Procedia Computer Science

Volume 51, 2015, Pages 2483–2492

ICCS 2015 International Conference On Computational Science

Security and Privacy Dimensions in Next Generation DDDAS/Infosymbiotic Systems: A Position Paper

Li Xiong[1] and Vaidy Sunderam[1]

Emory University, Atlanta, Georgia, USA
lxiong,vss@emory.edu

Abstract

The omnipresent pervasiveness of personal devices will expand the applicability of the Dynamic Data Driven Application Systems (DDDAS) paradigm in innumerable ways. While every single smartphone or wearable device is potentially a sensor with powerful computing and data capabilities, privacy and security in the context of human participants must be addressed to leverage the infinite possibilities of dynamic data driven application systems. We propose a security and privacy preserving framework for next generation systems that harness the full power of the DDDAS paradigm while (1) ensuring provable privacy guarantees for sensitive data; (2) enabling field-level, intermediate, and central hierarchical feedback-driven analysis for both data volume mitigation and security; and (3) intrinsically addressing uncertainty caused either by measurement error or security-driven data perturbation. These thrusts will form the foundation for secure and private deployments of large scale hybrid participant-sensor DDDAS systems of the future.

Keywords: security, privacy, dddas, infosymbiotics

1 Introduction

The DDDAS paradigm provides a powerful framework for applications in which simulations are dynamically integrated in a feedback loop with real-time data-acquisition and control components. Increasingly, these systems critically depend on *security* (protecting data integrity) and *privacy* (safeguarding sensitive information) in their measurement, feedback, control, and imperative phases. In particular, hybrid systems comprising both sensors and human participants fundamentally alter privacy and security requirements. At the same time, increased heterogeneity, complexity, and scale lead to technical challenges to ensure data integrity in the presence of uncertainty and faults. New mechanisms are urgently needed to integrally support large scale DDDAS systems manifesting such combinations of privacy, security, heterogeneity and uncertainty attributes. Including security and privacy functionality integrally within DDDAS frameworks will enhance adoption and facilitate their use in numerous emerging settings.

Selection and peer-review under responsibility of the Scientific Programme Committee of ICCS 2015

doi:10.1016/j.procs.2015.05.357

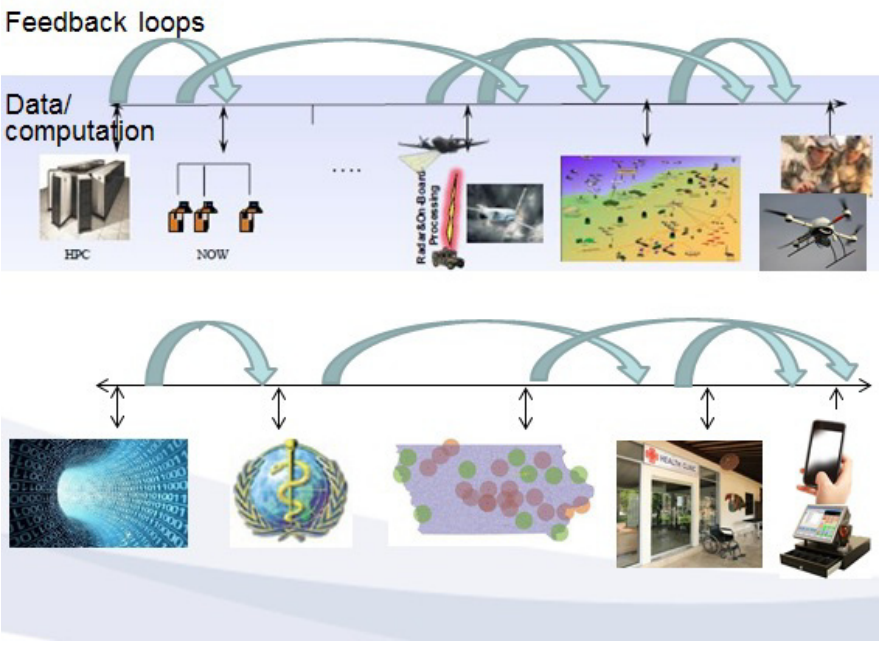

Figure 1: Crowdsensing participation in DDDAS systems

The major extension we envision to next generation DDDAS systems as shown in Figure1 [1] is the engagement of human or crowdsensing participants – both in the measurement domain and the simulation domain. Participants possessing one or more smart devices and wearable computers offer a tremendous expansion in opportunities for DDDAS-based applications, as observation and measurement entities and as local-regional simulation platforms to enable hierarchical feedback driven adaptive systems. In the general case, such entities are not dedicated or owned by an application (e.g. UAVs/UGVs) nor do they necessarily have secure communication channels to central servers. However, their privacy and security must be guaranteed to achieve high levels of voluntary participation and use.

