A pragmatic value-of-information approach for intruder tracking sensor networks

Damla Turgut and Ladislau Bölöni
Dept. of Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL 32816–2450
{turgut,lboloni}@eecs.ucf.edu

***Abstract*—Sensor networks are distributed systems where nodes embedded in the environment collect readings through their sensors and transmit data to customers. The overall goal of these systems can be stated as maximizing a metric of the sensing quality while limiting the consumption of a set of scarce resources.**

In this paper we consider an intruder detection and tracking system where the sensing quality is a metric of the *pragmatic value of the information* provided by the network. This metric depends not only on the quantity and accuracy of information, but also on when and how the customers will use this information. We design a system which adapts its information transmission to the disruptive decisions made by the user, including a consideration for the cost of incorrect decisions.

I. Introduction

Sensor networks are distributed systems where a number of nodes embedded in the environment collect readings through their sensors and transmit data to customers. The overall goal of these systems can be stated as *maximizing a metric of the sensing quality* while *limiting the consumption of a set of scarce resources*. Which resources are considered scarce depend on the application: they can include resources such as energy, bandwidth, spectrum and stealth.

In this paper we are considering an intruder detection system which operates over a large area with zones of different security needs. Multiple moving targets of different types can operate in this area, which might or might not represent a threat. We assume that the customer can make decisions about doing something about the specific intruders (for instance, intercept them). However, the customer is limited by its own resource limitations.

This paper introduces a model of sensing quality which sees the value of the information from the point of view of the *end user*. We contrast this with purely information theoretic metrics, where the sensing quality is independent on the use the humans put it: it takes the same number of bits/second to track a deer or an armed intruder. There is normally a limit of how much information theoretic information quantity can be obtained by a sensor network with a finite resource consumption. Within this limit, however, the pragmatic utility of the transmitted information can vary widely.

The practical advantage of considering such a sensing quality model is that it allows us to correctly set a low (or zero) value to information on which the customer is unable to act[1]. This way, we can obtain higher quality information supporting the actions we have actually decided to take. For instance, if we have two intruders, but only one patrol which we can use to intercept an intruder, the customer needs to decide which intruder to intercept. The value of information for the real time tracking of the intruder selected for interception becomes more valuable. The value, however, is limited by the practical needs of the interception task. For example, capturing a human intruder with a patrol unit does not require millimeter accuracy tracking.

The pragmatic information value model introduces a number of challenges:

- The value of information changes in time (even retroactively) in function of the decisions of the customer, which can be a human-in-the-loop or an automated decision agent.
- The system must support the decision making process of the human or agent decision makers, thus it must be aware of the impact of various pieces of information on the decisions.
- The choice of asymmetric distribution of sensing and reporting resources can offer great benefits in the case of correct decisions, but it can reduce the quality if the decision have been wrong (e.g. by misidentifying the threat posed by an intruder). The system must support recovery from erroneous consumer decisions.

This paper is organized as follows. Section II provides a formal treatment of the pragmatic value of information. Section III applies this model to the practical problem of an intruder detecting sensor network in a mixed-used area with limited resources. We describe a simulation study in Section IV. We discuss related work in Section V and conclude in Section VI.

II. A pragmatic model of the value of information

Let us assume that the sensor network delivers a chunk of data d to a customer C. At time t, the customer will have a collection of *raw data* $D = \{d_1, d_2, \ldots d_k\}$, which will be used to build a *model of the world* $M = f_{\mathrm{M}}(D, t)$. For the purpose

[1] An example is high accuracy real-time tracking of an intruder which we cannot intercept, nor take any other action (e.g. contact or warn the intruder, raise an alarm etc.)

of this paper, we will treat the model as a black box. The actual implementation choice of the model can range from a single scalar to lists of values, raster-based environmental models, linear or non-linear predictors, confidence ranges and other models of arbitrary complexity. The modeling function can be a combination of components such as filtering, interpolating, extrapolating, system identification and others.

The *value* of the model is a scalar $V = f_{\mathrm{V}}(M) = f_{\mathrm{V}}(f_{\mathrm{M}}(D,t)) \in \mathbb{R}$ which scores the detail, accuracy and timeliness of the model, weighted by the interests of the customer. The *value function* f_{V} might change in time. For instance, once the customer classifies a target as high priority, both the quantity and timeliness of the data concerning the target becomes more valuable.

