IVE: improving the value of information in energy-constrained intruder tracking sensor networks

Damla Turgut and Ladislau Bölöni
Department of Electrical Engineering and Computer Science
University of Central Florida
Email: {turgut,lboloni}@eecs.ucf.edu

***Abstract*—This paper proposes a reporting decision protocol called IVE (for Information Value - Energy tradeoff), where individual nodes of an intruder tracking sensor network make decisions about the transmission of information chunks. Instead of trying to achieve raw data metrics (such as total transmitted data) the protocol aims to optimize the *value of information* (VoI) maintained by the customer. To achieve this, the nodes will need to perform *inferences* about the behavior of other nodes and the customer, such that the nodes do not need to send information which the customer already received from other sources or information which it can guess based on previous data.**

A simulation study compares the performance of the IVE protocol with the current state of the art of on-demand periodic reporting.

I. Introduction

Sensor networks are distributed systems where sensing nodes embedded in the environment collect data and transmit it to the customers. The objective of the sensor network is to minimize the consumption of a set of *scarce resources* while maximizing a metric of *sensing quality*.

Scarce resources come in a variety of forms including energy, electromagnetic spectrum, access to retargetable sensors, the stealthiness of the sensor and even the limited attention span of the human operator. In this paper we consider the energy (and, implicitly, the expected lifetime) of the sensor network to be the critical scarce resource.

The metric of the sensing quality depends on the practical application scenario and the preferences of the customer. While sensing quality had been traditionally expressed in low-level networking terms, we argue that defining it in terms of high-level, user-pragmatic categories provides both more value to the user and a larger design space for the system builder [1].

Let us start by outlining three approaches to the definition of sensing quality. One choice is to equate sensing quality with the *quantity of information*: we can seek to maximize the bytes of information arriving to the customer together with metrics such as latency and jitter. The next step is to define the sensing quality in terms of the *accuracy of information*. This requires us to relate the transmitted data to the observed physical reality - thus the quality will need to become application dependent.

In this paper, we take a further step, and define the sensing quality in terms of the *value of information* (VoI) to the customer. For instance, if the customer receives a certain observation from two different sensors, the value of the second report will be zero - even if the report is accurate. This makes the value of a report dependent not only on the observed phenomena, but also on the previous knowledge (the *world model*) of the customer.

This paper we consider an *intruder tracking sensor network* [2] and introduce the **I**nformation **V**alue - **E**nergy tradeoff (IVE) protocol which allows the customer to explicitly set a tradeoff between the VoI it requires from the network and the energy cost it is willing to pay for it. The goal of the protocol is to allow an IVE-running system to provide higher VoI for similar energy usage compared to the current state of the art (or, alternatively, a lower energy usage for equivalent VoI).

IVE is a *reporting decision protocol* - its purpose is to decide what information will be transmitted and forwarded. In most current systems, sensors are configured to transmit on a periodic basis, sometimes coupled with a *transmission condition* to avoid transmitting empty messages. For instruder tracking sensor networks, the transmission condition is normally the presence of an intruder. We will call this policy *on-demand periodic reporting* (ODPR) and we will use it as a baseline to compare IVE against.

For a complete system, the reporting decision protocol must be combined with a routing protocol which decides the path the information takes to the destination.

II. Value of information for intruder tracking

A. Value of information as avoided damage

We define the value of information provided by an intruder tracking system in pragmatic terms, from the point of view of a customer. Let us consider a customer C, interested in an interest region R with area $area(R)$. An intruder I entering the area can cause damage, which we will assume to be additively accumulating during the presence of the intruder in the area. We define the *damage per unit of time* as a time-variant function $k_I(t)$.

We say that an intruder is *untracked* if the customer doesn't know about its existence or it is completely uncertain whether the intruder is inside or outside the interest area. For these situations, the damage reaches an intruder dependent maximum value $k_I(t) = k_I^{max}$.

