Poster: Infusing Trust in Indoor Tracking

Ryan Rybarczyk
Indiana University-Purdue University Indianapolis (IUPUI)
Indianapolis, IN
rrybarcz@cs.iupui.edu

Rajeev Raje
Indiana University-Purdue University Indianapolis (IUPUI)
Indianapolis, IN
rraje@cs.iupui.edu

Mihran Tuceryan
Indiana University-Purdue University Indianapolis (IUPUI)
Indianapolis, IN
tuceryan@cs.iupui.edu

ABSTRACT
An indoor tracking system is inherently an asynchronous and distributed system that contains various types (e.g., detection, selection, and fusion) of events. One of the key challenges with regards to indoor tracking is an efficient selection and arrangement of sensor devices in the environment. Selecting the "right" subset of these sensors for tracking an object as it traverses an indoor environment is the necessary precondition to achieving accurate indoor tracking. With the recent proliferation of mobile devices, specifically those with many onboard sensors, this challenge has increased in both complexity and scale. No longer can one assume that the sensor infrastructure is static, but rather indoor tracking systems must consider and properly plan for a wide variety of sensors, both static and mobile, to be present. In such a dynamic setup, sensors need to be properly selected using an opportunistic approach. This opportunistic tracking allows for a new dimension of indoor tracking that previously was often infeasible or unpractical due to logistic or financial constraints of most entities. In this paper, we are proposing a selection technique that uses trust as manifested by its a quality-of-service (QoS) feature, accuracy, in a sensor selection function. We first outline how classification of sensors is achieved in a dynamic manner and then how the accuracy can be discerned from this classification in an effort to properly identify the trust of a tracking sensor and then use this information to improve the sensor selection process. We conclude this paper with a discussion of results of this implementation on a prototype indoor tracking system in an effort to demonstrate the overall effectiveness of this selection technique.

CCS Concepts
• Information systems → Information systems applications → Spatial-temporal systems → Location based services.

Keywords
indoor tracking, sensors, subset selection, trust, accuracy.

1. INTRODUCTION
The ability to accurately track an object as it moves through an indoor environment remains an important and often difficult task. Such accurate indoor tracking is necessary in many application domains – e.g., asset tracking in a typical healthcare facility or providing first response to critical events. Unlike outdoor environments, in which there exists a single global tracking system that is readily available, there are no such pervasive options for indoor tracking. Instead, a mixture of different sensors and sensing techniques are often necessary in order to accurately track an object. Traditionally, indoor tracking has relied on statically deployed sensing infrastructure that is either non-pervasive and/or infeasible for many application domains. With the emergence of inexpensive sensors and the proliferation of mobile devices, often containing a wide range of sensing capabilities, it is now possible for many new application domains to make use of these sensors to track objects in an indoor environment. In addition, these new sensors can augment existing infrastructure, when present, and increase the scale and scope of the tracking process. This *ad-hoc*, or opportunistic, tracking creates many new challenges that did not exist or were not fully considered in a static tracking environment.

Irrespective the nature (i.e., static or dynamic) of the indoor tracking environment, any indoor tracking system is inherently an asynchronous and distributed system that includes various types of events such as object detection, sensor selection, and data fusion. Hence, a key task of any indoor tracking system is the event of sensor selection – a necessary precursor to the final calculation of the location information of a moving object. Selecting sensors then becomes critical in deciding which sensors to not only to use but also how to handoff between these sensors during the process of tracking. In the case of a static tracking infrastructure, the challenge of sensor selection is eased by the fact that the sensors are known a priori and an offline classification can often be constructed. Even in such a static scenario, the sensors themselves may behave unpredictably during the course of their deployment and thus, prove to be untrustworthy. For instance, in the case of a single modal environment (i.e., all sensors are of same kind and are functionally homogeneous) there still may be variations of that class of sensors present (e.g., cameras may have different properties and performance values) – these challenges are further exaggerated in a multi-modal system (e.g., a combination of vision and Wi-Fi sensors). Hence, the two key challenges that make sensor selection a difficult task in indoor tracking are: a) a wide variety of different classes of sensors having varying capabilities and characteristics and b) a dynamic and heterogeneous sensing infrastructure

