties in critical infrastructure and counter-terrorism operations. In summary, modelling and quantifying uncertainties in CI/CT operations are crucial for effectively implementing security measures. Detection and observational

uncertainties are two prominent sources of uncertainty that must be accounted for when designing and implementing CI/CT operations. By using uncertainty models, security personnel can make informed decisions and take appropriate actions to reduce uncertainty and increase the chances of success in CI/CT operations.

**Representing Observational Uncertainty in CI/CT Operations**

Observational uncertainty is a critical factor that must be considered in CI/CT operations. The paper by Bondi et al. proposes to represent observational uncertainty in the conservation domain.[13] The uncertainty matrix Π is used to capture the conditional probability $Pr[\omega\hat{}|\omega]$ for all $\omega\hat{}$, $\omega \in \Omega$, where $\omega\hat{}$ denotes the attacker's observed signaling state, and $\omega$ denotes the true signaling state based on the defender signaling scheme. To simplify the uncertainty matrix, we assume logically that a weak signal will never be observed as strong, and the signaling state without any resource ($n$) will never be observed as strong or weak. This leads to a reduced uncertainty matrix $\prod$ that is parameterized by $\kappa$, $\lambda$, and $\mu$, where:

1. $\kappa = Pr[n|\sigma_0]$ (probability of observing state 'nothing' when drone sent a 'weak signal')
2. $\lambda = Pr[n|\sigma_1]$ (probability of observing state 'nothing' when drone sent a 'strong signal')
3. $\mu = Pr[\sigma_0|\sigma_1]$ (probability of observing 'weak signal' when drone sent a 'strong signal')

$$\Pi = \begin{bmatrix} Pr[n|n] = 1 & Pr[\sigma_0|n] = 0 & Pr[\sigma_1|n] = 0 \\ Pr[n|\sigma_0] = \kappa & (1-\kappa) & Pr[\sigma_1|\sigma_0] = 0 \\ Pr[n|\sigma_1] = \lambda & Pr[\sigma_0|\sigma_1] = \mu & (1-\lambda-\mu) \end{bmatrix}$$

*Note*: *Matrix represents the various possible probabilities of uncertainty in signalling. Read the matrix with signal states 'nothing', 'weak' and 'strong' signal states along both rows and columns. It covers all the permutation probabilities of each state. The total probabilities along the rows add up to 1.*[14]

The uncertainty in the observational state can lead to unexpected terrorist behaviour. For example, if the terrorist is in thick vegetation and has difficulty seeing the strong signal, they may choose to attack only when there is no drone rather than attacking a weak signal. To represent this behaviour, we use a vector $\eta \in \{0,1\}^3$, where $\eta_i$ represents the attacker's behavior for each observation $\{n, \sigma_0, \sigma_1\} \in \Omega$. A value of 1 in $\eta_i$ indicates that the attacker will

attack no matter what signalling state is observed, while a value of 0 indicates that the attacker will never attack.

**Reaction Stage**

The Reaction Stage is a crucial part of the strategy for dealing with uncertainty in CI/CT operations. Below are the main points discussed in this section:

- It is a way for the defender to respond or adjust their strategy based on what is happening in the field.
- It occurs after the defender has committed to a mixed strategy and executed a pure strategy allocation and after the attacker has selected a target to attack.
- Sensors come into play at this stage, detecting the attacker with some uncertainty, and signalling the defender based on a predetermined scheme.
- Based on this information, the defender can re-allocate patrollers to check on particularly uncertain sensors or previously unprotected targets.
- If a sensor detects the attacker, nearby patrollers will go to that target, and the game ends. If no sensors or patrollers detect the attacker, they move to another target to check for the attacker.
- Finally, the attacker observes the signal with some level of uncertainty and chooses whether to continue the attack or run away.

By being prepared to respond and adjust their strategies based on what is happening in the field, the defender can improve their chances of success and protect their areas of responsibility more effectively in CI/CT operations.

## Defender Strategies

In CI/CT operations, the defender's primary objective is to deny the attacker's freedom of movement and to gather intelligence about their movements and intentions. The Defender Strategy focuses on randomised resource allocation, reallocation, and signalling. The methodology of patrolling in CI/CT operations involves a grid-based deployment, with one company operating base covering a specific section of the geographical area. The layout of the operations starts from infiltrating an insurgent to hinterland operations.

A deterministic resource allocation and reallocation strategy for the patrollers and sensors consists of allocating them to $k$ and $l$ targets, respectively, and designating a neighbouring target to which each patroller moves if no attackers are observed. Reallocation can also be considered by matching

each patroller's original target to a neighbouring one. A patroller goes to the matched target only if the attacker is not observed and may respond to any nearby sensor detection, regardless of matching. In our context, the pure strategy must represent not only if the target is assigned a patroller, nothing, or a sensor but also the allocation in neighbouring targets. Bondi et al. propose pure strategy of a defender which can be encoded via six allocation states for each target.[15] In this framework, a target can either be assigned a patroller ($p$), nothing ($n$), or a sensor ($s$). If there is no patroller near a sensor ($\overline{s}$), then no one can respond to the sensor's detection. If a nearby patroller exists, the target is either matched ($n^+$, $s^+$) or not matched ($n^-$, $s^-$). For example, a target in-state $n^+$ was initially not allocated a patroller or sensor. Still, in the reaction stage, a patroller from a neighbouring target could respond and match with the target. By compactly encoding the possible allocation states for each target, security forces can optimise their resource allocation strategies for CI/CT operations. This pure strategy can be encoded via six allocation states for each target, denoted by $\Theta = \{p, n^+, n^-, \overline{s}, s^+, s^-\}$ (Refer Figure). For example, $n^+$ is the state of a target that was not allocated a patroller or sensor but, in the reaction stage, has a patroller from a neighbouring target ('patroller matched').

