International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.10, pp : 1013-1016 1 Oct. 2013

Confidentiality and Honesty-Conserving Range Requests in Instrumental Networks

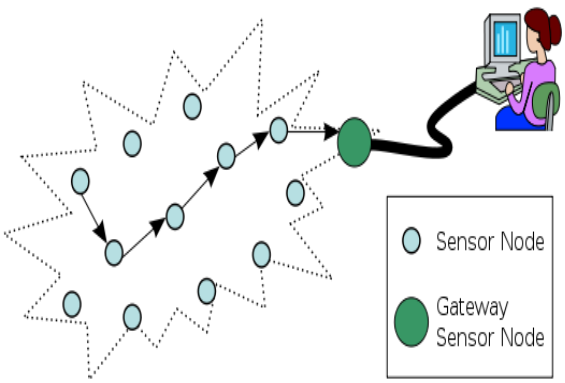
V. Munemma[1], P. Srilatha[2]

Global College of Engineering & Technology, Kadapa

Abstract-We consider a sensor network that is not fullytrusted and ask the question how we preserve privacy for the collected data and how we verify the data reply from the network.Master nodes collect datafrom sensor nodes and answer the queries from the network owner.It offers data confidentiality by preventing master nodes from reading hosted data and also enables efficient range-query processing.Previous work on data-centricrouting has shown it to be energy-efficient data disseminationmethod for sensor nets. Toimprove performance, we propose an optimization technique usingBloom filters to reduce the communication cost between sensorsand storage nodes.

INTRODUCTION:

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omnidirectional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound,pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.



The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

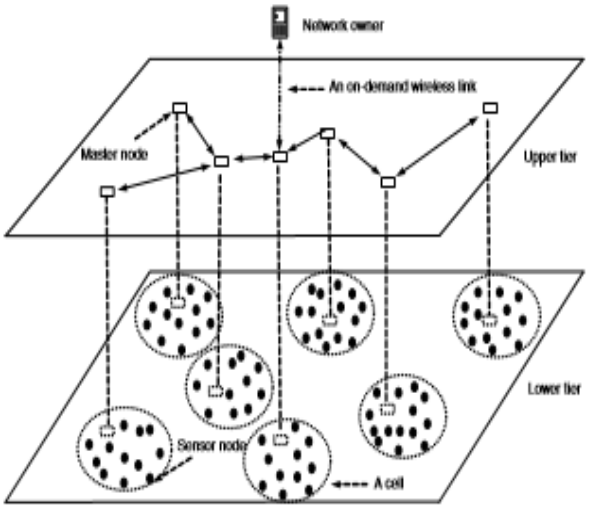
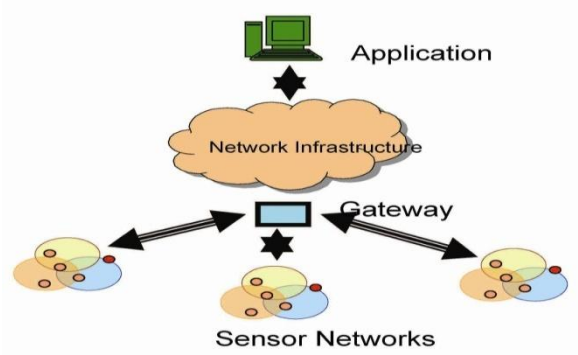


Fig. 1. An abstract two-tier sensor network architecture.

The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work.Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.10, pp : 1013-1016 1 Oct. 2013



A major challenge in developing sensor network systems and algorithms is that transmitting data from each sensor node to a central processing location may place a significant drain on communication and energy resources. Such concerns could place undesirable limits on the amount of data collected by sensor networks.Herein, we propose a useful companion method, datacentricstorage (DCS).In DCS, relevant data are stored by name at nodes within the sensor net all data with the same general name (e.g., elephant sightings) will be stored at the same sensor net node.In this paper, we propose SafeQ, a novel privacy- and integrity-preserving range query protocol for two-tiered sensor networks. The ideas of SafeQ are fundamentally different from the S&L scheme. SafeQ is a privacy preserving protocol that uses a novel technique to encode both data and queries.

RELATED WORK:

This paper considers the same system model, in which some storage nodes are deployed as the intermediate tier for data archival and query response.The basic idea is to divide the domain of datavaluesintomultiplebuckets,thesizeofwhichiscomputed based on the distribution of data values and the location of sensors.In sensor networks, secure aggregation is a similar topic to our work on reply verification. Their basic goal is to prevent malicious aggregators from forging the result.