We envision a hierarchical DDDAS architecture that consist of multiple loosely organized local cohorts of participants and sensors at the "field" level, one or more intermediate levels of "regional" computational or simulation engines (or data repositories), and possibly a centralized high-end system where appropriate to an application. Interactions and feedback-driven measurement, analytics, and decision-making can and do occur at each level, as well as across levels in the hierarchy. Canonically, end-devices (participants and sensors) make measurements or observations upon which individual or local cooperative analysis may be performed, raw or aggregated data is fed into regional or central simulations, that in turn provide steering feedback to the end-devices. In this position paper, we propose privacy and security overlays on this DDDAS model, identify some of the critical issues to be addressed in such an enhanced feedback driven adaptive system and propose several key approaches to security, privacy and uncertainty handling.

[1]Original DDDAS paradigm depicted in Figure 1 due to Dr. Frederica Darema (http://1dddas.org), reproduced with permission. Dr. Darema reserves all rights to use graphic in Figure 1 or portions thereof in future presentations or publications without express consent

2 Central Concepts

The key tenet of our approach is that *privacy preserving techniques can work in tandem with uncertainty handling, multi-source data assimilation and adaptive decision support* to provide an integrated framework for dynamic data driven sensor-participant application systems. In DDDAS systems, uncertainty can result from multiple sources e.g. measurement noise, unpredictable trajectories, and perturbation or cloaking for obfuscation; techniques to handle privacy-induced uncertainty can address other causes as well. Similarly, aggregation or consolidation are methods employed to manage large data volumes; privacy preserving techniques can be superimposed on such schemes without degrading utility. When data from multiple sources are combined – either to reduce volume or to increase fidelity – algorithms to weight the credibility of individual inputs can simultaneously protect private source data. Secure multiparty computation schemes can enable localized-distributed DDDAS decision-making, thereby reducing delays and expensive communications, without disclosing sensitive data.

Our framework seeks to fundamentally advance the state-of-the-art in privacy preserving and secure DDDAS. We initially focus on hybrid participant-sensor systems and investigate techniques for: dynamic sensor-participant task management and alerts, aggregation of multiple data streams/observations with confidence metrics, and localized distributed computations for multi-level decision making. Our ongoing PREDICT [2] project that has established preliminary foundations for privacy-enabled DDDAS will be enhanced as a hierarchical, nested-feedback architecture that is scalable and resilient to uncertainty and failures. It is intended to support dynamic task assignment, multi-source data acquisition and fusion, decision support and control. Specifically, we are developing an adaptive privacy-preserving hybrid framework for DDDAS that addresses:

1. *Secure feedback-driven task assignment and alerts* in the context of cloaked or encrypted sensor-participant location data, including dynamic trajectory prediction to optimize sensing cost and target coverage.
2. *Privacy-preserving data assimilation* for modeling data streams from sensors, devices and participants, correlating and combining them with high fidelity and low disclosure.
3. *Distributed-localized secure computing* that is resilient to uncertainty and faults, and enables semi-autonomous decision making at multiple levels in the simulation and feedback loops of the DDDAS paradigm.

3 Background and Context

In addition to greatly increased complexity and scale, the next generation of DDDAS/Infosymbiotics frameworks will depend critically on *security and privacy* in the data acquisition, transmission, feedback and control phases of an application. DDDAS systems are becoming much more comprehensive and now include human participants at all levels including data acquisition, policy, steering and computation. As demonstrated by numerous crowdsensing applications, literally every human can engage in, and contribute to, various subsets of applications in DDDAS arenas. While there is tremendous and limitless potential for leveraging the capabilities of participants to complement sensors, devices, networks and algorithms, engagement by participants is predicated on security and privacy protection, in terms of identity and location disclosure as well as other factors such as trajectory and temporal activity characteristics. Next generation DDDAS frameworks must centrally address participant management with security and privacy preservation [15, 1, 11, 4].

