Evolving Visualization of Intruder paths in Sensor Networks

James A. Shine, US Army (retired)
James E Gentle, George Mason University
JSM 2013, Montreal, Quebec, Canada
5 August 2013

Abstract

This work builds on our previous efforts to identify intruder paths in sensor networks. Our previous work determined the probabilities that sensor activations were caused by different potential intruders, given the location of the sensor on a spatial grid and the distances and times between current and previous activations. In this paper we present a visualization algorithm to show possible intruder paths on a spatial grid as they develop, and we also show our intruder probability matrix as it develops in real time. These and other advances in the approach will be presented and discussed.

Key Words: visualization, intruder identification, spatial mapping

Introduction

This paper discusses the implementation of a tool first presented as a demonstration concept in 2012 [1]. We are looking at sensor data events that are highly unusual and indicative of an unexpected (and possibly unwelcome) intruder. We are looking at a contiguous geographic region (usually but not necessarily rectangular) with a number of fixed sensors at specific locations in that region. The data will be in the form of a sequence of sensor activations, with the number of the sensor (and implicitly its location) and the time of activation for each data observation. The system is delimited by the convex hull of the sensor locations. An example is shown in Figure 1. The stars indicate successive activations at sensor 20 (time 1.2), sensor 3 (time 3.4), sensor 13 (time 6.7), and sensor 1 (time 7.1). The overall region is shown in the solid box with relative longitude and latitude scales represented, and the convex hull is shown within this box by the dotted line.