We say that an intruder is *tracked* if its location is known with an accuracy sufficient for the customer to take action to avoid damage. For example, this might specify the acceptable error $e < e_{acc}$ for a security guard to intercept the intruder. For indoor environments, the acceptable accuracy might require the system to identify the room in which the intruder is currently present. Without loss of generality, we will assume that for a tracked intruder, the damage per unit of time is zero[1].

What remains is to define the damage for intermediate values of tracking knowledge. We will define the *area of uncertainty* as the circle with the radius e from which we subtract a circle with the radius e_{acc}, with area $A_{unc} = (e^2 - e_{acc}^2)\pi$. This is the area where the intruder can possibly be. We will assume the damage per unit of time to scale with a power of the ratio of the area of uncertainty and the area of the interest region.

$$k_I(t) = k_I^{max} \min\left(1, \max\left(0, \left(\frac{(e^2 - e_{acc}^2)\pi}{area(R)}\right)^c\right)\right) \quad (1)$$

The exponent c needs to be determined empirically to match the intuition about the loss of VoI in function of decreasing accuracy. In our paper, the value used is $c = 12$

Definition 1: The *value of information* (VoI) provided by an intruder tracking system is the *avoided damage* compared to an environment without an intruder tracking system.

Thus we can define the VoI per unit of time and intruder I as:

$$v_I(t) = (k_I^{max} - k_I(t)) \cdot p_I(t) \quad (2)$$

where the *presence function* $p_I(t)$ has a value of 1 if the intruder is inside the interest region R and 0 otherwise. In a system, the VoI evolves in time, and we can have more than one intruder operating in the region of interest. To find the *total VoI* provided by the system we need to sum over the intruders and integrate over time:

$$V = \sum_I \int_{t_{start}}^{t_{end}} v_I(t) \quad (3)$$

We can made several observations with regards to this definition. First, the VoI is defined in terms of high level, pragmatic user concepts and measured in real world currency (dollars). Another observation is that the VoI depends on the intruders and the damage they can do: if there are no intruders or they can do no damage, the VoI is zero. This matches well with our practical intuition about intruder tracking systems: such systems should be deployed in places where intruders are likely and the potential damage is high.

[1]Naturally, even a tracked intruder can do damage. However, we are interested in the value of the intruder tracking system to the customer, thus we can define the value *at the margin*, subtracting the unavoidable damage from the value considered.

B. Location estimation at the customer side

Let us now investigate the way in which the customer acquires and maintains knowledge about the intruder. The customer receives a series of reports from the sensor nodes in the form[2] $R = \{I, (x, y), t\}$ signifying that intruder I had been sighted at location $\vec{r} = (x, y)$ at time t.

Over time, the customer will receive a series of reports $\{R1, \ldots, R_n\}$, which it will maintain in the form of a list sorted by increasing values of t (which might not necessarily be the order of the arrival of the reports to the node).

Let us now consider the perspective of the customer at a time $t > t_n$. The customer wants an up-to-date estimate of the location and presence of the intruders, a *world model*. The simplest estimation method it can use is Last Known: assume that the intruder is at the last reported location, that is the location $\vec{p}_n = (x_n, y_n)$ from the last report R_n.

Alternatively, the customer can deploy *predictive estimation methods* which can take as input the full set of reports $\{R1, \ldots, R_n\}$, additional knowledge about the intruder I and *a priori* knowledge about the environment. The best choice of predictive estimation method depends on the application, the environment, the accuracy and trustworthiness of the sensor and the available computing power. In open areas with no obstacles, an Inertial Estimation model can be used which assumes that the intruder maintains a constant speed vector. If the intruder is confined to paths as roads, we can use a Path Following model, which assumes that the intruder follows the current path with a constant speed. Finally, in areas with many obstacles, such as indoor environments, Particle Filter based models are appropriate, which can track the possible locations of the intruder while integrating location reports and *a priori* information [3] about the environment.