Let us now consider the perspective of a sensor node which has a chunk of data d. If the node sends the chunk to the customer, it will be added to the set of raw data: $D' = D \cup d$, yielding an updated model $M' = f_{\mathrm{M}}(D', t)$. We define the value of the data chunk to the customer d as $V(d,t) = f_{\mathrm{V}}(M') - f_{\mathrm{V}}(M) \geq 0$.

If $V(d,t) = 0$, the data was worthless for the customer. This can happen if the data was already received from other sources[2] or it is of no interest to the node.

$V(d,t)$ depends on the time t when the customer receives the data. This is *not* the time when the data was acquired, nor the time where the information it contains refers to. For instance, the data chunk d might contain the locations of the intruder over a number of timepoints $\{(x_1, y_1, t_1) \ldots (x_j, y_j, t_j)\}$. Naturally, all these timepoints will be earlier than t.

Usually, the value of data is decreasing in time: $t_1 \leq t_2 \Rightarrow V(d,t_1) \leq V(d,t_2)$. The rate of the depreciation depends on the modeling function, the value function and the other raw data received by the customer between t_1 and t_2.

Some aspects of the information value functions are commonsensical: more accurate models are better, if an information chunk does not change the model, its value is zero. But beyond this, however, many different functions can serve as a value function. In this paper we shall use a systematic approach for defining the value of the information in terms of *pragmatics*, that is, the decision making of the agents which use the information.

Let us denote with $f_{\mathrm{V}}(M, A)$ the pragmatic value of a model of the world M for an agent A. We define this value to be the cummulative value of the actions which had been taken while using the model as source of information.

This definition appears to simply push the problem of defining the value of information one step further. However, in practice, value judgements are much easier in the application domain, especially in terminal states. It is much easier to assign a certain value to catching an intruder than assigning a value to the transmission of a certain measurement at certain time.

[2]In some circumstances a second, independent confirmation of a data chunk can have some value.

From the point of view of the information needs, we distinguish two types of decisions:

- **Disruptive decisions** change the algorithm for calculating the pragmatic value of information. One can usually think about them as a commitment to a new plan, such as the decision to intercept the intruder.
- **Incremental decisions** do not change the algorithm for calculating the pragmatic value of information. Examples of a class of incremental decisions are the path corrections necessary to intercept an intruder. Incremental decisions have predictable information needs. These predictions do not extend past the disruptive decisions.

We assume that making a disruptive decision is a free privilege of the customer - although we can make probabilistic calculations about what the decision will be. For an intruder tracking sensor network the most important disruptive decisions are (a) the classification of the intruder and (b) the manner of tracking the intruder (will a physical interception be attempted?).

In practice, most intruders turn out to be non-threatening. In consequence, the impact of the disruptive decisions is *almost always* a decrease in the value of information. Targets classified as no threat or low threat would have a lower value of the information, thus less information will be collected. Note however, that disruptive decisions can act in the other direction as well: it is possible to upgrade the threat level of a target, and thus increase the value of information.

Nevertheless, the effect of any errors made in "downgrade" type disruptive decisions will be amplified: if we have misclassified an intruder (e.g. by mistaking an armed intruder for a known friendly human), this will reduce the amount of future received data, thus lowering the ability to later reconsider the classification. The possible cost of being wrong must be considered by the system, and information which would make the system reconsider a disruptive decision must be assigned a high value.

III. A PRACTICAL SCENARIO

For a practical scenario we consider a section of the UCF research park (see Figure 1) containing a mix of zones with various security needs:

- Buildings and areas with high security requirements (US Naval Air Warfare Center)
- Buildings and areas with moderate security requirements (Institute for Simulation and Training)
- Areas with no specific security requirements (university buildings, businesses such as Universal Window Coverings, and wildlife preservation areas).

The objective is to cover the area with an intruder monitoring and tracking system. We assume a heterogeneous mix of sensors (vision, proximity, metal detectors and weight sensors) deployed in an engineered manner (which means that the location of each sensor is known). The sensor are communicating with a unique command center. The total flow of information to the command center is bitrate-limited.

Fig. 1. A portion of the Central Florida Research Park.

