A Proactive Risk-Aware Robotic Sensor Network for Critical Infrastructure Protection

Jamieson McCausland[1], **George Di Nardo**[2], **Rafael Falcon**[1,2], **Rami Abielmona**[1,2], **Voicu Groza**[1], and **Emil Petriu**[1]

[1] School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada
[2] Research & Engineering, Larus Technologies Corporation, Ottawa, Canada
E-mail: jmcca080@uottawa.ca; george.dinardo@larus.com; rafael.falcon@larus.com; rami.abielmona@larus.com; groza@site.uottawa.ca; petriu@eecs.uottawa.ca

Abstract— **In this paper, a risk-aware robotic sensor network (RSN) is proposed in the context of Critical Infrastructure Protection. Such a network will be comprised of mobile sensor nodes that perceive various aspects of their environment and topologically reconfigure in order to secure a strategic area of interest. Risk awareness is provided through the application of a recently developed Risk Management Framework to the RSN. The risk level of each node is assessed in terms of their degree of distress, proximity factor, and terrain maneuverability. Risk monitoring alerts are issued whenever any given sensor node's quantitative risk metric exceeds a user-defined threshold value. At this point, a node-in-distress (NID) has been identified as the weak point of the securing structure around which the RSN is deployed. The NID can no longer be used with confidence and the effective perimeter coverage of the RSN has been reduced, thus creating potential security breaches in the area of interest. In response, the remaining nodes will self-organize to maximize the perimeter coverage while minimizing the cost of doing so. A limited set of contingency network topologies is produced via evolutionary multi-objective optimization using the Non-Dominated Sorting Genetic Algorithm (NSGA-II) and then ranked according to a human-guided alternative selection algorithm. The security operator picks the most suitable topology, which is then effectuated upon the environment. Results indicate that NSGA-II is capable of producing feasible network topologies to satisfy maximum perimeter coverage, while reducing the energy required for topology reconfiguration. As far as we are concerned, this is the first time a RSN applied to a CIP scenario is self-organized in response to a risk analysis conducted on every sensor node on the basis of multiple risk features.**

Keywords—robotic sensor networks; risk management; self-organization; critical infrastructure protection; territorial security

I. Introduction

Robot Sensor Networks (RSNs) [1] can be applied in the domain of Critical Infrastructure Protection (CIP). In such an application, a RSN is deployed to safe-guard some critical infrastructure (e.g., building, pipeline, etc.) in a secure and reliable fashion. The network would consist of a collection of mobile sensor nodes capable of perceiving different aspects about their environment. Unlike typical wireless sensor network nodes, RSN nodes are capable of moving which in turn allows the network to dynamically self-configure by adopting a different topology. A self-organizing network is very appropriate in CIP. Deployed sensor networks are subject to various forms of unavoidable risk, thus increasing the probability of sensor node failure and coverage gaps. Risk can arise in many fashions such as: low battery power, harsh environmental conditions, malicious attacks, terrain hostility, etc. Although a large body of research focuses on how to avoid these risks, an alternative proposed in [2] features how risk can be assessed, monitored and mitigated. A risk-aware RSN node can utilize all its sensing instruments and evaluate its total risk at any point in time. Raw sensor data feeds are turned into useful risk features, specifically degree of distress, intruder proximity risk, and terrain maneuverability risk, all enabling the sensor network to monitor the risk feature space. A node-in-distress (NID) is identified (i.e., a sensor node whose risk value exceeds a certain threshold) and the network must explore a possible solution to assist such a node in imminent danger, as it may cause a coverage gap that increases the probability of undetected intrusions. In a RSN, a new topology can be computationally derived to meet the operational goals of the network. We model the discovery of a new network topology as a multi-objective optimization problem over a combinatorial search space. Good solutions are sought via the Non-dominated Sorting Genetic Algorithm II (NSGA-II) [3], which provides a set of mutually non-dominated candidate network topologies. To the best of our knowledge, this is the first paper that addresses self-reconfigurability issues in a RSN from a risk-aware perspective in a CIP scenario.