Let us now consider the VoI from the perspective of the sensor node. The VoI had been defined from the point of view of the knowledge of the customer. To judge the value of a potential report R_k the sensor must estimate the contribution to the world model of the user.

If the customer uses a Last Known estimation, with the last report being R_n, the sensor node needs to compare it to the report's timestamp t_k. If $t_k \leq t_n$, the report is obsolete and provides no new value. On the other hand, if $t_k > t_n$, the new report, if transmitted, would provide the new estimate. Still, if $dist\left((x_n, y_n), (x_k, y_k)\right) < e_{acc}$, the VoI contribution will be zero as the intruder is currently sufficiently tracked. Even if the value is larger, the VoI gain will need to be traded against the cost of transmission (in our case, in the form of energy consumption). In IVE, the sensor node will transmit only when the expected VoI is larger than a user specified threshold.

If the customer uses Inertial Estimation, the sensor must try to predict the customer's estimate and compare it with

[2]The reports might include additional information, for instance, additional sensed features of the intruder. From the point of view of this paper, an important consideration would be if the sensor is able to directly measure the speed vector of the intruder $\vec{v}$. Unfortunately, such sensors, such as Doppler radars or LIDARs are rarely used in intruder detection systems

(x_k, y_k). Even if the intruder had performed a significant movement from the last reported location, it will still be no need for transmission, as long as the movement was inertial. As soon as the intruder changes its movement pattern (for instance, by stopping or by making a sharp turn), the estimates will diverge and the value of the report will increase, making its transmission justifiable.

All these techniques require that the sensor node to estimate the customer's estimate - in effect to build a model of the customer's world model. A sensor node will normally underestimate the accuracy of the customer's world model, because (a) it might not be able to fully reproduce the customer's estimation due to limited resources[3] and (b) because the customer might have information from other sources. There are a number of situations when the sensor node might overestimate the customer's world model: for instance, if the reports have been lost, or if the customer received (and believed) misleading information from the other sensor nodes.

The underestimation of the customer's accuracy is a helpful simplifying factor, as it avoids a situation where a sensor node would mistakenly withhold information in the belief that the customer does not need it.

III. Inference and estimation in the IVE protocol

The IVE protocol is based on the general idea of *reasoning about reports*. The sensor nodes can maintain a local knowledgebase of reports and a local estimate of the customer world model. Some reports will be forwarded to the customer. The customer uses the reports to create a world model which can estimate the current location of the intruders in the system.

The reasoning process of the nodes involves:

- maintaining their own knowledgebase of intruders
- making decisions about forwarding reports to the customer
- making decisions about the forwarding path

The maintenance of the local knowledgebase is based on a number of *inferences*.

- Direct observation of the intruder creates a report.
- A received transmission will create a report (the node will assume that it is responsible for the transmissions).
- An overheard transmission creates a report, but not an obligation.
- A report older than a specific time frame will be expired from the knowledgebase.
- New reports about the same intruder lead to the expiration of the reports. The number of reports maintained depends on the estimation technique. For Last Known, only the most recent report is kept. For Inertial Estimation, the nodes keep a sufficient number of reports to be able to estimate the speed vector $\vec{v}$ with a sufficient lead-in time.

The maintenance of the local estimate of the customer's world model (LECWM) involves the following inferences:

- A report sighted by the local node is added to the LECWM at the moment when it is transmitted.
- A report received for forwarding is added to the LECWM when it had been successfully forwarded.
- A report overhead is added to the LECWM at the moment of overhearing.
- When the transmission decision module asks the LECWM for an estimate of the customer's model, it will perform an estimate based on the reports in the LECWM and a local estimation technique.
- Expire reports from the LECWM based on a policy appropriate to the local estimation technique.