A. Classifying the intruders

Classifying the intruders is a disruptive decision which allows us to assign value to the passive tracking of the given intruder. We classify the detected intruders into the following classes:

- A Small animals (rabbits, racoons): have a small weight, no metallic components, do not perform purposeful movement and do not stick to roads.
- F Friendly persons: have a weight and shape appropriate for a human, no metallic components, perform purposeful movement and restrict themselves to traveling on the road. They can be visually identified by operator.
- I Armed intruders: have a weight and shape appropriate for a human, have metallic components (weapons), they might be identified by an operator.
- V Vehicles: large weight, metallic, traveling on the road.
- U Unmanned ground vehicles (assumed to be intruders): small weight, metallic, perform purposeful movement.

When first sighting an intruder, the system starts with no concrete information (except prior probabilities). As a single observation rarely leads to a conclusive classification, the system must have a technique to integrate the various, occasionally contradictory evidence arriving from the observation.

Our approach will be to use the Dempster-Shafer theory of evidence to model the knowledge we gather about the classification of the intruders. Any observation about the intruder is considered as an evidence with a specific mass function, defined on the powerset of possible classifications. For instance a strong signal from a metal detector lends evidence towards the intruder being a vehicle, a UGV or an armed person, while providing evidence against it being an animal or an unarmed person.

The calculation of the evidence in the Dempster-Shafer model yields two values, the *belief* and the *plausibility*. This needs to be contrasted to the single value, of probability, which we would obtain if we would use, for instance, a Bayesian network. The system uses both the belief and the plausibility values:

- The *belief* is used as an input to the operator in order to support a disruptive decision. The operator is not obliged to make a decision in a predictable way based on the belief value. A human operator, for instance, can act on a hunch, it can delay the decision, and so on. Operators implemented as software agents are more likely to act in a predictable way. For our experiments we will assume that the operator will make a disruptive decision of classification as soon as the belief in the classification exceeds 0.5.
- The *plausibility* value is always larger than or equal to the belief value. The plausibility value is used to assess the cost of being wrong. For instance, if we identified a human as most likely friendly, but with still a high plausibility for the case of being an armed intruder, the system must prepare for the possibility of the customer changing his mind about the classification.

TABLE I
THE DEMPSTER-SHAFER MASS EVIDENCE FUNCTIONS FOR SENSOR SIGNALS

Sensor and signal	Evidence mass function
weight sensor high mass	{V,F,I}=0.5 + s, {A,U} = 0.5 - s
weight sensor low mass	{A,U} = 0.5 + s, {V,F,I} = 0.5 - s
metal detector low reading	{A,F} = 0.5 + s, {V,U,I} = 0.5 - s
metal detector high reading	{V,U,I} = 0.5 + s, {A,F} = 0.5 - s
sticking to road	{F,V} = 0.5 + s, {F,V,A,I,U} = 0.5 - s
visual identification as friendly	{F} = 0.90, {F,I} = 0.10

Table I describes the evidence mass functions for the classification of the intruder types.

B. Tracking decisions and information value

The second class of decisions the operator must take are the tracking decisions, which decide how the system will track the intruder. This can include active actions, such as physical interception. The tracking decision is not tied to the classification, although there is a strong probabilistic relation. The operator is more likely to decide to intercept an armed intruder than a small animal. The tracking decisions are limited by the available resources: we assume that the system has resources for at most one physical interception at a time, while bandwidth constraints prevent the simultaneous high resolution tracking of an arbitrary number of intruders. We consider that the operator has the choice of three tracking decisions:

- **Tracking metric for interception (TM-I)**: the utility is the high accuracy real-time location of the intruder (inside the interest area). This is a model suitable for the interception of an intruder.
- **Tracking metric for following (TM-F)**: the utility is the location of the intruder, with any accuracy within the tolerance range of $d_t = 5m$ having the same value. This is a model suitable for the following of an intruder judged to be of low threat.
- **Tracking metric for historical path reconstruction TM-HPR**: the utility of the location is the error of the path reconstruction done at time tolerance t_t after the real time.

In the following subsections we describe the calculation of information value for the different tracking models.

