Maritime Smuggling Detection and Mitigation using Risk-Aware Hybrid Robotic Sensor Networks

Nicolas Primeau*, Rami Abielmona*†, Rafael Falcon*† , Emil Petriu*
* School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada
† Research & Engineering Division, Larus Technologies Corporation, Ottawa, Canada
Email: nprim050@uottawa.ca, rami.abielmona@larus.com, rafael.falcon@larus.com, petriu@uottawa.ca

***Abstract*—With the rise of more resourceful unmanned aerial vehicles (UAVs), their inclusion into robotic sensor networks (RSNs) is inevitable. The highly mobile nature of UAVs allows greater monitoring capabilities, making them most suitable for RSNs. Compared to traditional nodes in RSNs, UAVs suffer even more from communication disruptions and energy depletion, must often rapidly determine actions for themselves, and consequently require more autonomy.**

Prior work has been done in wireless sensor network (WSN)/aerial sensor network (ASN) coordination in a few applications such as protecting critical infrastructure, restoring communication between nodes, and healing networks, while other work has been accomplished on using the UAV network for augmenting the monitoring capabilities of WSNs.

We introduce a novel methodology to integrate UAVs into RSNs for monitoring purposes by formulating the problem in the context of a risk management framework (RMF). This methodology allows a more precise risk feature classification and a more efficient task allocation for the ground network by utilizing the monitoring capabilities of the UAVs to informatively warn the RSN of any incoming events.

We also present a fictitious but credible maritime smuggling scenario near the Port of Barcelona based on expert knowledge, and apply the methodology to detect and mitigate maritime smuggling. The network's behaviour is traced throughout the scenario and is repeated with civilian ships to assure that they are not flagged as smugglers. The applied methodology results in a successful classification and mitigation of the smuggling activity.

I. Introduction

Wireless sensor networks (WSNs) have proved themselves useful with many applications in the military, environmental, home, and health domains [1]. They are networks of simple static sensor nodes that forward sensed data to sink nodes. Such networks suffer from communication disruptions due to hardware failures or network reconfigurations, and low resources. Consequently, their lifespans are fundamentally limited by their efficiency. [2].

One extension, the sensor/actuator network (WSAN), adds actuator nodes controlled by the sink node to complete the control loop [3]. WSANs must also confront new issues such as task allocation [4]. A robotic sensor network (RSN) is a network where each node is as simple as a single wireless sensor or as complex as multi-sensor, multi-actuator, highly-mobile robots [2]. Data is often refined within the network before being sent to the sink nodes, if sent at all.

RSNs have proved useful for Risk mitigation applications. [5]–[7] describe a risk management framework (RMF) that determines risky situations by using a fuzzy inference System (FIS) [8] with inputs of carefully selected risk features, then presents MRTA risk-mitigating solutions generated by a multiobjective genetic algorithm to a human operator.

The described RMF uses ground based RSNs. These nodes usually have longer lifespans and are capable of more robust mitigation plans but lack the ability to monitor expansive areas, and the opposite is typically true for their aerial counterparts. There is synergy by combining both. The ability to warn the ground network of any developing risky situations is advantageous since it results in a more efficient MRTA in terms of resource usage and risk mitigation. Hence, a need exists to properly integrate UAVs into RSNs.

Our contributions in this paper are as follows: (1) a methodology to integrate UAVs into RSNs by formulating the problem in the context of risk management is explained; (2) a scenario based on expert knowledge about maritime smuggling is modeled and simulated; (3) An application of the methodology to detect and mitigate maritime smuggling is developed.

The proposed methodology allows the design of a RMF based on a heterogeneous RSN that combines the mitigation capabilities of ground nodes with the monitoring capabilities of aerial nodes. It can be summed up in three steps, similar to those described in [5] and [7]. First, risk features must be determined to identify risky situations. A second set of risk features that can harness the additional data gathered by the aerial nodes is then defined. Finally, a set of risk mitigating actions are defined for the ground network.

The scenario involves maritime smuggling in an environment loosely based on the area near Barcelona, where a bigger vessel rendezvous with three smaller ones to engage in smuggling activities [9], an event typcially refered to as *Coopering*. The scenario is implemented in an agent based simulation with vessel models using the methodology defined in [10]. Finally, the methodology is applied to mitigate the smuggling operation in this scenario.

The paper is structured as follows. Section II presents related works. Section III presents the proposed methodology for risk mitigating heterogeneous RSN/aerial sensor network (ASN). Section IV clarifies the ASN data gathering optimization process. Section V presents the simulation environment and the maritime smuggling scenario. The methodology is applied for this scenario in Section VI, with the results given in Section VII. Finally, a conclusion is given in Section VIII.

II. Related Work

The focal point of this paper is not determining coarse grain anomalous maritime behaviour. Nevertheless, anomaly detection is crucial to the ASN as a triggering event. The authors of [11] use hidden markov models (HMM) to identify maritime pirates, while [12] identifies five features, then use fused sensor data with a bayesian belief network (BBN) to detect illicit activity. The study in [13] optimizes the paths of surveillance assets to gather information on possible anomalous vessels, then use a BBN to identify anomalous behaviour such as piracy and other illicit activities.