[3]This is not an issue for inertial estimation, but it is a major concern for particle filter based estimation

A. Considerations about the Inertial Estimation technique

Inertial Estimation assumes that the intruder is moving with a constant speed on a straight trajectory. We need to estimate the speed vector $\vec{v}$ of the intruder at the last confirmed location $\vec{r}_n = (x_n, y_n)$ and and time t_n. The future location at time t will be estimated by:

$$\vec{r} = \vec{r}_n + \vec{v} \cdot (t - t_n) \tag{4}$$

The challenge here is that most sensors are not able to directly estimate $\vec{v}$. Instead we need to estimate $\vec{v}$ based on the location estimates. A naïve approach would be to estimate based on the last two receiver values:

$$\vec{v} = \frac{\vec{r}_n - \vec{r}_{n-1}}{t_n - t_{n-1}} \tag{5}$$

The problem, unfortunately is that the t_n and t_{n-1} values can be close together or even identical. If $t_n = t_{n-1}$, which is possible if the reports came from different sensors, the value of the expression is undefined. But, even if we enforce $t_n > t_{n-1}$, for small values of $t_n - t_{n-1}$ the Equation 5 amplifies the localization errors. For instance, it can lead to a speed vector which is the exact opposite of the real one. In order to avoid such errors, we want the time points used in the Equation 5 to be separated by a sufficient lead-in time t_{min}. To achieve this, the previous point might not necessarily be $\vec{r}_n$, but the latest report which maintains the minimum lead-in compared with the most recent one.

IV. Simulation Study

In the following, we describe a series of simulation studies, designed to investigate the relative benefits of the IVE reporting decision protocol in contrast to on-demand periodic reporting (ODPR), for different estimation techniques and parametrization choices.

A. Simulation environment

We have simulated an area $R_{sim} = 1500 \times 1000$m, with the sensors deployed in a "grid with noise" model in a region $R_{depl} = 1000 \times 500$m, with the interest area being $R = 800 \times 300$m. Notice that the sensor nodes have been deployed in an area somewhat larger than the interest area - this allows the system to estimate the presence function p (that is, whether the intruder is actually in the area or not). This is an important consideration, because the sensors outside the intruder area can

actually provide negative signals for p, which has a significant contribution to the VoI calculation.

We assume that a number of 2..80 intruder nodes are active in the area R_{sim} over the course of the 2 hours simulated time. However, only a subset of these nodes will be present inside the interest area R. We have modeled the movement of the intruder nodes using a random waypoint model.

The customer behavior will be described with the specification `C-pe` where `pe` is a parameter which describes the estimation technique deployed by the customer, with the possible values `LK` - Last Known and `IE` - Inertial Estimation.

For the sensor node behavior, we have the following choices:

`S-ODRP-pi` - the sensor node performs on-demand periodic reporting. When the sensor node first sights an intruder, it sends a report immediately. Future reports will be transmitted at a fixed time interval `pi` as long as the intruder is in sight.

`IVE-pe-pc` - the sensor node performs the IVE protocols with the choices described in the parametrization. The parameter `pe` describes the estimation protocol used by the sensor node to predict the reasoning of the node, which can take the values LK (Last Known) and IE (Inertial Estimation). The parameter `pc` specifies the information value trigger level, the level of sufficient information value increase at which the node decides to transmit.

B. Energy and VoI in function of number of intruders

In the first experiment, we measure the sum of the network-wide transmission energy (used for the transmission of reports), and the total VoI achieved by the system, while varying the number of intruders operating in the area. Note that the number of intruders ranges between 2-40. Naturally, this is a very large number for actual human intruders, however, it is a typical value for outdoor environments, where the majority of moving targets are small animals.

- `C-LK+S-ODPR-10` - Customer uses Last Known estimate, sensor nodes use ODPR with time interval 10 seconds
- `C-LK-S-IVE-LK-1` - Customer uses Last Known estimate, sensor nodes use IVE with Last Known estimate and VoI transmission threshold 1.0
- `C-IE-S-IVE-IE-5` - Customer uses Inertial Estimation, sensor nodes use IVE with Inertial Estimation and VoI transmission threshold 5.0

Figure 1-lower shows the evolution of the VoI for these three configurations. As expected, the total VoI increases approximately linearly with the number of intruders present for all three configurations. The deviations from the linearity are due to the random movement of the intruders which might spend more or less time on average in the interest area. However, the VoI achieved by the three configurations are near-identical.