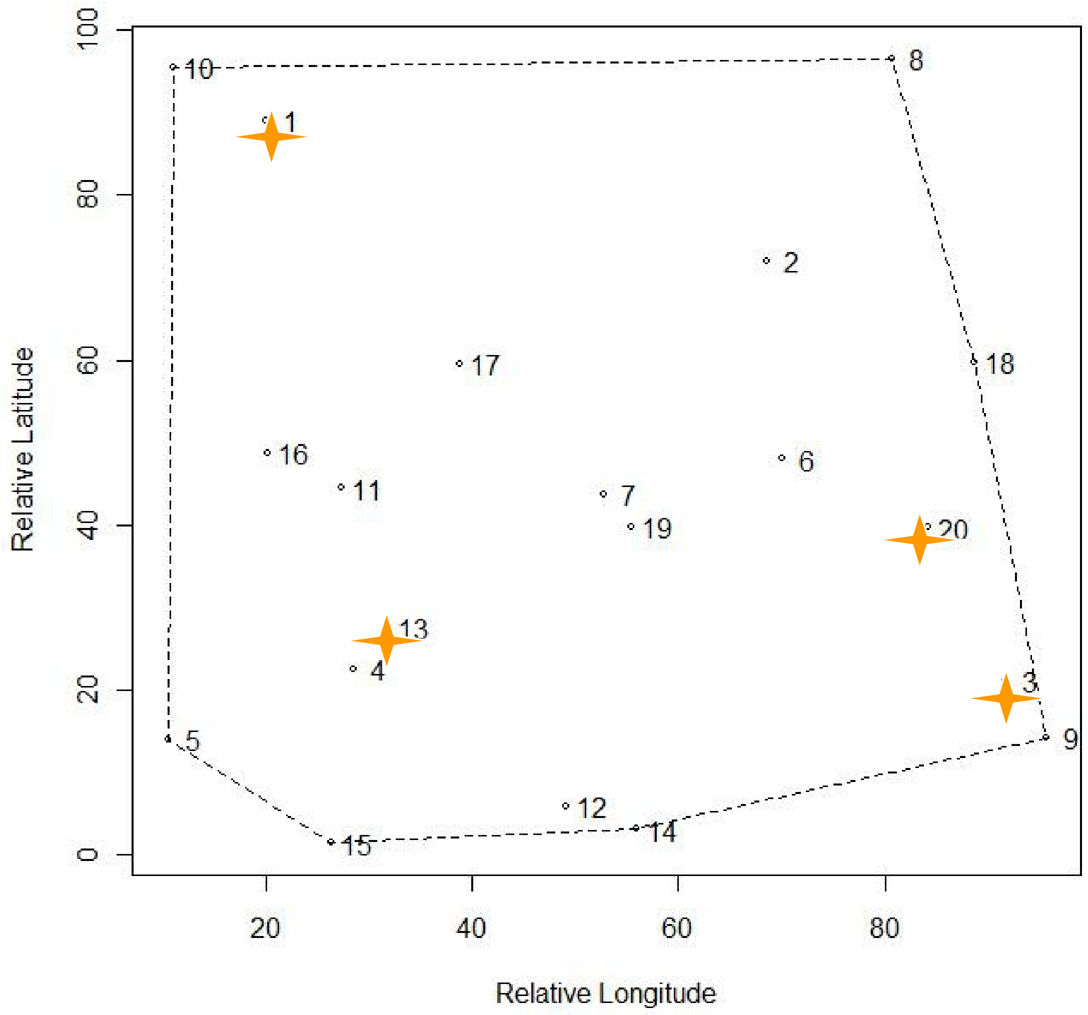

Figure 1: An example setting

Related work:

There is limited related work in published literature. Much of this work relates to camera sensor networks, while our model is more general [2], [3], [4]. Wireless sensor networks, mobile sensor networks, and possible intrusion responses such as robots dispatched to the site of the intrusion are also covered by several researchers [5], [6], [7], [8], [9], [10]. Unlike these efforts, we are developing a probabilistic tool to track intruders in a sensor network.

Applications:

There are a few important areas where the setting is relevant and our tool could be valuable. The main application would be for ongoing surveillance of sensitive facilities such as nuclear power plants and other classified locations, where intruders are a very serious issue. Along the same lines, another application would be in military outposts, looking for possible surprise attacks or infiltration by special units. Another application would be in national park or wilderness areas for monitoring wildlife population.

Description and example output:

Our main objective in this work is to determine the probability of unique intruders (and specifically, how many unique intruders) entering a system, based on the record of sensor activations and times.

We start by setting up the region to be studied, with the sensors and their locations. We then create a convex hull of the sensor locations, as shown in Figure 1. These outermost sensors are more likely to be activated by an entering intruder.

We next compute the "edginess" of each point based on its location in the grid. Points on or near the convex hull (and the grid perimeter) get a higher value of edginess, and points in the interior get a lower edginess value. This quantifies the concept that sensor activations closer to the perimeter are more likely to be caused by a new intruder, as opposed to an existing intruder who is already in the system and has activated one or more sensors already. Similarly, sensors deep in the interior of the region (especially ones with one or more sensors between them and the perimeter) are more likely to be activated by an intruder who has already entered the system and activated one or more outer sensors first.

For any given sensor activation, the two explicit variables are the sensor label and the time of activation. Other implicit variables derived from these two and the specifics of the grid layout are latitude and longitude (x and y), nearest neighbor, distance between the sensor and the complex hull, distance between the sensor and the previous activated sensor, and edginess.

These variables are used to create probability values for each possible intruder at that location. As more sensors are activated, we also develop and visualize probable tracks for intruders. For each activation, we assign an identity label for a possible new intruder, and assign a probability that a new intruder caused the activation. We also update probabilities for previous possible intruders for both causing this activation and remaining in other locations. These values are tracked in an evolving upper triangular matrix. Possible intruder paths are also output on a graph of the region, giving both numerical and visual analysis options.

A specific example is shown in Figure 2 and Table 1. Both represent the activation sequence
1. Sensor 20, time 1.988
2. Sensor 3, time 4.049
3. Sensor 13, time 6.729
4. Sensor 1, time 7.769
5. Sensor 2, time 12.829

Figure 2 shows all possible paths that an intruder (or intruders) could take. The blue arrows represent possible paths taken by new intruders into the region to activate the five sensors, and the red arrows show possible paths that existing intruders could take to get from one sensor to another.