In an effort to address these two challenges, we are proposing a technique that includes the integration of trust (defined as the conformance of a sensor's behavior to its specification) as the criterion during the selection process. Although trust of any indoor tracking system can be analyzed at both the functional and QoS levels here we focus only on the accuracy of the sensor – i.e., how accurately a sensor can compute the position of an object. Through the use of trust as a selection criterion, we are hypothesizing that the sensor selection can be improved which

DEBS '16, June 20-24, 2016, Irvine, CA, USA
ACM 978-1-4503-4021-2/16/06.
http://dx.doi.org/10.1145/2933267.2933538

This is the author's manuscript of the article published in final edited form as:
Rybarczyk, R., Raje, R., & Tuceryan, M. (2016). Infusing Trust in Indoor Tracking: Poster. In Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems (pp. 374–377). New York, NY, USA: ACM. https://doi.org/10.1145/2933267.2933538

will ultimately lead to increased overall accuracy provided by the tracking system.

The rest of the paper is organized as follows. Section 2 provides background on related work with respect to trust; Section 3 provides the framework for evaluating trust associated with the parameter of accuracy and its role in sensor selection; Section 4 conducts the performance evaluations and impact of the integration of the proposed framework into a prototype indoor tracking system; and Section 5 concludes the paper with a discussion of future work.

2. RELATED WORK

Trust has received much attention in literature with respect its role as a QoS parameter. Specifically, trust has been frequently used in wireless sensor networks (WSN) and the role it plays in sensor selection. At the same time, little research has been done with respect to examining the role of trust for sensor selection in the context of indoor tracking. In addition, most prevalent approaches consider trust as a generalized concept rather than focusing on its specific constituents such as accuracy. For the sake of brevity, below we describe only the prominent trust-related efforts, mainly from the domain of WSN. Classification of trust has been extensively explored in literature [3]. A majority of these approaches use collected evidences, through sampling, in order to establish either a belief or disbelief about the trustworthiness of an entity. This establishment of trust is nothing more than forming an opinion about the expected behavior of an entity. Hence, there is a level of uncertainty with respect to this opinion that is needed to be evaluated and considered as part of this establishment process. In [1], the author proposes the concept of subjective logic as a means to model this uncertainty or incomplete knowledge with the trust opinions. This approach results in a tuple that contains belief, disbelief, and uncertainty values which add to 1.

Specific relevant efforts related to the integration of trust into sensor networks can be found in [2] and [4]. In [2], the authors propose a framework that makes use of contextual information to collect evidences with respect to the expected behavior of a given sensor. This collecting of evidences is similar to our proposed approach but differs in the fact that their focus is on determining between faulty and malicious nodes as their criterion. In [4], the authors propose a combination between the use of an encryption technique and a trust management scheme. This combination is focused on the cost associated with such transmission in a sensor network and is not focused on the accuracy achieved with regards to the sensing data provided. Our work, in this paper, is focused on the overall accuracy achieved through trust-guided sensor selection.

3. TRUST

As indicated earlier, we define trust to be the level of belief/disbelief that a sensor's behavior (manifested by the accuracy of its data) will conform to its specification. This belief implicitly includes the behavioral history of a sensor and is determined by the evidences collected over the course of interactions with the sensor. This type of trust can be considered as data trust. This event of determining the validity of a sensor's data is important for the event of sensor selection and the accuracy of the tracking system as a whole. Formally, we define accuracy-related trust as the level of belief that a sensor will provide a precise location estimate of an object over a period of time. This trust-component is based upon the specification of a sensor and its past history.

In order to calculate the accuracy-related trust of a sensor, we must first examine the specifications of the sensors. We make the assumption that this information is made available by the manufacturer of that sensor and/or is provided by the developer of that sensor service[1] to the middleware layer upon the event of sensor service registration. With this information, we can then evaluate whether the actual performance (as depicted by the accuracy of the location estimate provided by a sensor) of the sensor meets or exceeds the expected performance (as indicated in the specification of that sensor). We use the following inequality for this comparison:

$$error.actual(x, y, z) \leq error.expected(x, y, z)$$

Each such comparison results in evidence. In an effort to evaluate these evidences, we are proposing the use of subjective logic defined in [1]. This approach uses a tuple consisting of belief, disbelief, and uncertainty {B, D, U}, where the sum of these three values is 1, to demonstrate the overall opinion about an entity. If the above inequalities are met then positive, or favorable, evidence is recorded. If the inequalities are not met then negative, or unfavorable, evidence is recorded. Finally, if the inequalities cannot be evaluated, due to lack of sufficient information, uncertain evidence is recorded. The goal of this tuple calculation process is to continuously collect evidences regarding a sensor throughout the course of interaction and then act upon these evidences to provide improved sensor selection.