Aerial assets in WSNs have seen applications in connectivity restoration [14], localization [15], for more efficient WSAN task allocations [16], in civilian contexts [17], or for critical infrastructure protection (CIP) [18]. Others have used WSNs to help coordinate the aerial assets, such as [19].

Falcon et. al. [5] describes an evolving RMF for WSNs. This RMF forms the basis of the CIP RSN described in [6]. In this framework, nodes capture risk features derived from raw data streams that are then quantitatively assessed. A risk is inferred from these local risk values via a FIS. Risk events are triggered whenever the overall risk of a system unit exceeds a user-defined threshold.

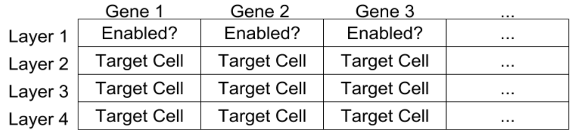
A set of robotic agents in the RSN that are most able to accept a mitigation task in the MRTA process is selected via market-based techniques [20]. The MRTA process is accomplished by a multiobjective evolutionary algorithm that yields a set of Pareto-optimal solutions that describe an allocation of tasks to all or a subset of the agents in the coalition. One of these solutions is then picked by an administrator. Tasks are sent to the proper agents as indicated by the solution that ultimately results in a mitigation of the identified risk.

III. Proposed Methodology

The methodology explains a method to incorporate UAVs into the RMF for RSNs for greater monitoring capabilities that lead to a better situational awareness. Situational awareness is crucial to the RMF as it allows for efficient task allocation and better risk inference. The UAVs allow the system to focus itself on situations that require more analysis.

The first step is to define a set of risk features and a FIS that can detect behaviour that warrants greater attention. These features work at a coarse level so they should try to be characteristic of behaviour that might be risky but not strive to be overly accurate. The purpose of this step is to guide the ASN to focus on certain areas, since it is inefficient to keep track of all of the area of interest (AoI) of the RSN. The process by which the ASN focuses on a certain area is described in Section IV.

The second step is to define risk features that utilize the data gathered by the ASN. These risk features along with another FIS make the final classification of the behaviour as either risky or not. The data set on the tracked ships is updated regularly since they are now being thoroughly monitored by the ASN, which leads to a classification made with the most current data.



	Gene 1	Gene 2	Gene 3	...
Layer 1	Enabled?	Enabled?	Enabled?	...
Layer 2	Target Cell	Target Cell	Target Cell	...
Layer 3	Target Cell	Target Cell	Target Cell	...
Layer 4	Target Cell	Target Cell	Target Cell	...

Fig. 1. Monitoring Task Chromosome

The third step is to define applicable data structures, fitness functions, and operators for the MRTA process so that it can find efficient mitigating task allocations, as done in [7]. Due to the availability of more actionable intelligence on the AoI, a more efficient and optimized MRTA process can take place.

IV. Aerial Network Optimization

The goal of this process is to give monitoring tasks to ASN nodes for certain regions of the AoI. The AoI is divided into a grid where each cells can be monitored by one UAV. A monitoring task is defined as relocating to the center of a specific cell in order to monitor it. The mobility of UAVs can be leveraged by allocating any UAV a sequence of such tasks in order to monitor multiple connected regions.

The MRTA process will utilize the same multiobjective genetic algorithm approach as used in other MRTA processes [7]. As such, proper data structures, operators, and fitness functions must be defined.

Figure 1 presents the chromosome that is used. Each gene corresponds to a UAV and can either be enabled or disabled, determining if the UAV is assigned tasks or not. It has a sequence of cells to monitor for the UAV. A mutation operator for this chromosome is defined as follows.

$$C = \{Cell_{0,0},\ Cell_{0,1},\ ...,\ Cell_{n-1,n-1}\} \tag{1}$$

$$A = \{0, 1\},\ W = f_P(C) \tag{2}$$

Where A is an activation layers, C is the set of all cells in the AoI, W is the set of cells that require monitoring, and f_P is a function yielding the cells that require monitoring. A gene can be described as follows.

$$Gene = \begin{bmatrix} a\ \epsilon\ A \\ w_1\ \epsilon\ C \\ w_2\ \epsilon\ C \\ w_3\ \epsilon\ C \end{bmatrix} \tag{3}$$

Where a waypoint constitutes the center of a cell and a deadline to meet. Too many layers of waypoints constrain the ASN for too long, while less layers result in repeated costly MRTA processes. A limit of three has proved to strike a fair balance between these. The mutation operation can be defined as follows, where Gene' is the mutated gene.

$$Gene^{'} = \begin{bmatrix} P_A \\ P_W \\ P_W \\ P_W \end{bmatrix} \tag{4}$$

$$P_A = \begin{cases} 0.5 & a = 0 \\ 0.5 & a = 1 \end{cases} \tag{5}$$

$$P_W = \begin{cases} 1/|W| & w \mid w \,\epsilon\, W \\ 0 & else \end{cases} \tag{6}$$

The one-point crossover operator is used [21]. Three fitness functions are minimized. The first evaluates the energy needs of the chromosome and is presented in Algorithm 1.