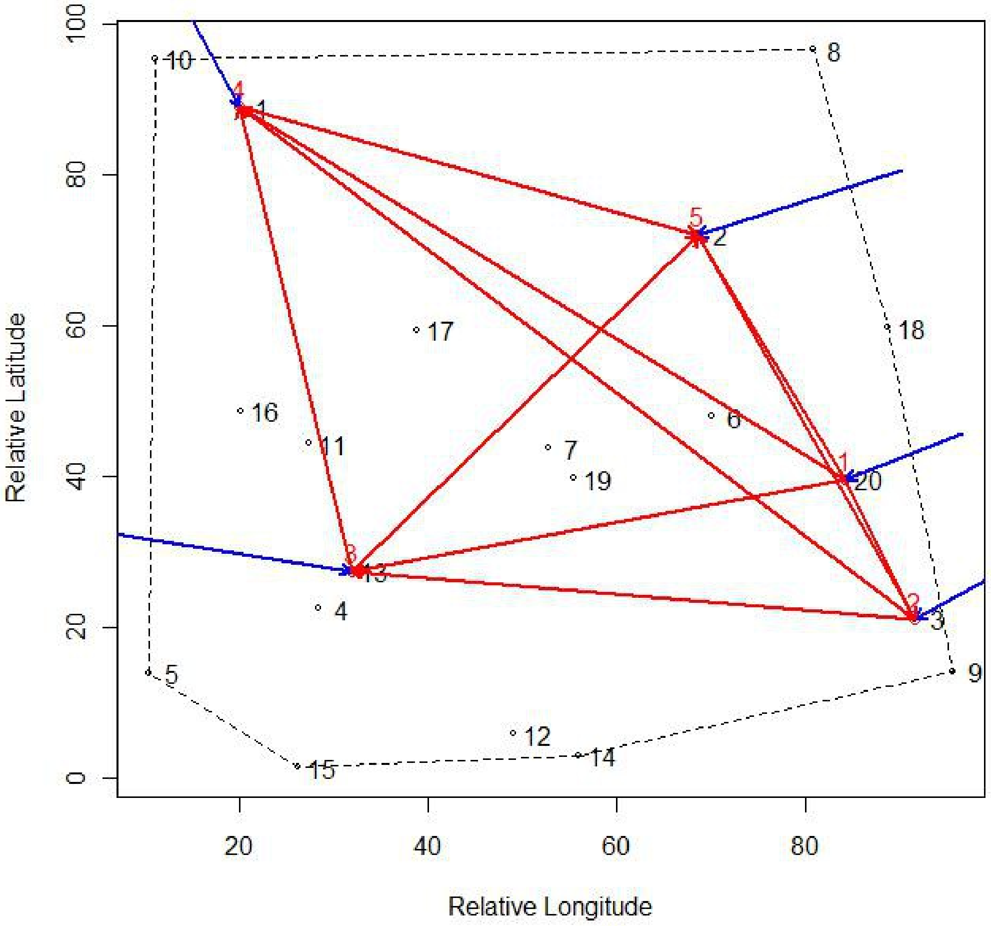

Figure 2: Visualization of possible intruder paths for successive activations at sensors 20, 3, 13, 1 and 2

Table 1 shows the evolving probability matrix after the activation at sensor 2. The first row represents probabilities for different locations for an intruder who entered the system by activating sensor 20. We are assuming that all intruders remain in the region (and do not leave) for this example. The last column, P(in system), represents that probability that a new intruder at the given sensor is still in the system/region. For the first intruder row, that will be 1, since we definitely had a new intruder for the first sensor. For other rows, it will be less than 1, since there is a nonzero probability that an existing intruder or intruders activated the sensor. This particular example tends to favor existing intruders instead of new intruders because of the particular sensor activation sequence and the times.

IntruderEntry	At 20	At 3	At 13	At 1	At 2	P(in system)
20	0.06	0.12	0.22	0.19	0.42	1.00
3	0	0.19	0.10	0.11	0.20	0.60
13	0	0	0.25	0.05	0.11	0.41
1	0	0	0	0.41	0.15	0.56
2	0	0	0	0	0.11	0.11

Table 1: Upper triangular matrix showing probabilities after successive activations at sensors 20, 3, 13, 1, and 2.