[2] PREDICT is an acronym for PRivacy Enhancing Dynamic Information Collection and moniToring

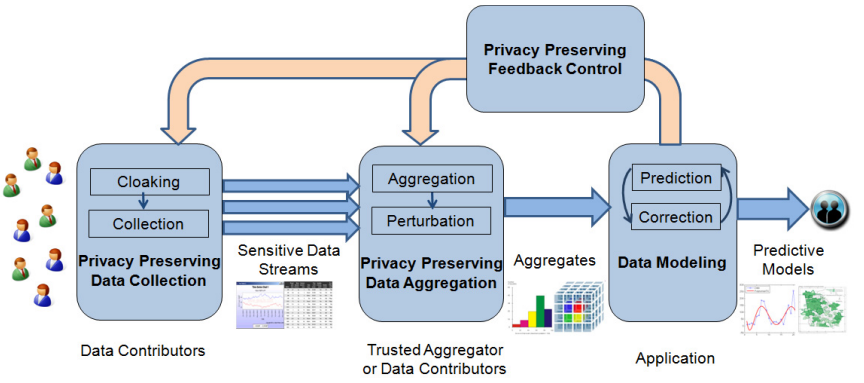

Figure 2: PREDICT Architecture

In current and emerging DDDAS systems, exponentially increasing data are acquired by participants, heterogeneous sensors and controllers, each with greatly improved computational capabilities. Applications involving complex streaming data are sensitive to privacy concerns as well as to volume issues, especially when participant data and sensor data are fused in complementary ways. These situations will benefit greatly from privacy protection coupled with reduced data modeling. Data uncertainty brings additional challenges, with sensors subject to measurement error, power, environmental and component failure issues while reliability of participant-provided data is susceptible to human factors. Thus there is a need to perform aggregation and condensed data representation, while maintaining sufficient integrity to enable decision making at all levels, including locally.

Privacy mechanisms are coincidentally well-aligned with techniques that deal with uncertainty, complexity, and volume challenges. For example, target tracking can be accomplished cooperatively by participants whose exact locations are unknown (e.g. either deliberately obscured for privacy or due to measurement inaccuracy) by using privacy-preserving probabilistic task assignment schemes [13]. In many DDDAS settings, high volume data can be aggregated in ways that retain key statistical properties; equivalent algorithms can be developed that add privacy-protection while simultaneously reducing volume, and maintaining high information fidelity [6, 5]. Advances in privacy and security can also enable localized distributed processing through mechanisms such as secure multi-party computation that does not divulge private data to untrusted peers but can compute decision-support functions without the need for a (trusted, but distant and therefore expensive) central server [8].

Foundational Work We have established the viability of such approaches in the foundational phase of the PREDICT project, and have developed several new techniques for privacy preserving task assignment, stream data sampling and aggregation, and multiparty computation. Our feedback driven framework focusing on privacy preserving data collection, data aggregation, and data modeling is illustrated in **Figure 2**.

Detailed descriptions and results in each of the privacy-preserving collection, aggregation, and modeling stages in PREDICT are described elsewhere, but to briefly summarize:

1. Privacy preserving data collection with feedback control – we consider the problem of assigning data-targets to participants with privacy protection (using cloaked participant

locations), while maximizing coverage and minimizing (travel) costs. Using a two-stage process where a central server makes initial assignments using cloaked locations that are refined locally by individual participants, we show that high levels of coverage can be achieved with reasonable cost when participants and targets are fixed. In many DDDAS settings, mobile targets and participants are the norm and we are developing extensions to handle the much more challenging and fundamentally different situation involving multiple moving targets and uncertain/unreliable, mobile, participants.

2. Privacy preserving data aggregation and modeling with feedback control – in many situations, aggregating and sampling can reduce data volume while providing functionally adequate information content. We have developed techniques to deliver high data utility/integrity, with rigorous privacy guarantees such that source data is not disclosed. Data are assumed to be single stream, and "true". In emerging DDDAS systems, multiple uncertain streams (from sensors and participants) need to be fused, and characterized with a confidence metric that quantifies the trust level of the function output, a focus of our ongoing work.