Algorithm 1 Resource Fitness Function

```
Resources ← 0
for each $Gene \mid Gene.a = 1, Gene \,\epsilon\, Chromosome$ do
    Segment$_1$ ← Distance (UAV$_i$, Gene.w$_1$)
    Segment$_2$ ← Distance (Gene.w$_1$, Gene.w$_2$)
    Segment$_3$ ← Distance (Gene.w$_2$, Gene.w$_3$)
    Path ← Segment$_1$ + Segment$_2$ + Segment$_3$
    Resources ← Resources + UAV$_i$.efficiency * Path
end for
Return Resources
```

The second fitness function measures network connectivity and is presented in Algorithm 2. It uses the k-connectivity metric, defined in Algorithm 3 of [22], that measures the number of alternative communication paths around a certain node.

Algorithm 2 Connectivity Fitness Function

```
Redundancy ← 0
for each Cell Layer in Gene do
    for each $Gene|Gene \,\epsilon\, Chromosome$ do
        Metric ← k-redundancy (UAV$_i$, Cell Layer)
        Redundancy ← Redundancy + Metric
    end for
end for
Return -1 * Redundancy
```

The third and final fitness function, Algorithm 3, measures the relevancy of the paths over the projected area of the tracked object. The function f$_P$ returns the cells that are intersected by traveling in a straight line between two points.

V. Experiment Design

An agent-based simulation of a scenario where a smuggling event in an environment loosely based on the coast of Barcelona is used to validate the methodology.

A. Environment Design

The simulation's environment is based on the Port of Barcelona and surrounding areas. Actual location names are used but the scenario is entirely fictitious. Vessel behaviours will be modeled following the methodology defined in [10]. Due to space constraints, brief descriptions of the scenario are presented within this paper.

Algorithm 3 Relevancy Fitness Function

```
Path ← ∅
for each $Gene \mid Gene.a = 1, Gene \,\epsilon\, Chromosome$ do
    S$_1$ ← $\{\ Cell \mid Cell \,\epsilon f_P(C,\ UAV_i,\ Gene_i.w_1)\}$
    S$_2$ ← $\{\ Cell \mid Cell \,\epsilon f_P(C,\ Gene_i.w_1,\ Gene_i.w_2)\}$
    S$_3$ ← $\{\ Cell \mid Cell \,\epsilon f_P(C,\ Gene_i.w_2,\ Gene_i.w_3)\}$
    Path ← $Path \bigcup S_1 \bigcup S_2 \bigcup S_3$
end for
Covered Cells ← $\{\ Cell \mid Cell \,\epsilon\, Path,\ Cell \,\epsilon\, W\}$
Return $-1\ *\ |Covered|\ /\ |W|$
```

The first vessel model is the merchant vessel (MV) that is equipped with an Automatic Identification System (AIS), and is used in commercial enterprises, such as moving cargo or commercial fishing. AIS is used to automatically send identification information and is often used to track ships or to coordinate their movement to avoid conflicts. These systems are mandated by the International Maritime Organization for any qualifying ship. MVs enter at certain points on the perimeter of the environment corresponding to high traffic lanes, head for the industrial port or Port Vell, the civilian section of the Port of Barcelona, and leave after some time has elapsed. A MV may enter a state known as loitering, corresponding to real situations where vessels may loiter due to traffic, breakdowns, waiting for pilotage, etc.

The second vessel model is the ferry. Ferries enter at the same points as MVs and follow similar behaviour, except that Ferries always head to Port Vell instead.

The third vessel model is the large private vessel (LPV) requiring AIS data, such as yachts. LPVs follow approximately the same behaviour as the two previous vessels, however they may enter the environment at any point, and may head to either Port Vell or Port Forùm, a nearby marina.

The small recreational vessel (SRV) is the fourth model and incldue vessels such as speed boats or sailing ships. It is not required to transmit AIS as it does not meet the requiremetns. SRVs depart from either Port Vell, Port Olìmpic, Port Forùm or Marina de Badalona, the last three being local marinas. SRVs depart with higher probability during the day towards one of many predesignated areas, and will switch between these areas until they decide to return to their source port.

The last two models are the smugglers. The smuggling MV is based on the MV, and can enter the a rendez-vous state from the loitering state, but otherwise acts as a normal MV. It waits for smuggling SRVs while in the rendez-vous state. Smuggling SRVs act similarly to SRVs, but head directly for a Smuggling MV from any of the civilian ports, spend some time at the rendez-vous, then head back to a civilian port.