The model is built using conditional probabilities and so results in a Bayesian network. We compute prior and transitional probabilities using the configuration of the sensor network. However, prior information could also be incorporated both for initial intrusions and for movements between sensors.

The software has adjustable parameters to weight the input of the distance between sensors, the time between activations, and the importance of a sensor's "edginess" (closeness to the region perimeter or convex hull). It is designed with both test options (to optimize parameters) and to function with streaming, real-time data. It has low computational overhead. It can be used as a surveillance tool for tracking potential intruders.

Some of our assumptions for this work are that the same sensor cannot be activated twice, no intruder leaves the system once they enter, and each sensor activation indicates only one intruder (not more than one). All of these assumptions could be altered for future work.

Conclusions and Future Work

We have developed a preliminary tool for predicting the probabilities of different intruders at sequential sensor activation events. This tool can be used, among other things, to estimate the number of unique intruders in the system based on the sensor activation records. The tool shows possible intruder paths as different sensors are activated, and actively updates a matrix of probabilities that any given intruder is at any given sensor. The tool requires minimal computation and can easily be adapted for real-time sensor networks and their activations.

There are a number of possible improvements that can be added to this tool in the future. Our work to date has used Euclidean distance as a function when considering the distance between two different sensors. This has been the same for all sensors and in all directions. However, the effects of terrain (such as hills, bodies of water, and other barriers) will make some distances more difficult to traverse than others, and this can be modeled. Also, alternatives to Euclidean distance (such as Manhattan distance when the terrain contains a grid of roads) can be implemented.

It would also be useful to adjust the thickness of the line width on the visualization tool to reflect the probability of that path; a thicker line would have a higher probability than a thinner one.

References

[1] J. Shine and J. Gentle, "Identification of Intruder Paths in Sensor Networks", proceedings of the Joint Statistical Meetings 2012, San Diego, CA, August 2012.

[2] P. Skraba and L. Guibas, “Energy Efficient Intrusion Detection in Camera Sensor Networks”, J. Aspnes et al. (Eds.): DCOSS 2007, LNCS 4549, pp. 309–323, 2007. _c Springer-Verlag Berlin Heidelberg 2007.

[3] M. Winkler, G. Barclay and K. Hughes , “Theoretical and practical aspects of military wireless sensor networks”, *Journal of Telecommunications and Information Technology (JTIT)*, February, 2008.

[4] T. Bokareva, W. Hu and S. Kanhere, “Wireless Sensor Networks for Battle field Surveillance”, *Land Warfare Conference*, Brisbane, 2006

[5] A. Sutagundar and S. Manvi, “Context Aware Multisensor Image Fusion for Military Sensor Networks using Multi-agent System”, International Journal of Ad hoc, Sensor and Ubiquitous Computing, Volume 2, #1, March 2011.

[6] Y. Li and L. Parker, “Intruder detection using a wireless sensor network with an intelligent mobile robot response”, IEEE Southeast Conference, 2008.

[7] G. Keung, B. Li and Q. Zhang, “The Intrusion Detection in Mobile Sensor Network”, IEEE/ACM Transactions on Networking, Vol 20, #4, August 2012.

[8] A. Sutagundar and S. Manvi, “Context Aware Multisensor Image Fusion for Military Sensor Networks using Multi-agent System”, International Journal of Ad hoc, Sensor and Ubiquitous Computing, Volume 2, #1, March 2011.

[9] S. Shaikh, H. Chivers, P. Nobles, J. Clark and H. Chen, “Characterizing intrusion detection sensors”, Network Security, September 2008.

[10] S. Shaikh, H. Chivers, P. Nobles, J. Clark, and H. Chen, “A Deployment Value Model for Intrusion Detection Sensors”, J.H. Park et al. (Eds.): ISA 2009, LNCS 5576, pp. 250–259, 2009.