C. Information value of real-time tracking

Intuitively, the tracking error is the distance from the real location of the intruder to the location where the customer believes it to be. To treat accuracy as an information value metric, however, we need to consider the interests of the customer and treat the boundary conditions with care. Assuming that the customer is interested in the geometric area described by the rectangle R, let us consider an intruder node T, for which the customer has a model $M(T)$. If the customer does not have a model of the intruder (for instance, if it didn't yet receive a report about it), we will assume that it believes it to be outside the interest rectangle. The calculation of the tracking error $\varepsilon(T, M(T))$ considers the following cases:

- $T \in R \wedge M(T) \in R \Rightarrow \varepsilon(T, M(T)) = dist(T, M(T))$: if both the intruder and the model are inside the interest rectangle, the tracking error is the distance from the model to the intruder.
- $T \in R \wedge M(T) \notin R \Rightarrow \varepsilon(T, M(T)) = dist(T, R)$: if the customer believes the intruder to be outside the interest rectangle but T is inside rectangle R, the tracking error is the distance from T to the closest edge of rectangle R.
- $T \notin R \wedge M(T) \in R \Rightarrow \varepsilon(T, M(T)) = dist(R, M(T))$: if the intruder is not in the interest rectangle, but the customer believes it is, the tracking error is the distance from the model to the closest edge of the rectangle R.
- $T \notin R \wedge M(T) \notin R \Rightarrow \varepsilon(T, M(T)) = 0$: if the intruder is not in the interest rectangle and the customer does not believe it to be in the interest rectangle, the tracking error is zero.

Thus, the tracking error is continuous as the intruder moves in and out of the interest rectangle. In addition, it respects our intuition that the customer does not care about the intruders outside the area, but penalizes the customer for believing that the intruder is in the interest area while it is not and vice versa.

This definition allows us to define an information value function. If the information chunk d allows the customer to build a better model $M'(T)$, then $V(d, t) = \varepsilon(T, M(T)) - \varepsilon(T, M'(T))$.

D. Information value of historical path recognition

Another aspect of intruder tracking is the reconstruction of the path taken by the intruder in the interest area. Understanding which points the intruder visited is of a special interest in many applications. The reconstituted path can, for instance, allow the customer to classify the intruder or recognize the activity performed by the intruder. In this case, historical information can be useful, and the depreciation rate is slower.

The reports sent for real time data tracking can be used to outline a crude approximation of the path of the node. We can estimate the path of the intruder between two successive location reports with a straight line. It is possible, however, that the intruder made a detour between the two reported points.

Let us assume that we receive two reports about the intruder. The first report states that the intruder is at location $P_1(x_1, y_1)$ at time t_1, while the second one, that the intruder is at location $P_2(x_2, y_2)$ at time t_2. We denote with d the distance between these points. We can be confident that the path of the intruder between these two points is a straight line only if the maximum velocity of the intruder is exactly $d/(t_2 - t_1)$. If the intruder has a higher maximum velocity v_{max} which allows it to traverse a path of length $d_{max} = v_{max}(t_2 - t_1) > d$ the intruder could have visited many other points in the meanwhile.

Simple geometric place considerations show that the points which the intruder could have visited are the interior of an ellipse with the focus points P_1 and P_2, with the semimajor axis $a = d_{max}/2$ and the semiminor axis $b = \sqrt{d_{max}^2 - d^2}/2$ (Figure 2-a).

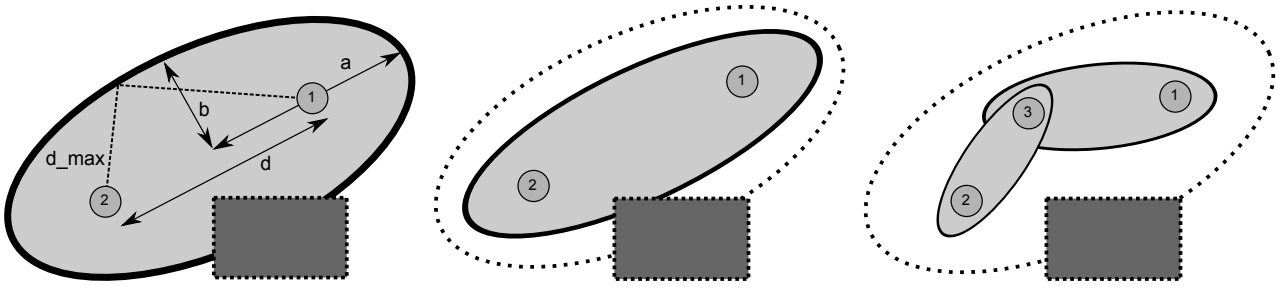
An intuitive metric of our uncertainty about the points which were traversed by the intruder can be expressed by the area of the ellipse $A = \pi ab = 0.25 \cdot \pi \cdot d_{max}\sqrt{d_{max}^2 - d^2}$.