B. Scenario

The proposed methodology is used to detect and mitigate smuggling. Maritime smuggling of weapons, illegal goods [23], or humans [24] is a real problem for ports around the world. A common smuggling tactic involves the use of a bigger vessel to transport the bulk of the smuggled goods, often titled a "Mother Ship", that then meets with smaller vessels for distribution [9]. The meet-up event itself is often referred to as a rendezvous or a coopering event.

The scenario will be as follows: A smuggling MV will arrive near the Port of Barcelona and loiter off the coast, only to rendez-vous with three smuggling SRVs. The MV will then continue towards the industrial port and the SRVs will head towards the Marina de Badalona, Port Olìmpic, and Port Forùm. To gauge the accuracy of the smuggling behaviour classification, this scenario will be repeated with normal SRVs.

VI. Real-World Scenario

The following is an application of the methodology to mitigate maritime smuggling activities based on coopering.

A. Suspicious Behaviour Detection

The first step is to define the risk features that can be used to direct the ASN towards possibly risky situations. The goal is to catch maritime smuggling involving a mother ship that is an AIS enabled by detecting coopering. This rendezvous would warrant additional monitoring but does not necessarily indicate smuggling activity. It could simply be a chance crossing, bunkering, or a tug-operation, to name a few legitimate rendezvous-based activities. The risk features to detect rendezvous are defined as follows.

AIS Off Time (A): This risk feature is defined as $1-e^{-10*t}$, where t is the percentage of time the AIS transceiver perceived to be offline. This feature has the following linguistic terms and membership functions: Small (Trapezoidal: 0, 0, 0.05, 0.15), Moderate (Trapezoidal: 0.1, 0.15, 0.45, 0.6), and Large (Trapezoidal: 0.45, 0.6, 1, 1).

Risk of Departing Port (P): An indicator of the risk of the departing port between 0 and 1 that relies on expert knowledge. Some source ports are known to be less secure than others [9]. This feature has the following linguistic definitions: Low (Trapezoidal: 0, 0, 0.25, 0.5), Medium (Triangle: 0.25, 0.5, 0.75), High (Trapezoidal: 0.5, 0.75, 1, 1).

Distance to Nearest Vessel (D): Normalized distance to the closest vessel measured in the vessel's width, with a maximum of 20 widths. Not all vessels transpond AIS, so the exact position of each vessel is not always known but detecting and tracking targets through data fusion [25] is possible. This feature has the following linguistic definitions: Close (Triangle: 0, 0, 0.5), Medium (Triangle: 0.25, 0.5, 0.75), Far (Triangle: 0.5, 1, 1).

Time of Day (T): The current hour and minutes, normalized between 0 and 1. This feature has the following linguistic definitions: Pre-Dawn (Trapezoidal: 0, 0, 0.15, 0.25), Morning (Trapezoidal: 0.2, 0.25, 0.45, 0.54), Afternoon (Trapezoidal: 0.45, 0.54, 0.7, 0.8), Evening (Trapezoidal: 0.75, 0.8, 1, 1).

Risk (R): The inferred suspicious risk. This feature has the following linguistic definitions: Low (Trapezoidal: 0, 0, 0.25, 0.5), Medium (Triangle: 0.25, 0.5, 0.75) High (Trapezoidal: 0.5, 0.75, 1, 1).

The inference rules are given below, with A Mamdani-type FIS [8].

- If D is Far then Risk Low.
- If T is Morning or Afternoon and D is Close and P is Low and A is Small then R is Low.
- If D is Medium and P is not Low and A is not Small then R is Medium.
- If T is Pre-Dawn or Evening and D is Close and P is Low and A is Small then R is Medium.
- If T is Morning or Afternoon and D is Close and P is not Low and A is not Small then R is Medium.
- If Time of Day is Pre-Dawn or Evening and Distance to Nearest Vessel is Close and Risk of Departing Port is not Low and AIS Off Time is not Small then Risk is High.
- If D is Close and P is High and A is Large then R is High.

B. Smuggling Behaviour Detection

The second step requires the definition of risk features for a more fine-grained assessment. In this context, the ASN is tracking the SRVs that were in rendezvous with the MV. Consequently, additional information is available.

Prior Smuggling Risk (S): This feature is the previously smuggling risk feature, enabling the risk assessment to remember past evaluations. This feature has the following linguistic definitions: Low (Trapezoidal: 0, 0.25, 0.75), Medium (Triangle: 0.25, 0.5, 0.75), High (Triangle: 0.75, 1, 1).

Illumination (I): Normalized estimation of the extracted illumination emanating from a ship, gathered through light source identification analysis with the images of the tracked vessel gathered by the UAVs. This feature has the following linguistic definitions: Poor (Trapezoidal: 0, 0, 0.25, 0.75), Good (Trapezoidal: 0.25, 0.75, 1, 1).

Evasiveness (E): The absolute difference between subsequent a value defined as the average distance of the vessel to other vessels versus the average distance. This is used to capture the behaviour of vessels that are constantly attempting to keep a distance from other vessels. This feature has the following linguistic definitions: Social (Trapezoidal: 0, 0, 0.25, 0.75), Evasive (Triangle: 0.25, 1, 1).