To help in the process of collecting these evidences, we introduce the concept of accuracy agent into the framework of an indoor tracking system. The role of a tracking accuracy agent (TA) is to collect information regarding a sensor's performance and use this information to build the evidences (as previously described) in order to establish an opinion regarding a sensor. This agent can act in an active or passive manner while collecting evidences about the behaviors of the sensors. In an active manner, the TA can query the individual sensor for information directly; whereas in the passive role, it can simply observe the data being sent to the middleware layer. Each sensor participating in the tracking process is assigned a corresponding agent to monitor the sensor's behavior when the sensor is registered with the tracking system. This assignment is done by the tracking middleware during through service registration. In the case of failure of an agent, the tracking middleware is responsible for triggering an event process to create a replacement agent. This replacement agent will fill the void left by the failed agent and begin anew, the process of calculating the accuracy or responsiveness of the given sensor. These agents will then attempt to determine the respective accuracy or responsiveness of a sensor.

3.1 Accuracy-related Trust Framework

To evaluate the accuracy-related trust of a specific sensor, we need to examine the evidences collected by the sensor's TA. These evidences are used to compute the B, D, U tuple for that sensor. This tuple is then compared with a trust threshold value in order to determine whether the evidences collected prove that the sensor is trustworthy, untrustworthy, or undecidable. We define this comparison between the threshold value and the given tuple via the ">" operator as indicated by the equation below. In this equation, we define the trust ($\boldsymbol{t_S}$) of a sensor's ($\boldsymbol{S_i}$) data with respect to an object ($\boldsymbol{O_j}$)and the given threshold, $\boldsymbol{\delta_S}$,. \This threshold is determined by the tracking middleware by averaging

[1] We assume that each physical sensor is wrapped as a software service in this paper.

trust tuples of obtained from other TAs for a particular sensing modality. The initial threshold value for the tracking system is established as {0, 0, 0}. This is also the default value associated with the threshold in the case in which no other TAs are present and thus, no global threshold can be determined due to insufficient information. This method allows for the tracking system to dynamically adapt based upon the current tracking infrastructure and account for the presence of mobile, or transient, sensors.

$$t_S(S_i, O_j) > \delta_S$$

If the above inequality is met then the sensor can be classified as trustworthy and its corresponding evidence associated with the belief is incremented. Similarly, if the inequality is not met then the evidence associated with the disbelief is incremented. Finally, if sufficient data is not available then the evidence associated with the uncertainty part is incremented. The modification of these evidences and associated normalization is indicated below. The tuples created by using the below algorithm are used in the selection process as discussed in the next subsection.

Input: Sensor Set *S,* Object *O*
Output: *B, D, U* – *S*[n]

for each sensor S[n] in S (where n = {0, ⋯ , S.length})
| if SUFFICENT_DATA_AVAILABLE(S[n]]) then
| | if S[n]. $actual(O) \leq S[n].expected(O)$ then
| | | evidence(S[n])$_{\text{belief}}$ + +
| | elseif S[n]. $actual(O) > S[n].expected(O)$ then
| | | evidence(S[n])$_{\text{disbelief}}$ + +
| else evidence(S[n])$_{\text{uncertainty}}$ + +
| B = evidence(S[n])$_{\text{belief}}$ / sum(evidence(S[n]])
| D = evidence(S[n])$_{\text{disbelief}}$ / sum(evidence(S[n]])
| U = evidence(S[n])$_{\text{uncertainty}}$ / sum(evidence(S[n]])
| return {*B, D, U*}
end

3.2 Sensor Selection

We are proposing an improved sensor selection algorithm, shown below, that makes use of a selection criterion, *C*. *C* in this case is based on the accuracy – but in theory, it could be any type of selection criterion that can filter the sensors accordingly and thus, provide the output of a subset of sensors (S_i).

