

Data Alcott Systems  
 Old No.13/1, New No.27, Third Floor  
 Brindavan Street  
 West Mambalam  
 Chennai – 600033  
 Ph: (0)9600095047  
<http://www.finalsemprojects.com>  
<http://www.dataalcott.com>

## IEEE 2010 TITLES

S.NO	ABSTRACT	TECHNOLOGY
1.	<p><b>BINRANK: SCALING DYNAMIC AUTHORITY-BASED SEARCH USING MATERIALIZED SUBGRAPHS</b></p> <p>--- : KNOWLEDGE AND DATA ENGINEERING</p> <p>Dynamic authority-based keyword search algorithms, such as ObjectRank and personalized PageRank, leverage semantic link information to provide high quality, high recall search in databases, and the Web. Conceptually, these algorithms require a querytime PageRank-style iterative computation over the full graph. This computation is too expensive for large graphs, and not feasible at query time. Alternatively, building an index of precomputed results for some or all keywords involves very expensive preprocessing. We introduce BinRank, a system that approximates ObjectRank results by utilizing a hybrid approach inspired by materialized views in traditional query processing. We materialize a number of relatively small subsets of the data graph in such a way that any keyword query can be answered by running ObjectRank on only one of the subgraphs. BinRank generates the subgraphs by partitioning all the terms in the corpus based on their co-occurrence, executing ObjectRank for each partition using the terms to generate a set of random walk starting points, and keeping only those objects that receive non-negligible scores. The intuition is that a subgraph that contains all objects and links relevant to a set of related terms should have all the information needed to rank objects with respect to one of these terms. We demonstrate that BinRank can achieve subsecond query execution time on the English Wikipedia data set, while producing high-quality search results that closely approximate the results of ObjectRank on the original graph. The Wikipedia link graph contains about 108 edges, which is at least two orders of magnitude larger than what prior state of the art dynamic authority-based search systems have been able to demonstrate. Our experimental evaluation investigates the trade-off between query execution time, quality of the results, and storage requirements of BinRank.</p>	J2EE
2.	<p><b>CLOSENESS: A NEW PRIVACY MEASURE FOR DATA PUBLISHING</b></p> <p>--- : KNOWLEDGE AND DATA ENGINEERING</p> <p>The k-anonymity privacy requirement for publishing microdata requires that each equivalence class (i.e., a set of records that are indistinguishable from each other with respect to certain “identifying” attributes) contains at least k records.</p>	J2EE

	<p>Recently, several authors have recognized that k-anonymity cannot prevent attribute disclosure. The notion of <math>\ell</math>-diversity has been proposed to address this; <math>\ell</math>-diversity requires that each equivalence class has at least <math>\ell</math> well-represented (in Section 2) values for each sensitive attribute. In this article, we show that <math>\ell</math>-diversity has a number of limitations. In particular, it is neither necessary nor sufficient to prevent attribute disclosure. Motivated by these limitations, we propose a new notion of privacy called “closeness”. We first present the base model t-closeness, which requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table (i.e., the distance between the two distributions should be no more than a threshold <math>t</math>). We then propose a more flexible privacy model called <math>(n, t)</math>-closeness that offers higher utility. We describe our desiderata for designing a distance measure between two probability distributions and present two distance measures. We discuss the rationale for using closeness as a privacy measure and illustrate its advantages through examples and experiments.</p>	
3.	<p><b>DATA LEAKAGE DETECTION</b>  --- : KNOWLEDGE AND DATA ENGINEERING</p> <p>We study the following problem: A data distributor has given sensitive data to a set of supposedly trusted agents (third parties). Some of the data is leaked and found in an unauthorized place (e.g., on the web or somebody’s laptop). The distributor must assess the likelihood that the leaked data came from one or more agents, as opposed to having been independently gathered by other means. We propose data allocation strategies (across the agents) that improve the probability of identifying leakages. These methods do not rely on alterations of the released data (e.g., watermarks). In some cases we can also inject “realistic but fake” data records to further improve our chances of detecting leakage and identifying the guilty party.</p>	DOT NET
4.	<p><b>ON WIRELESS SCHEDULING ALGORITHMS FOR MINIMIZING THE QUEUE-OVERFLOW PROBABILITY</b>  ---: NETWORKING</p> <p>In this paper, we are interested in wireless scheduling algorithms for the downlink of a single cell that can minimize the queue-overflow probability. Specifically, in a large-deviation setting, we are interested in algorithms that maximize the asymptotic decay-rate of the queue-overflow probability, as the queue-overflow threshold approaches infinity. We first derive an upper bound on the decay-rate of the queue-overflow probability over all scheduling policies. We then focus on a class of scheduling algorithms collectively referred to as the <math>\alpha</math>-algorithms. For a given <math>\alpha \geq 1</math>, the <math>\alpha</math>-algorithm picks the user for service at each time that has the largest product of the transmission rate multiplied by the backlog raised to the power. We show that when the overflow metric is appropriately modified, the minimum-cost-to-overflow under the <math>\alpha</math>-algorithm can be achieved by a simple linear path, and it can be written as the solution of a vector-optimization problem. Using this structural property, we then show that when <math>\alpha</math> approaches infinity, the <math>\alpha</math>-algorithms asymptotically achieve the largest decay-rate of the queueoverflow probability. Finally, this result enables us to design scheduling algorithms that are both close-to-optimal in terms of the asymptotic decay-rate of the overflow</p>	JAVA