The remainder of this paper has been structured as follows. Section II briefly touches on relevant works in the literature. Section III outlines the application of the risk management framework (RMF) to a self-organizing RSN in the CIP realm. Section IV elaborates on the NSGA-II configuration as part of the RMF's response selection module. Section V sheds light on the empirical study whereas Section VI concludes the work.

II. Related Work

This section briefly touches on some relevant works regarding CIP using wireless sensors technology with and without risk analysis.

Coppolino et al [4] put forth a hybrid intrusion detection system (IDS) to protect critical information structures. The IDS regards sensors as the source and target of potential attacks and develops a two-tier solution to prevent sinkhole and sleep deprivation security breaches. Gomez and Ulmer [5] introduce a system prototype for stadium surveillance. Sensors detect dangerous crowd activities or situations and report alerts to a Command and Control (C2) centre, where a decision maker may choose to assign first responders and dispatch them to the incident scene. These works neither include risk analysis nor optimize the set of potential responses that will mitigate the risk condition.

Aubert et al [6] and Schaberreiter et al [7] propose risk modeling approaches for critical infrastructures. The former aims at modeling the security properties of interdependent systems and measures their risk levels and assurances. The latter constructs the service decomposition graph for risk assessment and showcases an online monitoring tool of three risk parameters. Despite performing risk feature extraction and assessment, these frameworks do not embrace considering a set of prospective responses to be actuated upon the environment.

Another loosely related group of studies optimize the sensor distribution either prior to or after deployment. Jin et al [8] employ a multi-objective differential evolution algorithm to derive sensor distributions over the monitoring region with maximum coverage and minimum overlap. Self-organization in cluster sensor networks after sensor failure is pursued via a local scheme in [9]. Intrusion detection in a mobile sensor network (MSN) is tackled in [10] by providing k-barrier coverage.

Our work touches on the three aspects mentioned above and, to the best of our knowledge, is yet novel in itself. We pursue self-organization in a RSN that protects a critical infrastructure in a proactive and risk-aware fashion. The proposed approach is an extension of the work presented in [2] in which risk analysis drives the entire operation of a sensor and robot network for CIP. However, [2] was not concerned with eliciting a set of promising responses to counter the perceived threat in the network. The authors recently augmented their RMF in [11] with a response selection module that utilizes NSGA-II as a multi-objective optimization method to evolve a group of promising responses that could be actuated upon the environment. The framework was successfully tested in the context of maritime Search and Rescue operations.

This paper applies the RMF to a CIP scenario similar to the one in [2]. As far as we are concerned, this is the first time a RSN is self-organized in response to a risk analysis conducted on every sensor node on the basis of multiple risk features.

III. Risk-Aware Robotic Sensor Networks

The proposed RSN is risk-aware, meaning that it is capable of evaluating the risk of each individual node and flag some of them as NIDs. Raw sensor data are transformed into risk features through the Risk Feature Extraction module of the RMF in [1]. The three risk features selected for this application are the following: degree of distress, intruder proximity risk and terrain maneuverability risk.

Degree of Distress:

This risk feature models the node's current battery level as a fuzzy set $\mu_{DD}(x_{battery})$. With the following triangular membership function: A=0, B=0, C=100.

Intruder Proximity Risk:

The proximity of detections by the sensor node can contribute to the overall risk of the sensor unit. An equipped laser range finder (LRF) provides depth perception to the sensor node. If we consider $x_{detection}$ to be the distance (in m) to the nearest LRF-detected intruder, then $\mu_{proximity}(x_{detection})$ is the fuzzy set modeling the object proximity risk. This fuzzy set uses a trapezoidal membership function with parameters A=0, B=0, C=1, and D=3.5;

Terrain Maneuverability Risk:

This risk feature is a nominal risk feature, which provides a terrain maneuverability metric given some localization context. The risk metric can be configured manually as appropriate for the deployment environment, or in the case of this paper, a random real value between 0.0 and 1.0 Future work will allow sensor nodes to update the KB from sensor percepts. That being said, the terrain information can be queried from the KB by providing the sensor's Cartesian coordinates, $P^i_{node}(p^i_x, p^i_y, p^i_z)$. Localization information can be provided by either a Global Positioning System (GPS) module or any other localization algorithm. The terrain maneuverability risk values are normalized between 0.0 (no terrain risk) and 1.0 (highest terrain risk).