3. In many DDDAS settings, (parts of) simulations may be performed locally or regionally, to minimize expensive or vulnerable communication with central servers. When local participants are mutually untrusted, and for increased responsiveness in the field, such computations must be performed without disclosing individual input values, true participant locations, or other sensitive information. Our preliminary work on secure computations without a trusted aggregator has demonstrated the viability of such mechanisms, and will form the basis for specific types of distributed-localized, secure versions of filtering, trajectory prediction, and decision-support algorithms.

In the ongoing and future phase outlined in this paper, we articulate several research challenges that still remain to be addressed in privacy and security, both in the context of the DDDAS model but also leveraging its capabilities and strengths.

Applications and Impact The proposed research will help overcome data privacy and security barriers and have significant impact in enabling DDDAS applications for an even wider range of domains. For example, real-time traffic activity, vehicle movements, and their environmental impacts can be measured and aggregated (through road-embedded sensors, traffic cameras and crowdsensing participants) for coordinated and environmental-friendly transportation planning. Since spatio-temporal vehicle information can disclose sensitive data about individuals, privacy preservation is imperative. Similarly, user downloads of voice, data and streaming video (again a privacy sensitive activity) can be aggregated in content and pattern analysis for real time load balancing in content delivery networks. Systems such as WIPER [14] have been proposed to use real-time aggregate cell phone data for dynamic population movement prediction and emergency response – viable only if user privacy is guaranteed. UAV/UGV systems for monitoring, e.g. crowd monitoring for border control, can be greatly enhanced through augmentation with crowdsensing participants (with assured privacy protection) who can respond and adapt in intelligent ways to the needs of the DDDAS application. Inevitably, in all these scenarios, user privacy issues arise in task assignment and acceptance, data collection, and usage modes. Data acquisition, aggregation and localized computation must be enabled in dynamic and adaptive ways that are compatible with DDDAS while maintaining provable privacy guarantees and quantifiable uncertainty bounds to make these systems a true reality.

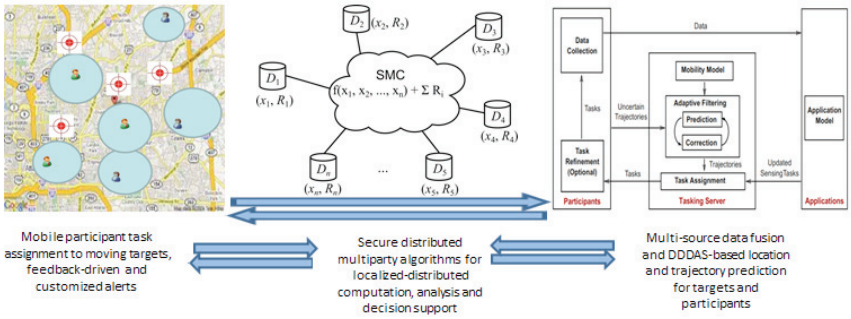

Figure 3: Next Generation DDDAS with Privacy and Security

4 Next Generation DDDAS with Privacy and Security

We are developing an adaptive privacy preserving framework for hybrid DDDAS systems focusing on dynamic participant management, data synthesis and localized-distributed computations, as illustrated in **Figure 3**. Our framework is intended to be realized as a hierarchical, nested-feedback architecture where local processing feeds consolidated data into higher level simulations that in turn provide steering, feedback, alerts and control signals.

The major thrusts of the PREDICT project include:

- *Privacy preserving dynamic crowd sensing task assignment* methods for adaptively assigning mobile targets to varying numbers of moving participants whose locations are cloaked. Given uncertain trajectories of participants, we are investigating schemes based on building mobility models and estimating (current and predicted) locations guided by filters and feedback loops for dynamically (re)assigning sensing tasks.

- *Data synthesis and validation techniques* for assessing data content and integrity in the presence of uncertainty. Sensor data and participant input are each subject to uncertainty; we are developing techniques to combine data sources based on trust estimates to deliver assimilated data with high confidence levels in DDDAS systems.

- *Secure localized distributed computation* to enable hierarchical processing and decision making, both for responsiveness and to leverage high end computational capabilities at end-computing devices, while reducing high volume data communication loads and security compromise risks.