Input: Sensor Set *S*, Selection Criteria *C*
Output: Subset of Sensors S_i

1. Identify the ground truth sensor S_{Ground} in *S*.
2. Apply the Accuracy Analysis to each sensor *S[n]* in *S* (where n = *{0, …, S.length}*) given the ground truth sensor S_{Ground}.
3. Filter the sensors based upon the analysis of the selection criteria *C*.
   - If $S[n].belief_{Accuracy}$ meets/exceeds the *C* requirement then add *S[n]* to S_i.
4. Repeat Step 3 until all sensors have been evaluated based upon the selection criteria.
5. Return array of subset of sensors S_i.

This selection criterion is an evaluation of the required performance level versus the actual performance level of a given sensor. This required performance level is specified by the application domain due to specific constraints or requirements. In this case, we make use of the tuples associated with accuracy and evaluate each entry in these tuples with respect to the selection criteria, *C*. For this action, we are evaluating the belief we have in the given tuples with respect to accuracy-related trust components and the given selection criteria.

4. EXPERIMENTATION

The approach described in section 3 has been implemented into an existing prototype indoor tracking system, the eDOTS [5]. This system was selected due in part to it being open and available, and providing the opportunity to discover and use different classes of tracking sensors. These extensions were then tested with the use of 20+ sensors (the vast majority being stationary Web Cameras attached to desktop machines) that were networked to machines running Windows 7 with 8 GiB of RAM. Three different types (of varying characteristics and qualities) of Web Cameras were used, to simulate vision-based tracking, along with mobile devices using wireless cards for signal strength trilateration.

The accuracy was defined through physical measurements taken in the environment and recorded through markers placed for reference. This information was then compiled off-line and used to analyze the overall performance of the tracking system with respect to the accuracy provided. The unit of the location measurement for all experiments was in meters.

The initial set of experiments was conducted in order to focus on the integration of trust-based accuracy into the tracking system. Each sensor upon registration was assigned a corresponding tracking accuracy agent (TA) that collected the specifications, per the service contract, and sampled the location data when available. These TAs then reported this data back to the middleware layer for analysis and ultimately a trust-based decision. These accuracy experiments were split into three categories based upon initial trust assignment: optimistic, pessimistic, neutral. In the optimistic approach the tracking system made the assumption that all sensors, upon registration, were trustworthy – and thus had a b, d, u tuple value of {1.0, 0, 0}. In the pessimistic approach, all of the sensors were assumed to be untrustworthy – and thus had a tuple value of {0, 1.0, 0}. Finally, in the neutral approach, the system assumed that insufficient data was available for the sensors and thus a level of uncertainty persisted – and hence, a value of {0, 0, 1.0} was assigned for each sensor.

The first experiment, to evaluate this trust-based accuracy, was to verify that the trust tuple associated with the accuracy was indeed being properly set and maintained for an individual sensor. To validate the existence of such tuples for each of the different categories, we identified a sensor that we knew to be trustworthy, in terms of its accuracy, and one that we knew to be untrustworthy, in terms of its accuracy, and ran our algorithm against these sensors. We achieved this identification of sensors through offline calibration of the sensor devices. In this test, only stationary sensors were used to mitigate the opportunity for additional error in regards to the location estimate into the final result. For each category and each sensor, we ran 100 data points through the algorithm and then examined the resulting trust scores. Tables 1, 2, and 3 highlight our findings for both the sensors in their respective categories – sensor A being the predefined trustworthy sensor and sensor B being the predefined untrustworthy sensor.

Table 1. Empirical Accuracy Analysis (Optimistic)

Sensor Name	Belief	Disbelief	Uncertainty
Sensor A	0.824	0.167	0.010
Sensor B	0.175	0.815	0.010

Table 2. Empirical Accuracy Analysis (Pessimistic)

Sensor Name	Belief	Disbelief	Uncertainty
Sensor A	0.813	0.176	0.010
Sensor B	0.098	0.892	0.010

Table 3. Empirical Accuracy Analysis (Neutral)

Sensor Name	Belief	Disbelief	Uncertainty
Sensor A	0.819	0.171	0.010
Sensor B	0.152	0.838	0.010

From Tables 1, 2, and 3, we can see that the algorithm appropriately determined the {B, D, U} tuples for the respective sensors. This analysis confirms the ground truth that we knew about each sensor going into the experiment regarding its trustworthiness, in terms of its accuracy. In each case, the algorithm provided a probability regarding the sensor's performance at 0.810 or higher. The one concern with this approach was the lack of true modeling of the uncertainty in the sensor's performance. We believe the reason behind the unchanging value of this parameter is due in part to the sample size that we were using to evaluate.