The RMF's Risk Assessment module considers these risk features to produce an overall risk metric for the sensor unit. We have followed the same evaluation scheme used in [2]. A user-defined risk threshold is compared against the overall risk of each sensor node in the network. Units exceeding the risk threshold are marked as NIDs, which represent a network vulnerabilities. This triggers the invocation of the RMF's Response Selection module so as to determine a new feasible network topology to mitigate the threat. The response selection process is explained in the next section.

IV. Risk-Driven Self-Organization In a RSN

Each candidate response topology is evaluated according to two different (and conflicting) objectives:

- F1 = Total Perimeter Coverage: The total area (in %) of the critical infrastructure covered by the RSN.
- F2 = Total Mobilization Cost: The total cost (in %) of mobilizing the nodes to their target locations.

An optimal solution is one that maximizes F1 and minimizes F2. Often, in a multi-objective optimization problem we run into a set of mutually non-dominated solutions (meaning that none is superior to the others). NSGA-II [3] is a well-known algorithm that efficiently produces a good spread of Pareto-optimal (i.e. non-dominated) solutions. The NSGA-II optimization algorithm, will maintain a Pareto Archive Set (PAS) over each generation. In the following, the NSGA-II's configuration for the problem under consideration is unfolded.

A. Algorithm Configuration

Once a NID is elicited by the RMF's Risk Assessment module, a snapshot of the network's current state is acquired and becomes the starting point for the self-organization phase. To begin exploring the solution space for new network topologies, the following information must be retrieved/derived from the RSN:

1. Sensor Node State, $\Phi_{node}^{i}(t)$, $\forall i = 1..N_a$
2. Sensor Node Response Regions, $\Omega_{response}^{i}$
3. Security Perimeter Contour, $\boldsymbol{c}_{security}$

1) Sensor Node State

The N_a sensor nodes are represented at time t by a simple model:

$$\Phi_{node}^{i}(t) = \begin{bmatrix} x_{battery}^{1}(t) & P_{node}^{1}(t) \\ \vdots & \vdots \\ x_{battery}^{N_a}(t) & P_{node}^{N_a}(t) \end{bmatrix} \tag{1}$$

The simulated battery level on board each node is provided as a percentage quantity. A constant discharge rate $\gamma_{discharge}$ (in %) occurs for a deployed sensor node. A power consumption rate of $\gamma_{movement}$ (in % per meter travelled) is used during sensor locomotion. Let $\Phi_{network}(t)$ be the state of the network at time *t*.

$$\Phi_{network}(t) = \begin{bmatrix} \Phi_{node}^{1}(t) & \cdots & \Phi_{node}^{N_a}(t) \end{bmatrix} \tag{2}$$

A detected NID will trigger a snapshot, which captures the network state $\Phi_{network}(t_{NID}) = \Phi_{network}^{NID}$. This state will simply contain the set of battery levels and the set of locations of each sensor node required for algorithm configuration. The state of each sensor node is crucial for the next steps of the algorithm configuration.

2) Sensor Node Response Region

A response region is assigned to each sensor node potentially involved in the response (new topology). A response region is defined as the area that contains a possible target location for a sensor node. The region itself is circular and defined by a center and a radius. The center of the region is set to the sensor node's current location whereas the radius ($r_{response}^{i}$) is a function of ***battery level*** ($x_{battery}^{i}$), ***distance to the NID*** (d_{NID}^{i}), and ***battery level threshold*** ($\lambda_{battery}$). The available battery power on the sensor node is a constraint on the maximum distance travelled. The battery level threshold is the minimum battery level necessary to engage the robotic platforms that are carrying the sensors in differential drive operations. Thus, the maximum response ring radius is:

$$R_{max}^{i} = \begin{cases} 0 & x_{battery}^{i} < \lambda_{battery} \\ \dfrac{x_{battery}^{i} - \lambda_{battery}}{\gamma_{movement}} & otherwise \end{cases} \tag{3}$$