Time of Day (T): The current hour and minutes, normalized between 0 and 1. The linguistic definitions are the same as in the Suspicious Behaviour Detection case.

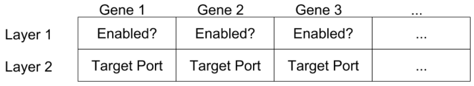
Risk (R): The inferred smuggling risk. This feature has the following linguistic definitions: Low (Trapezoidal: 0, 0, 0.25, 0.5), Medium (Triangle: 0.25, 0.5, 0.75), High (Trapezoidal: 0.5, 0.75, 1, 1).

A Mamdani-type FIS [8] is used again. The inference rules are given below.

- if E is Social and I is Good then R is Low.
- if E is Social and I is Poor and T is Morning or Afternoon and S is Medium then R is Low.

TABLE I
MITIGATING ASSETS

Type	**Cost**	**Risk Mitigation**	**Speed** (m/s)
Police cruiser	1	0.1	20
Police helicopter	10	0.5	70
Coast guard vessel	5	0.25	15



	Gene 1	Gene 2	Gene 3	...
Layer 1	Enabled?	Enabled?	Enabled?	...
Layer 2	Target Port	Target Port	Target Port	...

Fig. 2. Mitigation Task Chromosome

- if E is Evasive and I is Poor and T is Morning or Afternoon and S is Medium then R is Medium.
- if E is Social and I is Poor and T is Pre-Dawn or Evening and S is not High then R is Medium.
- if E is Evasive and I is Good and T is Pre-Dawn or Evening and S is not High then R is Medium.
- if E is Evasive and I is Poor and T is Pre-Dawn or Evening then R is High.
- if S is High then R is High.

C. Mitigation

The final step is to define appropriate data structures, operators, and fitness functions for the risk mitigation MRTA process. Police and coast guard vessels will serve as mitigating assets. This step attempts to give the best combination of components for a proper mitigating task allocation, so while these assets are not technically part of the RSNs, they could easily be exchanged in other contexts. As was done in Section IV, tasks will first be defined, then genes and chromosomes will be designed, followed by mutation and crossover operators. Finally, the fitness functions will be presented.

A path can be predicted for the smuggling vessel with the data gathered by the ASN, and certain ports can then be predicted as possible berthing points. A risk mitigation task is the relocation of a mitigation asset to one of the possible ports. Table I presents the assets considered and their parameters.

A chromosome is encoded as shown in Figure 2. Each gene corresponds to one asset and has 2 layers; an activation layer and a target port. It can be described as follows, where L is the set of predicted ports as given by the function f_L.

$$Gene = \begin{bmatrix} a \ \epsilon \ A \\ p \ \epsilon \ L \end{bmatrix} \tag{7}$$

$$L = f_L(C) \tag{8}$$

The mutation operator can be described as follows, where P_A is as previously defined.

$$f_M = \begin{bmatrix} P_A \\ P_L \end{bmatrix} \tag{9}$$

$$P_L = \begin{cases} 1/|L| & l \mid l \ \epsilon \ L \\ 0 & else \end{cases} \tag{10}$$

As solutions must aim to use as little resources as possible so a fitness function will evaluate the cost of a solution. The cost metric of a mitigating asset is simply a fiscal estimate of moving the asset by one meter. The fitness function is presented in Algorithm 4.

Algorithm 4 Cost Fitness Function

```
Cost ← 0
for each $Gene \mid Gene.a = 1, Gene \ \epsilon \ Chromosome$ do
    Distance ← Distance(Asset$_i$, Gene.Port)
    Asset Cost ← Asset$_i$.cost * Distance
    Cost ← Cost + Asset Cost
end for
Return Cost
```

The second fitness function evaluates the latency of a solution, with quicker solutions preferable. The speed parameter of mitigating assets is measured in meters per second. The fitness function is defined in Algorithm 5.

Algorithm 5 Latency Fitness Function

```
Latency ← 0
for each $Gene \mid Gene.a = 1, Gene \ \epsilon \ Chromosome$ do
    Distance ← Distance(Asset$_i$, Gene.Port)
    Latency ← Distance / Asset$_i$.speed
    Total Latency ← Total Latency + Latency
end for
Return Latency
```

The final fitness function measures the actual mitigating power of the solution encoded in the chromosome, with those that can adequately stop the smuggling behaviour preferred over ones that cannot. V refers to the set of tracked vessels. The fitness function is defined in Algorithm 6.

Algorithm 6 Risk Mitigation Fitness Function

```
Ports ← $\{Gene.p \mid Gene.a = 1, Gene \ \epsilon \ Chromosome\}$
P.risk ← $\sum_{i=0}^{|V|} Prob(V_i, P) \ \forall \ P \mid P \ \epsilon \ Ports$
for each $Gene \mid Gene.a = 1, Gene \ \epsilon \ Chromosome$ do
    Gene.p.risk ← Gene.p.risk * Asset$_i$.mitigation
end for
Return $\sum_{i=0}^{|Ports|} Ports_i.risk$
```

VII. EXPERIMENTAL RESULTS

This section traces the behaviour of the system defined in Section VI for the scenario and environment explained in Section V.