	probability, and empirically shown to maintain small queue-overflow probabilities over queue-length ranges of practical interest.	
5.	<p><b>SECURE DATA COLLECTION IN WIRELESS SENSOR NETWORKS USING RANDOMIZED DISPERSIVE ROUTES</b></p> <p>---: MOBILE COMPUTING</p> <p>Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, we study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, we develop mechanisms that generate randomized multipath routes. Under our design, the routes taken by the “shares” of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity of our mechanisms.</p>	JAVA
6.	<p><b>PAM: AN EFFICIENT AND PRIVACY-AWARE MONITORING FRAMEWORK FOR CONTINUOUSLY MOVING OBJECTS</b></p> <p>---: KNOWLEDGE AND DATA ENGINEERING</p> <p>Efficiency and privacy are two fundamental issues in moving object monitoring. This paper proposes a privacy-aware monitoring (PAM) framework that addresses both issues. The framework distinguishes itself from the existing work by being the first to holistically address the issues of location updating in terms of monitoring accuracy, efficiency, and privacy, particularly, when and how mobile clients should send location updates to the server. Based on the notions of safe region and most probable result, PAM performs location updates only when they would likely alter the query results. Furthermore, by designing various client update strategies, the framework is flexible and able to optimize accuracy, privacy, or efficiency. We develop efficient query evaluation/reevaluation and safe region computation algorithms in the framework. The experimental results show that PAM substantially outperforms traditional schemes in terms of monitoring accuracy, CPU cost, and scalability while achieving close-to-optimal communication cost.</p>	DOT NET
7.	<p><b>P2P REPUTATION MANAGEMENT USING DISTRIBUTED IDENTITIES AND DECENTRALIZED RECOMMENDATION CHAINS</b></p> <p>---: KNOWLEDGE AND DATA ENGINEERING</p> <p>Peer-to-peer (P2P) networks are vulnerable to peers who cheat, propagate malicious code, leech on the network, or simply do not cooperate. The traditional security techniques developed for the centralized distributed systems like client-server networks are insufficient for P2P networks by the virtue of their centralized nature. The absence of a central authority in a P2P network poses unique</p>	JAVA

	<p>challenges for reputation management in the network. These challenges include identity management of the peers, secure reputation data management, Sybil attacks, and above all, availability of reputation data. In this paper, we present a cryptographic protocol for ensuring secure and timely availability of the reputation data of a peer to other peers at extremely low costs. The past behavior of the peer is encapsulated in its digital reputation, and is subsequently used to predict its future actions. As a result, a peer's reputation motivates it to cooperate and desist from malicious activities. The cryptographic protocol is coupled with self-certification and cryptographic mechanisms for identity management and countering Sybil attack. We illustrate the security and the efficiency of the system analytically and by means of simulations in a completely decentralized Gnutella-like P2P network.</p>	
8.	<p><b>A DISTRIBUTED CSMA ALGORITHM FOR THROUGHPUT AND UTILITY MAXIMIZATION IN WIRELESS NETWORKS</b>  ---: NETWORKING</p> <p>In multihop wireless networks, designing distributed scheduling algorithms to achieve the maximal throughput is a challenging problem because of the complex interference constraints among different links. Traditional maximal-weight scheduling (MWS), although throughput-optimal, is difficult to implement in distributed networks. On the other hand, a distributed greedy protocol similar to IEEE 802.11 does not guarantee the maximal throughput. In this paper, we introduce an adaptive carrier sense multiple access (CSMA) scheduling algorithm that can achieve the maximal throughput distributively. Some of the major advantages of the algorithm are that it applies to a very general interference model and that it is simple, distributed, and asynchronous. Furthermore, the algorithm is combined with congestion control to achieve the optimal utility and fairness of competing flows. Simulations verify the effectiveness of the algorithm. Also, the adaptive CSMA scheduling is a modular MAC-layer algorithm that can be combined with various protocols in the transport layer and network layer. Finally, the paper explores some implementation issues in the setting of 802.11 networks.</p>	DOT NET
9.	<p><b>EFFICIENT AND DYNAMIC ROUTING TOPOLOGY INFERENCE FROM END-TO-END MEASUREMENTS</b>  ---: NETWORKING</p> <p>Inferring the routing topology and link performance from a node to a set of other nodes is an important component in network monitoring and application design. In this paper we propose a general framework for designing topology inference algorithms based on additive metrics. The framework can flexibly fuse information from multiple measurements to achieve better estimation accuracy. We develop computationally efficient (polynomial-time) topology inference algorithms based on the framework. We prove that the probability of correct topology inference of our algorithms converges to one exponentially fast in the number of probing packets. In particular, for applications where nodes may join or leave frequently such as overlay network construction, application-layer multicast, peer-to-peer file sharing/streaming, we propose a novel sequential topology inference algorithm which significantly reduces the probing overhead and can efficiently handle node</p>	JAVA