Table 1. Various Allocation States of a Target

| | **Covered By:** | **Near Patroller?** | **Patroller Matched?** | **Protected Overall?** |
|---|---|---|---|---|
| P | Patroller | N/A | N/A | Yes |
| n+ | Nothing | Yes | Yes | Yes |
| n- | Nothing | N/A | No | No |
| s | Sensor | No | N/A | No |
| s- | Sensor | Yes | No | Yes* |
| s+ | Sensor | Yes | Yes | Yes |

*Source*: E. Bondi, H. Oh, H. Xu, F. Fang, B. Dilkina and M. Tambe, 'To Signal or Not To Signal: Exploiting Uncertain Real-Time Information in Signaling Games for Security and Sustainability', in AAAI Conference on Artificial Intelligence, 2020.

- *Defender Pure Strategy:* The pure defender strategy involves allocating the patrollers and sensors to various targets and matching neighbouring targets based on the observed attacks. The strategy aims to deny the attackers freedom of movement while optimising the use of available resources. The security forces can deploy patrolling teams and sensors

along the border, road networks, and other approaches of insurgents to detect and deter any suspicious movement.

- *Resource Allocation and Reallocation:* The security forces can allocate resources such as patrollers and sensors to various targets based on threat perception and intelligence inputs. The resources can be reallocated to neighbouring targets based on the observed attacks or movement of the attackers. The security forces can use the terrain, weather conditions, and available technology to optimise resource allocation and reallocation.
- *Compact Encoding of Pure Strategy:* The security forces can use a compact encoding method to represent pure strategy, like the six possible allocation states mentioned previously in the article. The encoding can represent whether a target is assigned a patroller ($p$), a sensor ($s$) or nothing ($n$) and the allocation in neighbouring targets. Encoding can help optimise available resources and efficiently deploy patrolling teams and sensors.
- *Feasible Allocation State:* Security forces can define feasible allocation state vectors corresponding to the defender's pure strategies. Not all vectors in the allocation state are feasible, and the security forces must consider the limited number of patrollers and sensors while devising the strategy.
- *Defender Mixed Strategy:* The defender mixed strategy involves a distribution over feasible allocation state vector. The security forces can use a mixed strategy to optimise the use of available resources and adapt to changing attack patterns. The mixed strategy can be represented by a marginal probability vector, like the coverage vector used in basic Stackelberg Security Games with schedules.
- *Signalling Strategy:* The security forces can deploy a signalling process for each target to gather intelligence about the attackers' movements and intentions. The signalling strategy can be specified by probabilities of sending signals together with the allocation state. The signals can be sent based on or without the detection of attackers.
- *Joint Probability of Allocation State and Signal:* Security forces can use the joint probability of allocation state and signal to devise an optimal defender strategy. The joint probability can result in linear terms and help optimise the use of available resources and efficiently deploy patrolling teams and sensors.
- *Valid Signalling Strategy:* The security forces must ensure that the joint probability of the allocation state and signal lies between 0 and the marginal probability of the allocation state to get a valid signalling

strategy. The signalling strategy must be optimised to gather intelligence while minimising the risk of detection by attackers.

- *Joint Probability for Signalling without Detection:* Security forces must add the option to signal without detecting the attacker due to detection uncertainty. The joint probability of allocation state and signal can help devise an optimal strategy to gather intelligence with detection and observational uncertainty.
- *Defender Deployment Strategy:* The defender deployment strategy encompasses the allocation, reaction, and signalling scheme. Security forces can use the deployment strategy to optimise the use of available resources and adapt to changing attack patterns. The deployment strategy can be modified based on threat perception and intelligence inputs. The security forces can deploy patrolling teams and sensors in their respective areas of responsibility based on the finalised deployment strategy.

## Conclusion

In conclusion, the proposed conceptual framework for employing game theory in aerial sensor deployment for CI/CT operations in India has the potential to enhance the effectiveness of surveillance and counter-insurgency efforts in the country. Integrating signalling and sensor uncertainty into the game modelling can provide strategic insights into sensor placement and signalling, thereby reducing the risk of successful attacks by adversaries. By considering the uncertain nature of the environment, game theory can help in designing effective strategies for surveillance and counter-insurgency operations in CI/CT environments. Moreover, previous research has demonstrated the effectiveness of game theory in enhancing security outcomes in various domains. The proposed framework builds upon the existing literature on game theory and extends it to the context of CI/CT operations in India, which has been unexplored. However, implementing the proposed framework poses several practical challenges, including technical issues with deploying aerial sensors and the need for adequate training for patrollers and operators.