Our preliminary approaches to each of these thrusts is outlined below.

Privacy preserving dynamic crowd sensing task assignment. We consider a group of loosely coupled participants who are mutually addressable but whose exact locations are not disclosed to the cohort. This set of participants, either autonomously or augmented by a central server is to be collectively tasked with a cooperative effort e.g. target tracking. One current application scenario concerns tracking a specific vehicle moving through an urban area [7] for destination prediction and other uses. Another is surveillance and crowd control by a heterogeneous team of participants, UAVs and UGVs [10]. In these and similar scenarios, subsets of participants are dynamically assigned to make observations about their assigned targets, including trajectory estimation and rates of movement.

We are developing models for spatial task assignment in mobile crowd sensing that uses a dynamic and adaptive data driven scheme to assign moving participants with uncertain trajectories to sensing tasks, in a near-optimal manner. Our scheme explores building a mobility model from available trajectory history and estimating posterior location values using noisy/uncertain measurements upon which initial tasking assignments are made. These assignments can then be refined locally (using exact location information) and used by participants to steer their future data collection, completing the feedback loop.

In this project thrust, several research challenges are encountered:

1. Given partial trajectory history of a moving target and cloaked locations of n participants, how to assign subsets of participants such that at a series of future times, the target is covered by at least k participants. This challenge may be extended to map a set of participants to multiple moving targets, maximizing coverage while minimizing cost.

2. Given *mobile* participants whose trajectories are cloaked, each of whom may only accept assignments with a certain probability, assign subsets of participants to targets, maximizing coverage and minimizing cost.

Our preliminary approach to these research challenges is outlined below. To formulate the location transition process, Bayesian inference and Markov model are two popular methods which are being examined. For example, a grid-based road network with mapped trajectories can be used to build a Bayesian inference framework for next location prediction [16]. Similarly, a Markov model can be constructed which assumes a state for each node of a network, and for each pair of adjacent nodes, both transition directions are considered and the probability of each directed edge can be calculated based on location transition probabilities.

We are exploring a filtering component in our framework that provides estimates of noisy locations in order to improve the accuracy of location information. Using one of the mobility models above, a linear state space can be created and coupled with an observation model and a filtering algorithm can be used for posterior estimation of the true state to minimize error. This output, i.e. a set of filtered uncertain locations, can then be used in task assignment based upon new algorithms that optimize the assignment process using techniques from spatio-temporal approaches, including *k closest pairs of objects* (K-CPQ) [3] and bounding area methods. Initial assignments are then refined locally where true location information is used to further optimize assignments while maximizing application goals.

Data synthesis and validation techniques. In DDDAS application scenarios with possibly moving targets or data sources, sensing and data measurement/observation tasks are conducted by fixed and varying groups of mobile sensors and mobile participants. Observations especially from the latter two are subject to uncertainty and unreliability for reasons ranging from measurement inaccuracies to power issues to communication error to, in the case of participants, human ability, willingness, and security constraints.

The major challenges to be addressed to account for such uncertainties include:

1. Given multiple time series observations referring to the same event or phenomenon, each with some measurement error or privacy perturbation, how can we combine them to derive an estimation of the phenomenon that is as close as possible to the ground truth?

2. Further, if a subset of these observation streams are time-lagged, missing, or of different modalities, can they be fused to form an accurate estimate, especially if each source can be associated with a trust level?

The technical approaches we are adopting to address this challenge are as follows. We are attempting to develop methods that enhance knowledge and data accuracy about particular targets by combining sensor/participant data in ways that increase confidence levels in the fused information about a target or event. One issue concerns co-identification, i.e. recognizing an event or target as equal when reported upon by independent sensors, for which we are exploring spatio-temporal registration as well as repeated image identification techniques and named events such as those used by certain crowdsourcing applications. To compensate for unreliable inputs however, we need to develop trust-based mechanisms that combine historical information with modeling to improve confidence.

Methods based on probabilistic modeling offer the greatest promise. Recent works [12] have used graphical probabilistic models for truth discovery in crowdsourced detection of spatial events. However, they only consider the static case where the input is the user report at a given time stamp. We plan to extend the graphical models to consider dynamic users and temporal spatial events. We are analyzing a probabilistic framework that integrates the modeling of *time-variant* location popularity, participant reliability (trustworthiness), the trajectories and the temporal and spatial distributions of participants, peer behavior, as well as the spatial and temporal information of events/targets. We envision such a framework will allow dynamic and automatic data synthesis and validation while efficiently handling various types of uncertainty and unreliability.