This is the maximum change in position possible without depleting the battery below the $\lambda_{battery}$ level. The response radius is valid on the interval $0 \leq R_{response}^{i} \leq R_{max}^{i}$. The radius of the response region is defined in (4) using a combination of the maximum response radius and a monotonically decreasing exponential function of the distance from the NID. A value of β=0.45 was experimentally chosen to as a decay rate for the exponential function (shown in Figure 1), which produced desirable results.

$$R_{response}^{i} = R_{max}^{i} * e^{-\frac{d_{NID}^{i}}{\beta}} \tag{4}$$

So, we can define the response vector as in (5):

$$\boldsymbol{\Omega}_{response}^{i} = \begin{bmatrix} P_{response}^{i} & R_{response}^{i} \end{bmatrix} \tag{5}$$

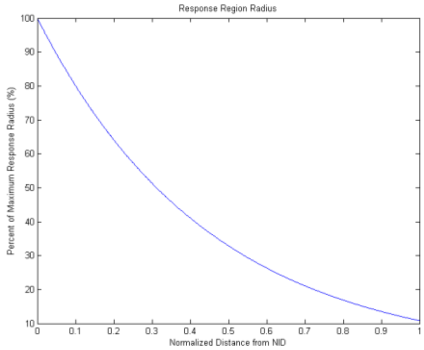


Fig. 1 Response region radius calculation. An exponential relationship ($e^{-\frac{d_{NID}^{i}}{\beta}}$) is defined between $R_{response}^{i}$ and d_{NID}^{i}. $\beta = 0.45$

Each sensor node is equipped with multiple sensors mounted on a differential drive robotic platform. Given a target location, a displacement vector for the sensor node can be calculated. A set of target locations are generated for each sensor node if $\left(R_{response}^{i} > 0 \right)$. Let the set of target locations be:

$$\boldsymbol{S}_{target_j}^{i} = \begin{Bmatrix} \left(r_{t_j}^{1} \cos\left(\theta_{t_j}^{1}\right), r_{t_j}^{1} \sin\left(\theta_{t_j}^{1}\right) \right), \dots, \\ \left(r_{t_j}^{N_t} \cos\left(\theta_{t_j}^{N_t}\right), r_{t_j}^{N_t} \sin\left(\theta_{t_j}^{N_t}\right) \right) \end{Bmatrix}$$

Where $r_{t_j}^{i} \sim U\left(0, R_{response}^{i}\right)$ and $\theta_{t_j}^{i} \sim U(0, 2\pi)$. $U(a, b)$ is a uniform distribution between *a* and *b*. Let **C** represent the algorithm's initialization matrix defined as in (6):

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{\Omega}_{response}^{1} & P_{node}^{1} & \boldsymbol{S}_{target}^{1} \\ \vdots & \vdots & \vdots \\ \boldsymbol{\Omega}_{response}^{N} & P_{node}^{N} & \boldsymbol{S}_{target}^{N} \end{bmatrix} \tag{6}$$

3) Sensor Network Coverage Objective

Sensor network coverage represents the extent of the security perimeter that can be surveyed by the sensor nodes. The perimeter is represented by a contour $\boldsymbol{c}_{security}$ around the critical infrastructure. The RSN must have near-complete coverage of this contour to succeed in detecting any intrusion attempts. Each sensor node in the RSN will contribute to the perimeter coverage by intersecting the sensor node's field of view with the entire contour or a segment of the contour. For computational purposes, let the contour be a set of perimeter points uniformly distributed on the contour, $P_s^k(x_s^k, y_s^k, z_s^k)$, where k=1..K represents the index of the perimeter point.

Let the field of view radius for the ith sensor be r_{fov}^i. By evaluating the distance between the sensor node's position and each discrete contour point, a node will have a contour point surveyed if and only if $\left(P_s^k - P_{node}^i\right) \leq f_{fov}^i$. The coverage of the security perimeter is the ratio of the number of perimeter points covered to the total number of perimeter points. NSGA-II will seek topology solutions which produce large perimeter coverage values. Coverage gaps (i.e. lower perimeter coverage values) must be avoided to reduce undetected intrusions.