Figure 1-upper shows the evolution of the total transmission energy for these three configurations. Again, as expected, the transmission energy is increasing with time. However, the expended energy is very different for the three configurations: the ODPR approach consumes about twice the energy of the IVE approach with Last Known estimation, and about four times the energy of IVE with Inertial Estimation.

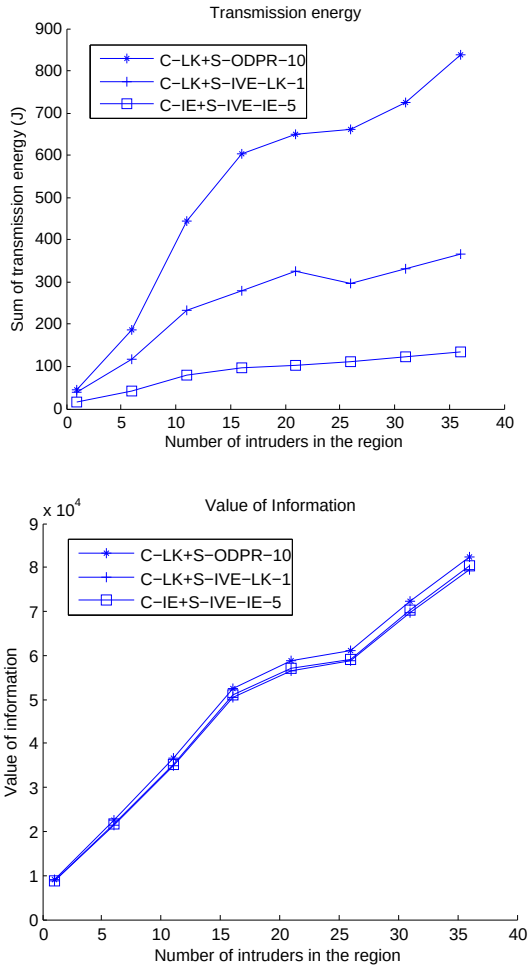

Fig. 1. Transmission energy (upper) and VoI (lower) function of the number of intruders.

In conclusion, we find that with appropriate parametrization, all the methods can be configured to achieve equivalent VoI - however, the energy consumption of the IVE methods are going to be significantly lower. Furthermore, between various IVE configurations, the more sophisticated the estimation method, the lower the energy consumption.

As a note, with a different parametrization we can achieve near identical energy consumption among ODRP and various IVE variants - however, in this case the VoI of the IVE variants will be higher.

C. The evolution of VoI in time

In this simulation study, we investigated the evolution in time of the VoI for two protocol combinations (`C-LK+S-ODPR-200` and `C-IE-S-IVE-IE-0`). We have

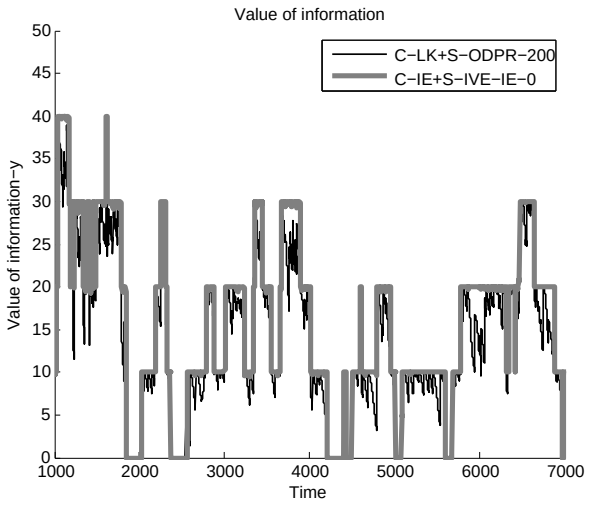

Fig. 2. Time series of the gain in VoI.

traced the evolution of the acquired VoI in time. The resulting time series graphs are shown Figure 2.