In this regard, we expect to adopt from information fusion work that is closely related to our efforts. For example, consensus-based filters have been used effectively for cooperative space object tracking [9]. Another closely related project is the URREF framework[2] that permits the specification of uncertainty levels and information credibility in fusion systems. In our approach we plan to generate parameterized estimations of spatio-temporal events from real and simulated data, and derived trust levels among crowd sensing participants. The theory of trust in multimodal fusion settings from URREF and similar projects will provide a platform for evaluating the effectiveness of our approaches to trust quantification.

Secure localized distributed computation. We adopt the most generalized interpretation of the DDDAS model wherein feedback loops are nested and hierarchical; data is adaptively collected and fused at lower levels providing input to simulations at higher levels, which in turn drive the collection process. In addition, there is also substantial potential and value in data transformations and simulations among peer entities at each level, i.e. localized distributed computations enabling feedback-driven decision making. In addition to greater responsiveness and reacting to local conditions, such an enhancement to DDDAS has several advantages including minimizing communication costs in low power devices, avoiding costly encryption and key management, and adapting to uncertainties and failures.

To facilitate both a model and practical scaffolding to enable multi-level nested feedback loops in DDDAS, several technological challenges must be overcome:

1. Analyzing and developing secure multiparty computation versions of key DDDAS algorithms such as multi-observation filtering and distributed consensus, e.g. trajectory prediction based on multi-perspective observations, collaborative assignment of participants to targets without mutual disclosure of exact participant locations.

2. Estimating performance tradeoffs between localized-distributed computation vs. encryption followed by transmission of observations to centralized trusted aggregator; quantifying temporal responsiveness in localized vs. centralized decision-support computations.

Secure multiparty computation is a key requirement for such localized distributed actions. We are building upon our recent work in developing efficient and distributed algorithms that can

perform certain types of computations while preserving data confidentiality [8]. For example, a group of participants tracking a moving target might perform secure multiparty filtering and trajectory estimation based on their own (private) locations to locally reassign monitoring responsibilities. For all the algorithms we develop in participant task management and data synthesis areas, we will develop the counterpart secure multiparty computation protocols to allow localized task assignment for data acquisition as well as field processing of combined participant and sensor data data.

For example, assigning static targets to participants that only disclose cloaked locations in a cost-optimal manner was previously accomplished by first transmitting cloaked locations to a central server whose preliminary assignments were then refined locally. A distributed version of the same is straightforward to implement via all-to-all sharing of cloaked locations and replicated local computations. Indeed, better results are likely due to the additional information available in the first stage of the process. A substantially bigger challenge is to make such assignments in the case of a moving target with only instantaneous trajectory vector information. In addition to distributed algorithms to compute such functions, a programming model and autonomous computing infrastructure will be required; we are investigating middleware for a distributed field setting that incorporates entity naming and addressing, communication protocols, and data alignment, correlation and analysis.

5 Summary

In this paper we posit that next generation DDDAS systems will critically depend on privacy and security, and conversely, that the provision of such functionality will greatly expand the applicability domain of the DDDAS paradigm. Our key insight is that mechanisms and data transformations for privacy preservation have a three-way benefit in protecting disclosure of sensitive data, aggregation to reduce data volumes and offset uncertainty, and enable local distributed computing that facilitates multi-level hierarchical feedback driven adaptive systems. We describe foundational work in these areas and outline new challenges as well as possible approaches to address them. Methodologies and techniques resulting from these efforts will provide significantly enhanced functionalities for emerging future generation DDDAS/Infosymbiotics systems.

6 Acknowledgments

This research is supported by the Air Force Office of Scientific Research (AFOSR) DDDAS program under grant FA9550-12-1-0240.

References

[1] *Report of the August 2010 Multi-Agency Workshop on InfoSymbiotics/DDDAS, The Power of Dynamic Data Driven Applications Systems.* Workshop sponsored by: Air Force Office of Scientific Research and National Science Foundation.