Overall, the proposed conceptual framework offers a promising avenue for future research in enhancing the effectiveness of CI/CT operations in India. Integrating game theory with aerial sensor deployment and surveillance can provide novel insights into security and counter-insurgency operations. The proposed framework can be further refined and tested through empirical studies and field experiments to assess its effectiveness in real-world CI/CT

environments. With these efforts, the proposed framework can improve the safety and security of India's citizens and infrastructure in CI/CT environments.

## Notes

1. D.L. Alderson, G. Brown, W.M. Carlyle, A.M. Giani, C.A. Phillips, and G.W. Taylor, 'Game Theory and Infrastructure Defense: A Preliminary Analysis', *Journal of Defense Modeling and Simulation*, Vol. 8, No. 1, 2011, pp. 5–27.
2. N. Basilico, G. De Nittis and N. Gatti, 'A Security Game Model for Environmental Protection', in Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence, IEEE, 2015, pp. 2354–2361.
3. N. Basilico, G. De Nittis and N. Gatti, 'A Security Game Combining Patrolling and Alarm-triggered Reactions Under Spatial and Detection Uncertainties', *International Journal of Game Theory*, Vol. 45, No. 3, pp. 639–675.
4. W. Enders and T. Sandler, 'Is Transnational Terrorism Becoming More Threatening? A Time-series Investigation', *Journal of Conflict Resolution*, Vol. 44, No. 3, 2000, pp. 307–332.
5. P. Singh, A. Mahajan and V. Kumar, 'A Game-theoretic Approach to Drone and Ground Forces Coordination for Critical Infrastructure Protection', *Journal of Defense Modeling and Simulation*, Vol. 17, No. 2, 2000, pp. 207–221.
6. M. Tambe, H. Nguyen and A.K. Jain, 'Security Games for Port Security: An International Perspective', *AI Magazine*, Vol. 32, No. 4, 2011, pp. 59–73.
7. J. Pita, R.H. Ordóñez-Hurtado, J. Meseguer and J.M. del Castillo, 'Game-theoretic Models for Security in Urban Transit Systems', in Proceedings of the 13th International Conference on Mobility and Transport for Elderly and Disabled Persons, Springer, 2016, pp. 1–9.
8. H. Xu, K. Wang, P. Vayanos and M. Tambe, 'Strategic Coordination of Human Patrollers and Mobile Sensors with Signaling for Security Games', in Thirty-Second AAAI Conference on Artificial Intelligence, Vol. 32, No. 1, 2018.
9. S. Gholami, S. Mc Carthy, B. Dilkina, A. Plumptre, M. Tambe, M. Driciru, F. Wanyama, A. Rwetsiba, M. Nsubaga, J. Mabonga, T. Okello and E. Enyel, 'Adversary Models Account for Imperfect Crime Data: Forecasting and Planning against Real-world Poachers', in Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18), 2018, pp. 823–831.
10. Lily Xu et al., 'Stay Ahead of Poachers: Illegal Wildlife Poaching Prediction and Patrol Planning Under Uncertainty with Field Test Evaluations (Short Version)', in 2020 IEEE 36th International Conference on Data Engineering (ICDE), pp. 1898–1901, available at https://network-games-muri.engin.umich.edu/wp-content/uploads/sites/439/2021/04/25.2020_icde_xu.pdf.

11. E. Bondi, R. Jain, P. Aggrawal, S. Anand, R. Hannaford, A. Kapoor, J. Piavis, S. Shah, L. Joppa, B. Dilkina and M. Tambe, 'Birdsai: A Dataset for Detection and Tracking in Aerial Thermal Infrared Videos', in IEEE Winter Conference on Applications of Computer Vision (WACV), 2020, available at https://ieeexplore.ieee.org/document/9093284; E. Bondi, F. Fang, M. Hamilton, D. Kar, D. Dmello, J. Choi, R. Hannaford, A. Iyer, L. Joppa, M. Tambe and R. Nevatia, 'Spot Poachers in Action: Augmenting Conservation Drones with Automatic Detection in Near Real Time', in Association for the Advancement of Artificial Intelligence (AAAI), 2018, available at https://www.cais.usc.edu/wp-content/uploads/2017/11/spot-camera-ready.pdf; M.A. Olivares-Mendez, C. Fu, P. Ludivig, T.F. Bissyande, S. Kannan, M. Zurad, A. Annaiyan, H. Voos and P. Campoy, 'Towards an Autonomous Vision-based Unmanned Aerial System Against Wildlife Poachers' Sensors, 2015.
12. E. Bondi, H. Oh, H. Xu, F. Fang, B. Dilkina and M. Tambe, 'To Signal or Not To Signal: Exploiting Uncertain Real-Time Information in Signaling Games for Security and Sustainability', in AAAI Conference on Artificial Intelligence, 2020.
13. Ibid.
14. Ibid.
15. Ibid.