4) Energy Cost Objective

The power required to execute a topological change must be minimized when exploring the search space for candidate solutions. Given $\gamma_{movement}$ (power consumption % per meter travelled), the total power required by the RSN to self-organize into the new topology can be estimated by (9):

$$Cost = \sum_{i=1}^{N} d_{response}^i * \gamma_{movement} \tag{8}$$

5) Algorithm Stop Criteria

The stopping criterion for the optimization algorithm is based on the algorithm's runtime $\xi_{runtime}$(in sec.).

B. Chromosome Design

A chromosome in our NSGA-II implementation represents a possible solution to the RSN self-organization problem. Each node's response region will consist of N_t possible target locations. Let $\alpha_{t_j}^i$ be the index of the jth target point for the ith node in the RSN. $\alpha_{t_j}^i \in \mathbb{Z}$ and can be a value on the interval of -1 to $(N_t - 1)$. The index value of -1 indicates that the asset is not used in the solution. Each chromosome can then be represented by the following vector:

$$Chromosome = \begin{bmatrix} \alpha_{t_j}^1 & \alpha_{t_j}^2 & \cdots & \alpha_{t_j}^{Na} \end{bmatrix} \tag{9}$$

A chromosome is a set of target location indices, one for each RSN node. The initial chromosome population in NSGA-II is randomly initialized using a uniform distribution in the specified range. Each node involved in the solution will be assigned a random index.

C. Crossover and Mutation

We implement uniform crossover with probability $p_{crossover}$. When two parent chromosomes are selected from the population to crossover, genes are randomly chosen from either parent.

During a mutation operation, all chromosomes in NSGA-II's extended population are investigated. For a given chromosome, the probability of a gene value being mutated is $p_{mutation}$. The algorithm will iterate through each gene value if the gene is to be mutated then a new random value in the range $[0; N_t - 1]$ is selected to replace the existing one.

V. EXPERIMENTAL RESULTS

A set of experiments using Microsoft Robotics Developer Studio (MRDS)[12] have been created to simulate a RSN deployed in an outdoor CIP scenario in a secluded area. Sensor nodes are shown as white rectangular units forming a perimeter around the building (i.e., critical infrastructure).

A total of seven sensor nodes are used in this experiment to form a secure perimeter around the building. The sensor node resides on a simple differential drive robotic platform and produces raw sensor data from a GPS, an electronic compass, and a laser range finder. The laser range finder equips the node with a sensor field of view (FOV) capable of detecting intrusions on the security perimeter. The FOV is modeled as a circular region with a sensing radius of 3.5 m.

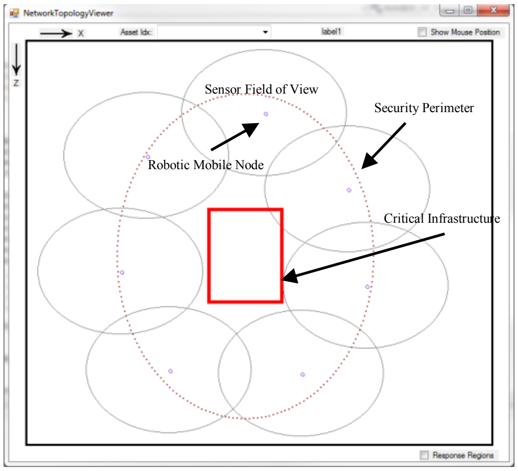


Fig. 2 A 2-D graphical representation of the 20.0 m (along x) by 22.5 m (along y) simulation environment. The red rectangle is the critical infrastructure. The dashed contour around the critical infrastructure represents the security perimeter. Dots encapsulated by circular regions are the sensor nodes and sensor FOVs.

The shape of the security perimeter is defined by an ellipse centered at the position of the building. The semi-major axis (along x-axis) is 5.42 m and the semi-minor axis (along z-axis) is 9.01 m. The elliptical contour is discretized into 200 points. Figure 2 shows a 2-dimensional representation of the scenario including additional visual entities to help visualize sensor FOVs and the elliptical security perimeter.

Table I outlines the initial conditions for the simulation. depicted in Figure 2.