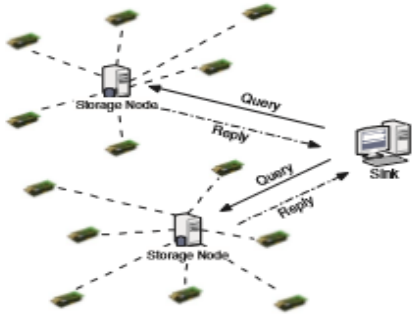


Fig. 1. Two-tiered System Model (with two storage nodes)

Privacy Preserving in Databases:

Database privacy has been studied in prior work. Hacigumus et al. first proposed the bucket partitioning idea for querying encrypted data in the database-as-service model (DAS), where sensitive data are outsourced to an un- trusted server. verifying the completeness of the result of relational database queries.Database integrity has also been explored in prior work independentoftheprivacy issues. It focuses on verifying the completeness of the result of relational database queries. This paper, for the first time in literature, investigates techniques to secure range queries in event-driven two-tier WSNs. We also use the bucketing technique [8], [9] to strike a balance between data confidentiality and query efficiency.

NETWORK MODELS AND PROBLEM STATEMENT:

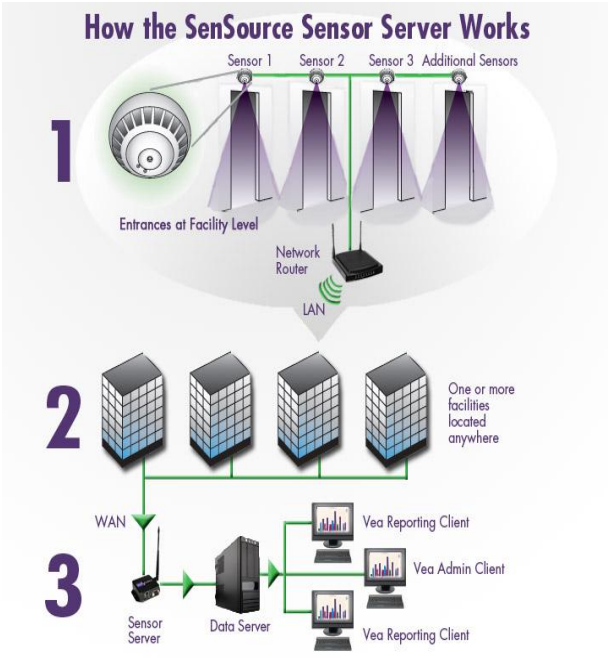
SYSTEM MODEL:

In this section we present our modeling approach to analyze the behavior of the sensor network.Our model consists of three building blocks that will be described and validated separately:

(i) The sensor model.
(ii) The network model and.
(iii) The interference model.

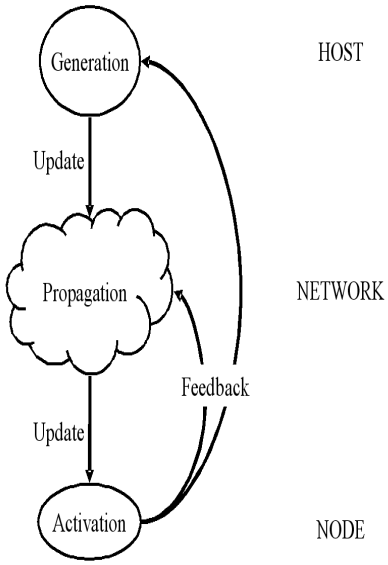
Sensor model:

In this model, it will specifies about the individual behavior of the sensor network. Also specifies about how to develop and how to transmit the data from one sensor to another. For that it divides time into individual time slots. i.e., the time interval necessary to transmit a data unit including the overhead required by the MAC layer.The below diagram shows how the data will be transferred from one sensor to another with the help of network router and data server.



Network model:

We now introduce our approach to modeling the sensor network. The sensor network can be regarded as an open queuing network in which each queue corresponds to the buffer of a sensor, and the external arrival rate to each queue corresponds to the data unit generation rate at the sensor.

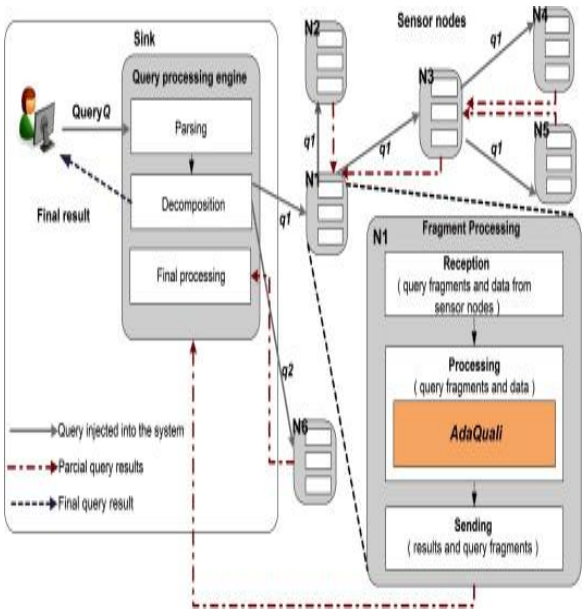


Interface model:

This model provides an interface between the sensors. The preserving range queries are use full for establishing interface between the sensors in sensor networks.