The first observation is that the graph shows a characteristic step-like structure. The height of the individual steps being an integer multiple of the maximum damage (in our case, 10), with the integer multiplier being the number of intruders currently in the interest area. When there is no intruder in the area, neither protocols achieve any VoI. In this particular case, the `C-IE-S-IVE-IE-0` configuration almost always achieves the maximum VoI (as this configuration will transmit at any opportunity when the estimate diverges more than e_{acc}). On the other hand, `C-LK+S-ODPR-200`, while still shows the same step structure, it can significantly fall behind the maximum possible VoI.

V. Related work

A. Energy constrained intruder tracking sensor networks

A number of recent papers are considering the interrelation between intruder tracking and the energy constraints of sensor nodes. One approach to reduce energy usage is to activate only a subset of the sensors. The challenge is to assign the active times in such a way that the tracking quality is maintained. Gui and Mohapatra [4] consider a target tracking sensor network and study the tradeoffs between the power conservation and the quality of surveillance. Yan et al. [5] discuss an approach in which nodes self-schedule their active time such that areas with different security requirements are provided differentiated services. Turgut et al. [2] quantify the stealthiness of a sensor node and show that try and bounce (TAB) protocol achieves significantly higher stealth for equivalent tracking accuracy, or, alternatively, lower tracking error for equivalent stealth expenditure. Wang et al. [6] 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.

B. The value of information in sensor networks

A relatively new research approach in sensor networks move from the consideration of quantitative metrics of data transmission to higher level, qualitative metrics, which are often called quality or value of information. Turgut et al. [1] 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. Bisdikian et al. [7] define quality of information as the ability of a network to answer questions such as "why, when, where, what, who, how". In recent years, these topics have become the focus of targeted research, among others in Gillies et al. [8], Tan et al. [9], Wei et al.[10], Liu et al. [11].

VI. Conclusion

In this paper we described IVE, a reporting decision protocol for intruder tracking sensor networks. By requiring the individual sensor nodes to reason about the VoI of the reports they are about to transmit, and implicitly, by requiring them to estimate the customer knowledge about the intruders, the IVE protocol allows us to significantly improve the trade-off between VoI and energy consumption. Our experimental results show that IVE approaches require significantly less energy to achieve equivalent VoI compared to state of the art on-demand periodic reporting systems. Furthermore, the more sophisticated estimation techniques are used by IVE, the lower the energy consumption.

References

[1] D. Turgut and L. Bölöni, "A pragmatic value-of-information approach for intruder tracking sensor networks," in *IEEE ICC*, June 2012.

[2] D. Turgut, B. Turgut, and L. Bölöni, "Stealthy dissemination in intruder tracking sensor networks," in *IEEE LCN*, pp. 22–29, October 2009.

[3] B. Turgut and R. Martin, "Restarting particle filters: an approach to improve the performance of dynamic indoor localization," in *IEEE Globecom*, pp. 1–7, December 2009.

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

[5] T. Yan, T. He, and J. Stankovic, "Differentiated surveillance for sensor networks," in *ACM SenSys*, pp. 51–62, November 2003.

[6] 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*, vol. 7, pp. 698–711, June 2008.

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

[8] D. Gillies, D. Thornley, and C. Bisdikian, "Probabilistic Approaches to Estimating the Quality of Information in Military Sensor Networks," *The Computer Journal*, vol. 53, no. 5, p. 493, 2010.

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

[10] 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 *IEEE PerCom Workshops*, pp. 93–98, March 2010.

[11] C. Liu, P. Hui, J. Branch, and B. Yang, "QoI-aware energy management for wireless sensor networks," in *Int. Workshop on Information Quality and Quality of Service for Pervasive Computing (IQ2S)*, pp. 8–13, 2011.