TABLE I. SIMULATION INITIAL STATE

Simulation Initial State, S[t_0]			
Sensor Nodes			
Asset,i	***$P_{initial}$(x, z)[m]***	***$x_{battery}$ (%)***	***f_{fov}^i [m]***
1	(12.8, -12.4)	30	3.5
2	(10.8, -17.8)	70	3.5
3	(11.9, -24.2)	80	3.5
4	(16.8, -26.6)	86	3.5
5	(20.4, -22.4)	86	3.5

Simulation Initial State, S[t₀]			
Sensor Nodes			
Asset,i	*$P_{initial}$(x, z)[m]*	*$x_{battery}$ (%)*	*f^i_{fov} [m]*
6	(21.2, -17.1)	86	3.5
7	(18.5, -12.2)	86	3.5

To detect a NID in the RSN, raw data streams from sensor nodes are used to extract the three risk features outlined in Section III. Risk Assessment.

During the course of the simulation, mobile sensor 1 becomes the NID as its overall risk is 0.73; this is attributed to the "degree of distress" risk feature as this node was deployed in the monitoring region with a battery level of 30%. After the identification of the NID, the NSGA-II optimization algorithm can proceed to initialize the population once the following information is calculated: *the distances to the NID from each node*; *the set of response regions for each node*; *the target locations for each node*

The set of distances of each sensor node's location to the location of the NID can be quickly computed by:

$$d_{NID} = \sqrt{(P_x^{node} - P_x^{NID})^2 + \left(P_y^{node} - P_y^{NID}\right)^2} \quad (10)$$

The response region is a function of both the battery power available on the node and the distance from the node to the NID. Evaluating equation (4), given that $\beta = 0.45$, $\lambda_{battery} = 0.30$, and $\gamma_{movement} = 0.05$ for each node, produces a set of response regions. The center of each response region $P^i_{response}$ is set to the location of the assets from the initial conditions (Table 1). The response region radii are described in Table IV.

TABLE II. RESPONSE REGION RADII

Response Region Radii, $R^i_{response}$ (m)							
Node	1	2	3	4	5	6	7
Value	▨	3.00	1.54	1.13	1.58	2.48	4.48

A set of target points are generated $\boldsymbol{S}^i_{target_j}$ for $0 \le j \le N_t$, $N_t = 200$. With target locations for each node, the chromosome population can be initialized. A population size of 100 chromosomes, $p_{crossover} = 0.8$, and $p_{mutation} = 0.1$ were used. The optimization runs until the stop criterion is satisfied, which in this case is a runtime of 120 seconds. The NSGA-II parameters of [11] were used as starting point, but were adjusted through experimentation to achieve desirable results.

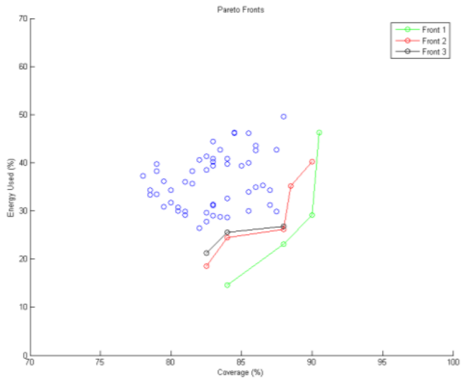
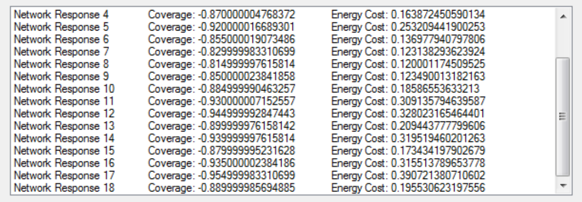


Fig. 3 Plots of the first three Pareto Fronts are displayed in ascending order from green, red, and blue. The remaining solutions (front > 4) are plotted as blue scatter points.