The uncertainty can be reduced either by having information about the maximum speed of the node between the two nodes, i.e. reducing d_{max} (Figure 2-b), or by having an additional data point P_3 at time $t_3 \in [t_1, t_2]$ (Figure 2-c). We can associate the value of a new piece of information with the reduction in the size of the uncertainty area. The value of information can be equivalated with the reduction of the uncertainty about the locations traversed by the intruder, that is, the difference between the area of the original ellipse, and the new smaller ellipses.

In many cases, our concern is less about the absolute value of the uncertainty, rather the conclusive answer to the question whether the node had traversed an area of high interest (such as a high security area). In the three examples in Figure 2, the rectangular region shows such a high interest area. For (a) and (b) the uncertainty area intersects with the high interest area. This does not mean that the intruder had entered the area, only that it could have entered it. The additional observation in (c) had reduced the uncertainty sufficiently that we can exclude the possibility that the intruder had entered the high interest area.

IV. Simulation study

We will consider the area described in Figure 1, of size 1000 x 1000 meters. We assume a relatively large number of 400 presence sensors, with smaller numbers of metal detectors, weight detectors, and cameras (25 each). For each sensor we assume a range of 50 meters. All observations are made with a Gaussian noise which increases with the distance from the sensor. The bottleneck of the wireless transmissions and the finite processing speed of the command center enforces that only a limited number of observations (in these experiments set to 300 observations / minute) can be used to update the model of the customer. We will consider four systems representing different attitudes towards the value of the information. All systems will select the messages to forward that, in the local perception of the network nodes, contribute the most to the value of the customer's model.



(a) Original (two observations) (b) Reduced uncertainty about v_{max} (c) Additional observation

Fig. 2. The possible positions of the target (a) initial (b) after more information about the maximum velocity and (c) after an additional datapoint. The intruder could have possibly traversed any point in the shaded area. The shaded rectangle is a high interest area (e.g. a high security zone). Only the case (c) can guarantee that the target did not enter the high interest area.

TABLE II
THE WEIGHT FACTORS OF THE VALUE OF INFORMATION. THE DOUBLE VALUES REFER TO VALUE WHEN DECIDED FOR INTERCEPTION / VALUE WHEN NOT DECIDED FOR INTERCEPTION.

	TM-INT	TM-NA	TM-HPR
A	0	0.1	0.1
F	0	0.1	0.1
I	3.0 / 0	0 / 1.0	0 / 0.2
V	0.1	0.5	0 / 0.2
U	3.0 / 0	0 / 1.0	0 / 0.2

UNIFORM: assumes that each intruder is equally important. This largely corresponds to the current state of the art in sensor networks.

PRAGMATIC: assumes the value of the information to be given by the classification decision and the action decision of the customer.

CAUTIOUS: augments the decision of the PRAGMATIC model with the plausibility value calculated by the Dempster-Shafer reasoner, raising the value of targets which are *classified* as low value but can *plausibly* be of high value.

UNLIMITED: a system which has an infinite amount of resources and can process the theoretical limit of the reporting capacities.

The utility metric will use the weight factors described in Table II. Different weight factors apply to the nodes chosen for interception, versus those which have been not.

We model a scenario which unfolds as follows: over a course of 10 minutes (600 seconds), 8 small animals are present in the area and perform random waypoint movement. At time t=100, a weapon carrying human target enters the area. The evolution of the classification decisions and action decisions was modeled as follows. To create a scenario which triggers the differences between PRAGMATIC and CAUTIOUS, we have enforced a noise level in the first encountered camera which causes the control center to mistakenly identify the target as friendly. With this setting, the UNIFORM, CAUTIOUS and UNLIMITED model recovered from the mistake around t=200. The PRAGMATIC model made a more aggressive downgrade of the value of information received about the intruder and thus received less future notifications. As a result of this it did not change its classification until about t=300. For all four systems, the customer took a decision to intercept the intruder at t=480.