The smuggling scenario will be first be simulated then repeated with three non-smuggling SRVs. The initial environment is illustrated in Figure 3. The coast of Barcelona can be see about 11 Km away. The environment grid cells have a dimension of 250m x 250m for the purposes of ASN optimization. The risk threshold to trigger aerial monitoring was set at 0.5, corresponding to a medium risk, while the risk threshold for smuggling mitigation was set at 0.75 corresponding to a high risk. The coalition size was limited to 7 and the genetic algorithm had a stopping criterion of 100 generations. This was needed to ensure a swift monitoring response.

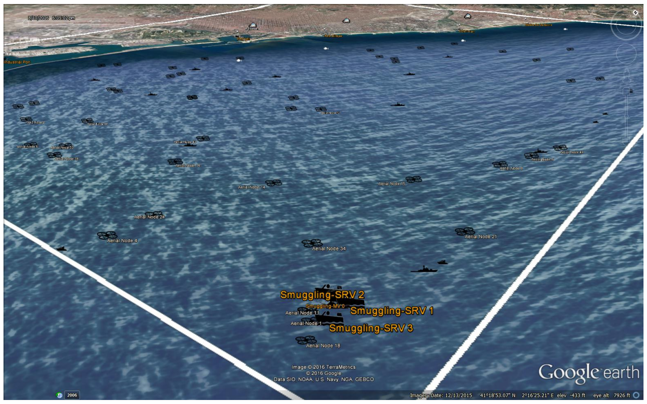


Fig. 3. Initial Environment

TABLE II
MONITORING SOLUTION FITNESS

Solution ID	Resources	Connectivity	Relevancy
1	0.0359	14	3
2	0.4465	14	21
3	0.3471	14	18

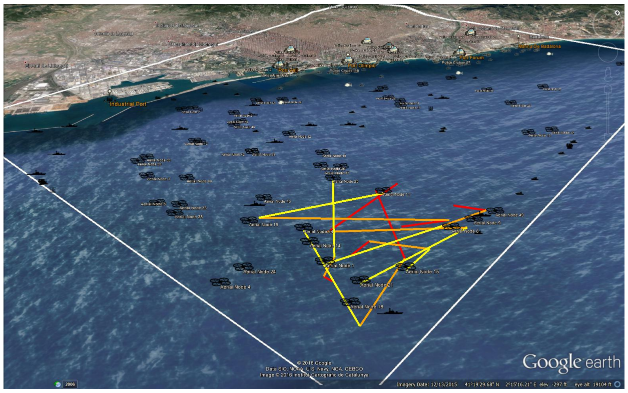


Fig. 4. Monitoring Task Allocation

The MV departed from a medium risk port (risk of 0.5). Its AIS was off for a period of 2 hours during a week long trip yielding a value of 0.1122 for the AIS off time feature. It is engaging in a rendezvous with three SRVs, a value of 0.1 for the distance to nearest ship feature, and the time is about 4h00 giving the time of day feature a value of 0.168. These features evaluate to a suspicious risk of 0.63219, well above the risk threshold of 0.5.

An ASN optimization generates non-dominated solutions. Table II presents 3 of the solution's fitness values. Solution 5 is shown in Figure 4, where yellow, orange, and red correspond to the first, second, and third segments of the path, respectively. This solution is an expensive one, resource-wise, but offers a good connectivity for each segment and a high relevancy.

Additional data that was not previously available is collected with the ASN monitoring service. Images of the suspected vessels can be taken, as well as their positions that were previously sporadically reported from third party sources. Tracking the first vessel yields a value of 0.63219 for prior smuggling risk, 0.72173 for illumination, 0.62495 for evasiveness, and 0.168 for time of day evaluating to a smuggling risk of 0.65637, only slightly below the smuggling risk threshold of 0.75. However, this risk is raised on subsequent evaluations as a consequence of the prolonged monitoring, ultimately resulting in a risk mitigating MRTA process. The smuggling risk over time is shown for the three SRVs in Figure 5.