	dynamics. We demonstrate the effectiveness of the proposed inference algorithms via Internet experiments.	
10.	<p><b>A DYNAMIC EN-ROUTE FILTERING SCHEME FOR DATA REPORTING IN WIRELESS SENSOR NETWORKS</b></p> <p>---: NETWORKING</p> <p>In wireless sensor networks, adversaries can inject false data reports via compromised nodes and launch DoS attacks against legitimate reports. Recently, a number of filtering schemes against false reports have been proposed. However, they either lack strong filtering capacity or cannot support highly dynamic sensor networks very well. Moreover, few of them can deal with DoS attacks simultaneously. In this paper, we propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our scheme, each node has a hash chain of authentication keys used to endorse reports; meanwhile, a legitimate report should be authenticated by a certain number of nodes. First, each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports. We design the hill climbing key dissemination approach that ensures the nodes closer to data sources have stronger filtering capacity. Moreover, we exploit the broadcast property of wireless communication to defeat DoS attacks and adopt multipath routing to deal with the topology changes of sensor networks. Simulation results show that compared to existing solutions, our scheme can drop false reports earlier with a lower memory requirement, especially in highly dynamic sensor networks.</p>	JAVA
11.	<p><b>PRIVACY-CONSCIOUS LOCATION-BASED QUERIES IN MOBILE ENVIRONMENTS</b></p> <p>---: PARALLEL AND DISTRIBUTED SYSTEMS</p> <p>In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it also raises concerns over potential intrusion into user location privacy. To protect location privacy, one typical approach is to cloak user locations into spatial regions based on user-specified privacy requirements, and to transform location-based queries into region-based queries. In this paper, we identify and address three new issues concerning this location cloaking approach. First, we study the representation of cloaking regions and show that a circular region generally leads to a small result size for region-based queries. Second, we develop a mobility-aware location cloaking technique to resist trace analysis attacks. Two cloaking algorithms, namely MaxAccu_Cloak and MinComm_Cloak, are designed based on different performance objectives. Finally, we develop an efficient polynomial algorithm for evaluating circular-region-based kNN queries. Two query processing modes, namely bulk and progressive, are presented to return query results either all at once or in an incremental manner. Experimental results show that our proposed mobility-aware cloaking algorithms significantly improve the quality of</p>	JAVA

	location cloaking in terms of an entropy measure without compromising much on query latency or communication cost. Moreover, the progressive query processing mode achieves a shorter response time than the bulk mode by parallelizing the query evaluation and result transmission.	
12.	<p>MANAGING MULTIDIMENSIONAL HISTORICAL AGGREGATE DATA IN UNSTRUCTURED P2P NETWORKS</p> <p>---: KNOWLEDGE AND DATA ENGINEERING</p> <p>A P2P-based framework supporting the extraction of aggregates from historical multidimensional data is proposed, which provides efficient and robust query evaluation. When a data population is published, data are summarized in a synopsis, consisting of an index built on top of a set of subsynopses (storing compressed representations of distinct data portions). The index and the subsynopses are distributed across the network, and suitable replication mechanisms taking into account the query workload and network conditions are employed that provide the appropriate coverage for both the index and the subsynopses.</p>	JAVA
13.	<p>ON EVENT-BASED MIDDLEWARE FOR LOCATION-AWARE MOBILE APPLICATIONS</p> <p>---: SOFTWARE ENGINEERING</p> <p>As mobile applications become more widespread, programming paradigms and middleware architectures designed to support their development are becoming increasingly important. The event-based programming paradigm is a strong candidate for the development of mobile applications due to its inherent support for the loose coupling between components required by mobile applications. However, existing middleware that supports the event-based programming paradigm is not well suited to supporting location-aware mobile applications in which highly mobile components come together dynamically to collaborate at some location. This paper presents a number of techniques including location-independent announcement and subscription coupled with location-dependent filtering and event delivery that can be used by event-based middleware to support such collaboration. We describe how these techniques have been implemented in STEAM, an event-based middleware with a fully decentralized architecture, which is particularly well suited to deployment in ad hoc network environments. The cost of such location-based event dissemination and the benefits of distributed event filtering are evaluated.</p>	JAVA