Figure 3 shows the evolution of the value of received information for the four systems. The UNLIMITED model shows the upper limit of information value which can be obtained with the set of sensors for the current set of intruders. If no high value targets are present, the value of information is naturally low, while in the cases when an intruder is selected for interception (in the time interval 480-600) the value of information is higher.

The lowest performance is obtained by the UNIFORM model, due to the fact that the system is wasting time on reporting on the low value targets (the small animals).

The PRAGMATIC model achieves the highest value of information among the resource limited models in cases when it correctly identifies the intruder. When it misidentifies the intruder (in our case in the time interval 100-300), however, it achieves a significantly lower utility than the CAUTIOUS model.

Finally, the CAUTIOUS model, avoids the low performance of the PRAGMATIC model when the customer misidentifies the system. In addition, the CAUTIOUS model recovers earlier from the misidentification than the PRAGMATIC model (at around t=200). On the other hand, the CAUTIOUS model can not quite match the performance of the PRAGMATIC model for the case when the identification is correct (as it will allocate part of the resources to plausible high-value targets).

V. RELATED WORK

A. Intruder tracking sensor networks

Intruder tracking sensor networks have been extensively studied, and the field covers a wide variety of technologies with their specific challenges. For sensor nodes with plentiful energy resources and guaranteed network connectivity, the scarcest resource is the attention of the sensing device. One example is the case when we have a retargetable sensor, such as a directional radar (Horling et al. [7]). In other papers the assumption is that only a subset of the sensors can be activated simultaneously (eg. Krishnamurty [8]).

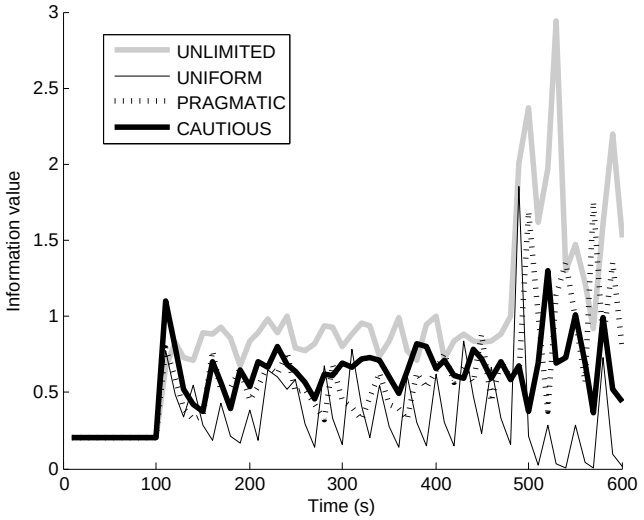


Fig. 3. The value of the information received by the customer during the scenario.

An alternative scenario is the case when the sensor nodes have limited energy resources. The challenge is to assign the active times in such a way that the tracking quality is maintained. Gui and Mohapatra [5] consider a target tracking sensor network and study the tradeoffs between the power conservation and the quality of surveillance. Yan et al. [14] discuss an approach in which nodes self-schedule their active time such that areas with different security requirements are provided differentiated services. Olariu et al. [10] employs a clustering approach that uses wedges and coronas to create a coordinate system and partition the area around each Aggregation and Forwarding Node (AFN). Wang et al. [12] considers the problem of detecting intruders in a network which covers the interest area incompletely and sensors can be heterogeneous in terms of transmission and sensing range. Zou and Chakrabarty [17] consider a target tracking sensor network with mobile units.

B. The value of information in sensor networks

Early sensor network research focused mainly on the networking / communication aspects. Soon, however, it became evident that significant benefits can be obtained by building a superstructure which provides an information centric view to the customer. Sensor databases provide a view of the wireless sensor network as a streaming database. The initial vision was outlined in Govindan et al. [4], with influential early implementations being TinyDB [9] and Cougar [15].