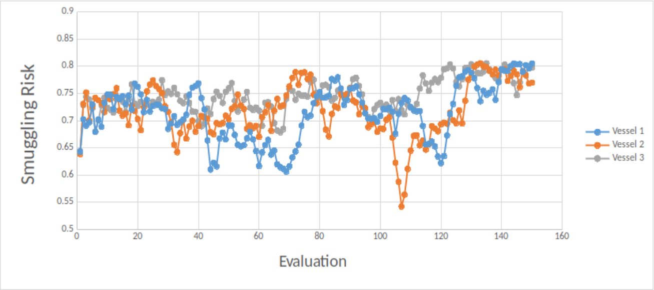


Fig. 5. Smuggling Ship Risk Over Time

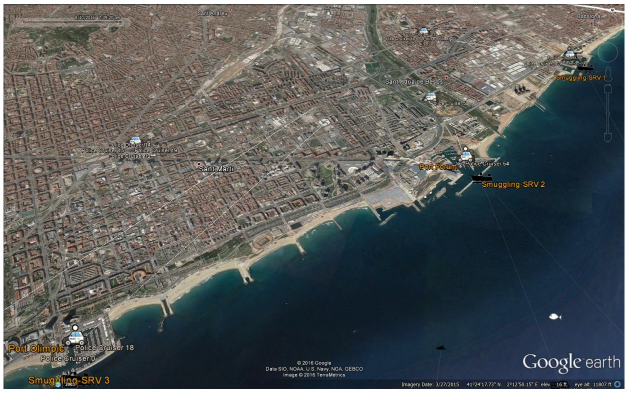


Fig. 6. Successful Risk Mitigation

TABLE III
MITIGATION SOLUTION FITNESS

Solution ID	Cost	Latency (s)	Mitigation (%)
1	64,976.21	1,439.9	0.33215
2	1,301,129.33	13,085.4	1.3539E-4
3	68,104.74	1596.3	0.29893

This risk mitigating MRTA process yields a set of non-dominated solutions. The fitness values of three of these solutions are presented in Table III. The end of the scenario is shown in Figure 6, where mitigating assets are present at the correctly predicted destinations of Port Olìmpic, Port Forùm, and Marina de Badalona. Some assets are sent to Port Vell due to the chosen mitigation solution that valued mitigation over cost. This successfully concludes the scenario.

The second scenario starts with the detected rendezvous with the aerial optimization. The second risk feature assessment for one of the vessels gives a value of 0.5516 for prior risk, 0.5432 for illumination, 1 for evasiveness and 0.168 for time of day. However, the monitoring service provided by the ASN gradually brings down the risk assessment to lower levels, as shown in Figure 7. The risk assessment spikes as the ship's behaviour is intermittently seen as anomalous. Indeed, a rendezvous between civilian ships off the coast in the middle of the night should be suspicious but he risk never exceeds the threshold, and tends to fall to lower values. The scenario successly ends with no mitigating actions against the SRVs.

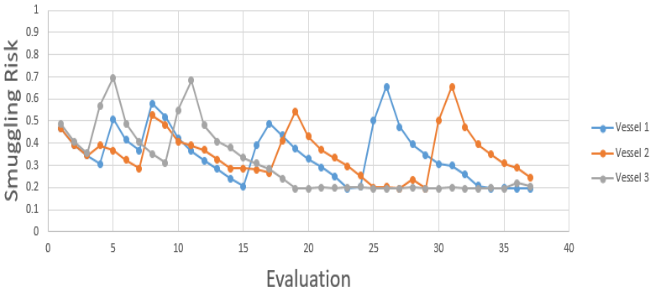


Fig. 7. Civilian Ship Risk Over Time

VIII. Conclusion

UAVs will play a prominent role in future RSNs due to their monitoring ability. Our methodology proposes a method to integrate UAVS in RSNs by formulating the problem in the context of risk management. We propose a scenario based on expert knowledge and successfully apply our methodology. It was shown that the network first determines potentially risky situations at a high level, then monitors the area to gather more information. It finally classifies the event as decidedly risky and takes actions against it, or deems it ultimately not risky.

UAV technology is in its infancy and the plethora of problems that exist in ASNs are only now starting to be researched, with communication primary among these issues [26]. Additionally, the data sources used are often not readily available in a real setting. As a result, there remains work to be done to bring a system such as the one proposed in this work to reality.

UAVs in RSNs have many uses that have yet to be explored. Future work will concentrate on using the ASN for administrative tasks, such as conducting auctions or being sink nodes. Additionally, MRTA processes can allocate shared tasks to both UAVs and ground nodes. Each of these concepts would bring hybrid RSN/ASN closer to reality.

Acknowledgment

This work was supported in part by Mitacs under Accelerate Cluster grant no. IT03458 and by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] F. Xia, Y. Tian, Y. Li, and Y. Sung, “Wireless sensor/actuator network design for mobile control applications,” Sensors, pp. 2157–2173, 2007.

[4] A. Nayak and I. Stojmenovic, Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication. John Wiley & Sons, 2010.

[5] R. Falcon, A. Nayak, and R. Abielmona, “An evolving risk management framework for wireless sensor networks,” in Proceedings of Conference on Computational Intelligence for Measurement Systems and Applications, Ottawa, CA, 2011, pp. 1–6.

[6] J. McCausland, G. Di Nardo, R. Falcon, R. Abielmona, V. Groza, and E. Petriu, “A proactive risk-aware robotic sensor network for critical infrastructure protection,” in Proceedings of Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications, Milan, IT, 2013, pp. 132–137.