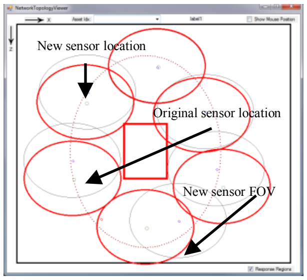
The Pareto Fronts from the PAS are displayed in Figure 3 to paint a clear picture of the non-dominated solutions discovered in the solution space. The first front indicates the truly non-dominated solutions discovered in the search space. The maximum coverage and minimum energy objective functions share equal weighting in the optimization by NSGA-II. It is due to this that extreme solutions are presented with poor coverage but with minimal energy cost along with others that present excellent coverage combined with very high energy cost values. Figure 4 shows a subset of the total set of optimized solutions. It can be observed that solutions are well spread across the Pareto front which confirms NSGA-II's ability to obtain such a uniform distribution of the solutions.



```
Network Response 4      Coverage: -0.870000004768372     Energy Cost: 0.163872450590134
Network Response 5      Coverage: -0.920000016689301     Energy Cost: 0.253209441900253
Network Response 6      Coverage: -0.855000019073486     Energy Cost: 0.136977940797806
Network Response 7      Coverage: -0.829999983310699     Energy Cost: 0.123138293623924
Network Response 8      Coverage: -0.814999997615814     Energy Cost: 0.120001174509525
Network Response 9      Coverage: -0.850000023841858     Energy Cost: 0.123490013182163
Network Response 10     Coverage: -0.884999990463257     Energy Cost: 0.18586553633213
Network Response 11     Coverage: -0.930000007152557     Energy Cost: 0.309135794639587
Network Response 12     Coverage: -0.944999992847443     Energy Cost: 0.328023165464401
Network Response 13     Coverage: -0.899999976158142     Energy Cost: 0.209443777799606
Network Response 14     Coverage: -0.939999997615814     Energy Cost: 0.319519460201263
Network Response 15     Coverage: -0.879999995231628     Energy Cost: 0.173434197902679
Network Response 16     Coverage: -0.935000002384186     Energy Cost: 0.315513789653778
Network Response 17     Coverage: -0.954999983310699     Energy Cost: 0.390721380710602
Network Response 18     Coverage: -0.889999985694885     Energy Cost: 0.195530623197556
```

Fig. 4 Response Selection form displaying a list of optimized solutions.

It is up to a decision maker to select a feasible response for this RSN. Figure 5 depicts the resulting topology when selecting network response 5, which provides an appropriate tradeoff between coverage and energy usage. Conversely, network response 17 provides the maximum perimeter coverage **(95.5%)**, but with the use of significant energy **(39.7%)**.



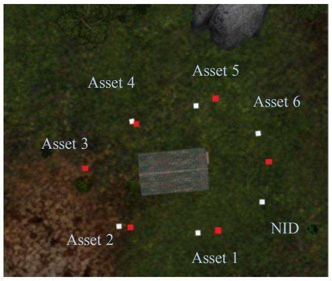


Fig. 5 (left) A 2-D graphical representation of the network response 15. The original and final sensor locations are shown. New sensor FOVs are displayed as the red circular regions. (right) A 3-D graphical view of the response network. Red dots denote the new node locations. White dots indicate the original node location.

Network response 5 provides a coverage metric of **92.0%** (a loss of **-3.5%** from response 17); however it can be achieved using **27.5%** (savings of **13.8%** from response 17) energy collectively from the network. A decision maker will likely choose a response that leans towards high coverage but with the energy cost minimized (i.e., select network response 5 instead of 17).

The algorithm was also tested on a simulated RSN of 47 robotic nodes, protecting a large L-shaped perimeter. After an optimization time of 120 seconds, the PAS contains four solutions. The initial coverage for the network is 99% and the NID causes a coverage gap of 2.23 m thus reducing the perimeter coverage to 97%. Figure 6 depicts the optimized solution with maximum perimeter coverage of **99.2%** and a collective energy consumption of **1.58%**.

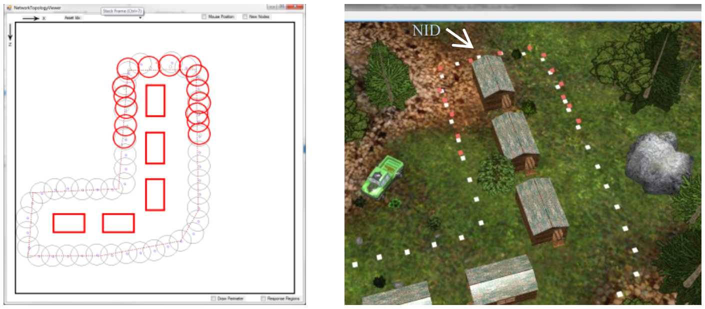


Fig. 6 (left) A 2-D graphical representation of the network response for maximum coverage. The original and final sensor locations are shown. New sensor FOVs are shown as the red circular regions. (right) A 3-D graphical view of the response network. Red dots denote the new node locations. White dots indicate the original node locations.