The final experiment explored the actual location accuracy that this new selection technique provided to the modified eDOTS. In this experiment, we did not pre-flag sensors based upon their expected performance. Instead, we attempted to simulate a realistic tracking environment and made use of the sensors "as is" within the sensing infrastructure. In order to validate our work, we ran identical experiments for both before the integration of accuracy guided sensor selection and then after. A tracking path, for moving an object, was determined and mapped within the lab environment in an effort to have maximum sensor coverage. Our goal was to provide a scenario in which we were always being tracked by at least five different sensors.

Figure 1 shows a visual representation of the output of the eDOTS without the presence of accuracy and responsiveness-guided sensor selection. This figure shows the prototype using its existing sensor selection technique in which the sensors are ranked based upon their modality classification [5]. The solid line in the figure represents the actual path of the object as it travelled through the environment.

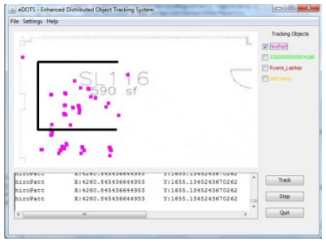

Figure 1. Without Accuracy and Responsiveness-guided Selection

Figure 2 shows a visual representation of the output of the eDOTS with the presence of accuracy and responsiveness-guided sensor selection. This figure shows the prototype while using our proposed selection algorithm. The solid line in the figure represents the actual path of the object as it travelled through the environment.

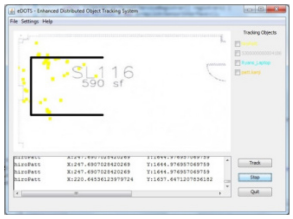

Figure 2. With Accuracy and Responsiveness-guided Selection

The empirical data regarding the actual versus the estimate error encountered by the system is shown in Table 4. This data verifies that the new selection technique did slightly improve the accuracy of the system and with the previously stated real lack of any additional overhead in terms of cost demonstrated the effectiveness of our proposed techniques within a prototypical indoor tracking system.

Table 4. Average Estimated Error

	Average Estimated Error (meters)
eDOTS	1.35
eDOTS (w/ Sensor Selection)	0.97

5. CONCLUSION

This paper has described the infusion of trust into an indoor tracking system with the goal of improved sensor selection and ultimately improved location estimate accuracy. The empirical data collected provides a generic benchmark for the application of this selection criteria and its important role in event-driven task of identifying subsets of sensors for the purpose of tracking. Future work includes analyzing the cost-benefit tradeoff with respect to the inclusion of other QoS parameters and the sensor selection process. This future work also includes the integration of an optimization function and the analysis of learning techniques to adapt and build system benchmarks for the application, development, and deployment of indoor tracking systems based upon specific application domain needs.

REFERENCES

[1] A. Josang. An algebra for assessing trust in certification chains. In Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999.

[2] W. Li., A. Joshi, T. Finin, "Cast: Context-aware security and trust framework for mobile ad-hoc networks using policies." Distributed and Parallel Databases, 31(2), pp.353-376, 2012.

[3] M. Momani, S. Challa, Survey of trust models in different network domains. International Journal Ad Hoc Sensors and Ubiquitous Computing, 1-19, 2010.

[4] N. Poolsappasit, M. Busby, S. Madria, "Trust Management of Encrypted Data Aggregation in a Sensor Network Environment," In Mobile Data Management (MDM), 2012 IEEE 13th International Conference on, pp. 157-166, 2012.

[5] R. Rybarczyk, R. Raje, M. Tuceryan, eDOTS 2.0: A Pervasive Indoor Tracking System, In Proceedings of the International Conference on Software Engineering and Knowledge Engineering (SEKE'13), pp. 429-434, Boston, MA, 2013.