One further step is to consider the needs of the customer not in terms of the raw data flow, but at a higher semantic level, as answers to questions such as "why, when, where, what, who, how" (Bisdikian et al. [1]). The *quality of information* provided by the sensors can be defined as the ability to provide answers to these questions. Such aspects have been considered implicitly in several papers dealing with sensor networks, such as He et al. [6] and Yeow et al. [16]. In the last three years these topics have become the focus of targeted research, among others in Bisdikian et al.[2], Gillies et al. [3], Tan et al. [11] and Wei et al.[13].

VI. Conclusion

In this paper we described an architecture which guides the data collection in an intruder-tracking sensor network while taking into consideration the pragmatic value of the collected information for the customer. Experimental results show that the architecture allows us to increase the quality of information reaching the customer about the targets judged to be high value. At the same time, the experimental results also show that the system must consider the possibility that the customer was mistaken in their classification of the intruder, and prepare for possible revisions of beliefs.

References

[1] C. Bisdikian, J. Branch, K. Leung, and R. Young. A letter soup for the quality of information in sensor networks. In *IEEE PerCom*, pages 1–6, March 2009.

[2] C. Bisdikian, L. Kaplan, M. Srivastava, D. Thornley, D. Verma, and R. Young. Building principles for a quality of information specification for sensor information. In *IEEE Intl. Conf. on Information Fusion (FUSION)*, pages 1370–1377, July 2009.

[3] D. Gillies, D. Thornley, and C. Bisdikian. Probabilistic Approaches to Estimating the Quality of Information in Military Sensor Networks. *The Computer Journal*, 53(5):493, 2010.

[4] R. Govindan, J. Hellerstein, W. Hong, S. Madden, M. Franklin, and S. Shenker. The sensor network as a database. Technical report, USC Computer Science Department, 2002.

[5] C. Gui and P. Mohapatra. Power conservation and quality of surveillance in target tracking sensor networks. In *ACM MobiCom*, pages 129–143, September - October 2004.

[6] T. He, S. Krishnamurthy, L. Luo, T. Yan, L. Gu, R. Stoleru, G. Zhou, Q. Cao, P. Vicaire, J. Stankovic, et al. VigilNet: An integrated sensor network system for energy-efficient surveillance. *ACM Transactions on Sensor Networks (TOSN)*, 2(1):1–38, 2006.

[7] B. Horling, R. Vincent, R. Mailler, J. Shen, R. Becker, K. Rawlins, and V. Lesser. Distributed sensor network for real time tracking. In *Int. Conf. on Autonomous Agents*, pages 417–424, May - June 2001.

[8] V. Krishnamurthy. Algorithms for optimal scheduling and management of hidden markov model sensors. *IEEE Transactions on Signal Processing*, 50(6):1382–1397, 2002.

[9] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong. Tinydb: an acquisitional query processing system for sensor networks. *ACM Transactions on Database Systems (TODS)*, 30:122–173, 2005.

[10] S. Olariu, M. Eltoweissy, and M. Younis. ANSWER: AutoNomouS net-Worked sEnsoR system. *Journal of Parallel and Distributed Computing (JPDC)*, 67(1):111–124, January 2007.

[11] R. Tan, G. Xing, X. Xu, and J. Wang. Analysis of Quality of Surveillance in fusion-based sensor networks. In *IEEE PerCom Workshops*, pages 37–42, March 2010.

[12] Y. Wang, X. Wang, B. Xie, D. Wang, and D. Agrawal. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. *IEEE Transactions on Mobile Computing*, 7(6):698–711, June 2008.

[13] W. Wei, T. He, C. Bisdikian, D. Goeckel, and D. Towsley. Target tracking with packet delays and losses-qoi amid latencies and missing data. In *IEE PerCom Workshops*, pages 93–98, March 2010.

[14] T. Yan, T. He, and J. Stankovic. Differentiated surveillance for sensor networks. In *ACM SenSys*, pages 51–62, November 2003.

[15] Y. Yao and J. Gehrke. Query processing in sensor networks. In *Conference on Innovative Data Systems Research*, January 2003.

[16] W. Yeow, C. Tham, and W. Wong. Energy efficient multiple target tracking in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 56(2):918–928, 2007.

[17] Y. Zou and K. Chakrabarty. Distributed mobility management for target tracking in mobile sensor networks. *IEEE Transactions on Mobile Computing*, 6(8):872–887, August 2007.