VI. Conclusions

It is impossible to escape the various risks associated with the operation of a RSN in any environment. The use of a risk-aware RSN grants a new level of perception to anticipate the failure of any given sensor node. In this paper, a simulated RSN was applied to critical infrastructure protection. The deployment goals of the network are: to maintain maximum perimeter coverage and to stay operational for as long as possible. In the event of the presence of a NID, the network is subject to a coverage gap; dramatically increasing the risk of undetected intrusion of the secure perimeter. Through multi-objective optimization with the NSGA-II it is possible to obtain a new network topology for the RSN that maximizes sensor coverage while balancing energy cost. The current work is limited to a single response for mitigating risk. Future work will introduce multiple detected NIDs and the mitigation of the induced risk using simultaneous network responses. In this research we hope to develop a more robust risk-aware RSN.

VII. References

[1] R. Falcon: “Towards Fault Reactiveness in Wireless Sensor Networks with Mobile Carrier Robots”, PhD Dissertation, University of Ottawa, April 2012.

[2] R. Falcon, R. Abielmona and, A. Nayak: "An Evolving Risk Management Framework for Wireless Sensor Networks," in 2011 Int’l Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA), pp.1-6, Sept. 19-21, 2011.

[3] K. Deb, A. Pratap, S. Agarwal and T. Meyarivan: “A Fast and Elitist Multi-objective Genetic Algorithm: NSGA-II”, IEEE Trans. on Evolutionary Computation, vol 6(2), pp. 182-197, 2002.

[4] L. Coppolino, S. D’Antonio, L. Romano and G. Spagnuolo: “An Intrusion Detection System for Critical Information Inffrastructures Using Wireless Sensor Network Technologies”, 2010 5th Int’l Conference on Critical Infrastructure (CRIS), pp. 1-8, Sept 20-22, 2010.

[5] L. Gomez and C. Ulmer: “Secure Sensor Networks for Critical Infrastructure Protection”, in 2010 4th Int’l Conference on Sensor Technologies and Applications (SENSORCOMM), pp. 144-150, July 18-25, 2010.

[6] J. Aubert, T. Schaberreiter, C. Incoul, D. Khadraoui, and B. Gateau. Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures. In Int’l Conference on Availability, Reliability and Security, pages 262–267, February 2010.

[7] T. Schaberreiter, C. Bonhomme, J. Aubert, C. Incoul, and D. Khadraoui. Support Tool Development for Real-Time Risk Prediction in Interdependent Critical Infrastructures. In IEEE Int’l Symposium on Sofware Reliability Engineering. 2009.

[8] L. Jin, J. Jia and D. Sun: “Node Distribution Optimization in Mobile Sensor Network based on Multi-Objective Differential Evolution Algorith”, in 4th Int’l Conference on Genetic and Evolutionary Computing (ICGEC), pp. 51-54, Dec 13-15, 2010

[9] R. Misra and C. Mandal: “Self-Healing for Self-Organizing Cluster Sensor Networks”, in 2006 Annual IEEE India Conference, pp. 1-6, Sept 15-17, 2006

[10] G.Y. Keung, B. Li and Q. Zhang: “The Intrusion Detection in Mobile Sensor Network”, IEEE/ACM Trans. on Networking, vol 20(4), pp. 1152-1161, August 2012.

[11] R. Falcon and R. Abielmona: “A Response-Aware Risk Management Framework for Search-and-Rescue Operations”, IEEE Congress on Evolutionary Computation (CEC), pp. 1540-1547, June 10-15, 2012.

[12] Microsoft: “Microsoft Robotics Developer Studio (Version 4)”. Available from http://www.microsoft.com/robotics/.