[2] Erik Blasch, Audun Jøsang, Jean Dezert, Paulo C. G. Costa, and Anne-Laure Jousselme. URREF self-confidence in information fusion trust. In *17th International Conference on Information Fusion, FUSION 2014, Salamanca, Spain, July 7-10, 2014*, pages 1–8, 2014.

[3] Muhammad Aamir Cheema, Xuemin Lin, Haixun Wang, Jianmin Wang, and Wenjie Zhang. A unified framework for answering k closest pairs queries and variants. *IEEE Transactions on Knowledge & Data Engineering*, 26(11), 2014.

[4] Delphine Christin, Andreas Reinhardt, Salil S. Kanhere, and Matthias Hollick. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11):1928 – 1946, 2011. Mobile Applications: Status and Trends.

[5] Liyue Fan and Li Xiong. An adaptive approach to real-time aggregate monitoring with differential privacy. *IEEE Trans. Knowl. Data Eng.*, 26(9):2094–2106, 2014.

[6] Liyue Fan, Li Xiong, and Vaidy S. Sunderam. Differentially private multi-dimensional time series release for traffic monitoring. In *Data and Applications Security and Privacy XXVII - 27th Annual IFIP WG 11.3 Conference, DBSec 2013, Newark, NJ, USA, July 15-17, 2013. Proceedings*, pages 33–48, 2013.

[7] Richard Fujimoto, Angshuman Guin, Michael Hunter, Haesun Park, Gaurav Kanitkar, Ramakrishnan Kannan, Michael Milholen, Sabra Neal, and Philip Pecher. A dynamic data driven application system for vehicle tracking. In *Proceedings of the International Conference on Computational Science, ICCS 2014, Cairns, Queensland, Australia, 10-12 June, 2014*, pages 1203–1215, 2014.

[8] Slawomir Goryczka, Li Xiong, and Vaidy S. Sunderam. Secure multiparty aggregation with differential privacy: a comparative study. In *Joint 2013 EDBT/ICDT Conferences, EDBT/ICDT '13, Genoa, Italy, March 22, 2013, Workshop Proceedings*, pages 155–163, 2013.

[9] Bin Jia, Khanh D. Pham, Erik Blasch, Dan Shen, Zhonghai Wang, and Genshe Chen. Cooperative space object tracking using consensus-based filters. In *17th International Conference on Information Fusion, FUSION 2014, Salamanca, Spain, July 7-10, 2014*, pages 1–8, 2014.

[10] Amirreza M. Khaleghi, Dong Xu, Zhenrui Wang, Mingyang Li, Alfonso Lobos, Jian Liu, and Young-Jun Son. A dddams-based planning and control framework for surveillance and crowd control via uavs and ugvs. *Expert Syst. Appl.*, 40(18):7168–7183, 2013.

[11] N.D. Lane, E. Miluzzo, Hong Lu, D. Peebles, T. Choudhury, and A.T. Campbell. A survey of mobile phone sensing. *Communications Magazine, IEEE*, 48(9):140–150, Sept 2010.

[12] R. W. Ouyang, M. Srivastava, A. Toniolo, and T. J. Norman. Truth discovery in crowdsourced detection of spatial events. In *ACM International Conference on Information and Knowledge Management (CIKM)*, 2014.

[13] Layla Pournajaf, Li Xiong, Vaidy S. Sunderam, and Slawomir Goryczka. Spatial task assignment for crowd sensing with cloaked locations. In *IEEE 15th International Conference on Mobile Data Management, MDM 2014, Brisbane, Australia, July 14-18, 2014 - Volume 1*, pages 73–82, 2014.

[14] Timothy Schoenharl, Student Member, Ryan Bravo, and Greg Madey. Wiper: Leveraging the cell phone network for emergency response. *International Journal of Intelligent Control and Systems*, 11:2006, 2007.

[15] Katie Shilton. Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. *Commun. ACM*, 52:48–53, November 2009.

[16] Andy Yuan Xue, Rui Zhang, Yu Zheng, Xing Xie, Jin Huang, and Zhenghua Xu. Destination prediction by sub-trajectory synthesis and privacy protection against such prediction. In *Proceedings of the 2013 IEEE International Conference on Data Engineering (ICDE 2013)*, ICDE '13, pages 254–265, Washington, DC, USA, 2013. IEEE Computer Society.