Data Storage and Query Processing

Different from existing query optimization techniques that consider only query plans for extracting data from sensors at individual nodes, our approach takes into account both of the sensing and communication cost in query plans.Smart sensors are small wireless computing devices that sense information such as light and humidity at extremely high resolutions. A smart sensor query-processing architecture using database technology can facilitate deployment of sensor networks. Smart-sensor technology enables a broad range of ubiquitous computing applications. Their low cost, small size, and untethered nature lets them sense information at previously unobtainable resolutions. We discuss about query processing in sensor networks.Queries in TinyDB, as in SQL, consist of a SELECT-FROM-WHEREclause supporting selection, join, projection, and aggregation. We alsoinclude explicit support for sampling, windowing, and sub-queries viamaterialization points.

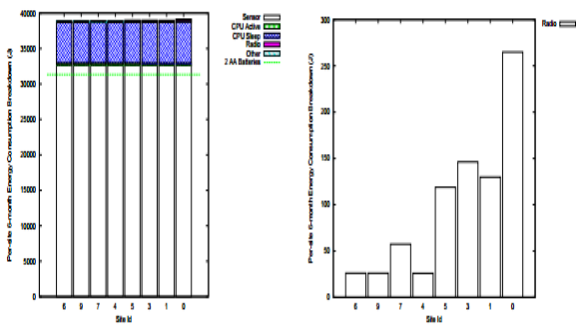


PERFORMANCE EVALUATION IN SENSOR NETWORKS:

The goal of this section is to present experimental evidence we have collected in support of our overall research hypothesis, viz. that the extensions to DQP techniques that are proven in the case of robust networks lead to effective and efficient DQP over WSNs.

The following can be observed:

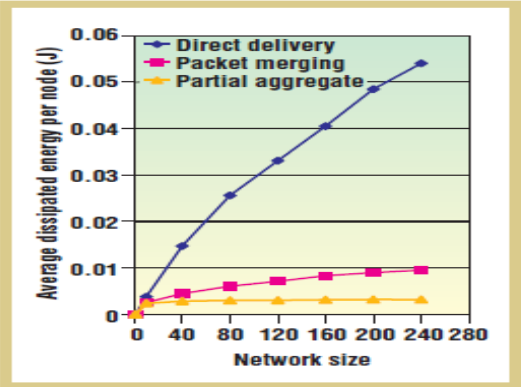
1. Fig. (a) shows that the sensor component is the dominant energy consumer (84%), but this is a consequence of our experimental set-up, insofar as the emulator we have used does not allow the sensor component to be sent to sleep mode.
2. Per-site energy consumption, as shown in Fig. 26(a), is roughly the same for all nodes in the network.
3. The detailed analysis of energy expenditure by the radio component (in Fig. (b)) shows that theper-site expenditure reflects the routing tree structure and the generated agenda.



(a) Per-component breakdown of energy consumption. (b) Energy consumption of the radio component.

Several simulations of our approachshowed that it works well in a controlled environment (often, simulation is the only way to get repeatable results out of noisy, lossy sensor

networks). We have a prototype of Cougar's query-processing layer runningin the ns-2 network simulator. Ns-2 is a discrete-event simulator aiming to simulate network protocols to highest fidelity.



CONCLUSION:

Sensor networks will become ubiquitous, and thedatabase community has the right expertise to address the challenging problems of tasking the network and managing the data in the network. In this paper, we consider an important problem in real sensor network deployment: how do we preserve the privacy and verify the query reply for a range query? We build our scheme in a network augmented with storage nodes that are equipped with more storage space. The efficacy and efficiency of our technique are confirmed by detailed evaluations. First, we propose SafeQ, a novel and efficient protocol for handling range queries in two-tiered sensor networks in a privacy- and integrity-preserving fashion.We propose an optimization technique using Bloom filters to significantly reduce the communication cost between sensors and storage nodes. To prevent the storage node from dropping data, an encoding number is generated on each sensor if no data in a range is collected on that sensor.

REFERENCES:

i. *F. Chen and A. X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.*

ii. *S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-centric storage in sensornets with GHT, a geographic hash table," Mobile Netw. Appl., vol. 8, no. 4, pp. 427–442, 2003.*

iii. *P. Desnoyers, D. Ganesan, H. Li, and P. Shenoy, "Presto: A predictive storage architecture for sensor networks," in Proc. HotOS, 2005, p. 23.*

iv. *D. Zeinalipour-Yazti, S. Lin, V. Kalogeraki, D. Gunopulos, and W. A. Najjar, "Microhash: An efficient index structure for flash-based sensor devices," in Proc. FAST, 2005, pp.*

v. *B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensor networks," in Proc. ACM MobiHoc, 2006, pp.*

vi. *B. Sheng, C. C. Tan, Q. Li, and W. Mao, "An approximation algorithm for data storage placement in sensor networks," in Proc. WASA, 2007, pp. 71–78.*

vii. *B. Sheng and Q. Li, "Verifiable privacy- preserving range query in two tiered sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 46–50.*

viii. *Xbow, "Stargate gateway (spb400)," 2011 [Online]. Available: http://www.xbow.com*