[7] J. McCausland, R. Abielmona, R. Falcon, A.-M. Cretu, and E. M. Petriu, “On the role of multi-objective optimization in risk mitigation for critical infrastructures with robotic sensor networks,” in Companion Publication of the Conference on Genetic and Evolutionary Computation, Vancouver, CA, 2014, pp. 1269–1276.

[8] S. Guillaume, “Designing fuzzy inference systems from data: An interpretability-oriented review,” IEEE Transactions on Fuzzy Systems, vol. 9, no. 3, pp. 426–443, 2001.

[9] J. van Laere and M. Nilsson, “Evaluation of a workshop to capture knowledge from subject matter experts in maritime surveillance,” in Proceedings of Conference on Information Fusion, Seattle, US, 2009, pp. 171–178.

[10] O. Vaněk, M. Jakob, O. Hrstka, and M. Pěchouček, “Agent-based model of maritime traffic in piracy-affected waters,” Transportation Research Part C: Emerging Technologies, vol. 36, pp. 157–176, 2013.

[11] M. Andersson and R. Johansson, “Multiple sensor fusion for effective abnormal behaviour detection in counter-piracy operations,” in Proceedings of International Waterside Security Conference, Carrara, IT, 2010.

[12] R. O. Lane, D. a. Nevell, S. D. Hayward, and T. W. Beaney, “Maritime anomaly detection and threat assessment,” in Proceedings of Conference on Information Fusion, Edinburgh, UK, 2010, pp. 1–8.

[13] B. van den Broek, A. Smith, E. den Breejen, and I. van de Voorde, “Inference of vessel intent and behaviour for maritime security operations,” in Proceedings of SPIE Security + Defence, Maryland, US, 2014, pp. 92 480E–92 480E.

[14] E. P. De Freitas, T. Heimfarth, I. F. Netto, C. E. Lino, C. E. Pereira, A. M. Ferreira, F. R. Wagner, and T. Larsson, “UAV relay network to support WSN connectivity,” in Proceedings of Congress on Ultra Modern Telecommunications and Control Systems and Workshop, Moscow, RU, 2010, pp. 309–314.

[15] P. Corke, R. Peterson, and D. Rus, “Coordinating aerial robots and sensor networks for localization and navigation,” in Proceedings of Symposium on Distributed Autonomous Robotic Systems, Toulouse, FR, 2004, pp. 295–304.

[16] M. Dorigo, D. Floreano, L. M. Gambardella, F. Mondada, S. Nolfi, T. Baaboura, M. Birattari, M. Bonani, M. Brambilla, A. Brutschy et al., “Swarmanoid: a novel concept for the study of heterogeneous robotic swarms,” IEEE Robotics & Automation Magazine, vol. 20, no. 4, pp. 60–71, 2013.

[17] I. Maza, F. Caballero, J. Capitan, J. R. Martinez-De-Dios, and A. Ollero, “A distributed architecture for a robotic platform with aerial sensor transportation and self-deployment capabilities,” Journal of Field Robotics, vol. 28, no. 3, pp. 303–328, 2011.

[18] J. A. Sauter, R. S. Mathews, K. Neuharth, J. S. Robinson, J. Moody, and S. Riddle, “Demonstration of swarming control of unmanned ground and air systems in surveillance and infrastructure protection,” in Proceedings of Conference on Technologies for Homeland Security, Waltham, US, 2009, pp. 51–58.

[19] S. K. Teh, L. Mejias, P. Corke, and W. Hu, “Experiments in integrating autonomous uninhabited aerial vehicles(uavs) and wireless sensor networks,” in Proceedings of Australasian Conference on Robotics and Automation, Canberra, AU, 2008.

[20] N. Primeau, R. Falcon, R. Abielmona, V. Groza, and E. Petriu, “Improving task allocation in risk-aware robotic sensor networks via auction protocol selection,” in Proceedings of Conference on Intelligent Engineering Systems, Budapest, HU, 2016, pp. 21–26.

[21] E. Cantú-Paz, “A survey of parallel genetic algorithms,” Calculateurs paralleles, reseaux et systems repartis, vol. 10, no. 2, pp. 141–171, 1998.

[22] N. Atay and B. Bayazit, “Mobile wireless sensor network connectivity repair with k-redundancy,” in Algorithmic Foundation of Robotics VIII. Springer, 2009, pp. 35–49.

[23] L. Joossens and M. Raw, “Cigarette smuggling in Europe: Who really benefits?” Tobacco control, vol. 7, no. 1, pp. 66–71, 1998.

[24] G. A. Antonopoulos and J. Winterdyk, “The smuggling of migrants in Greece: An examination of its social organization,” European Journal of Criminology, vol. 3, no. 4, pp. 439–461, 2006.

[25] R. R. Brooks, P. Ramanathan, and A. M. Sayeed, “Distributed target classification and tracking in sensor networks,” Proceedings of the IEEE, vol. 91, no. 8, pp. 1163–1171, 2003.

[26] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, “Flying ad-hoc networks (FANETs),” Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, 2013.