Performance Evaluation and Optimization of Wireless Sensor Networks

Prashant Sen[1], Anil Rao Pimplapure[2], Dr Jayant Dubey[3]
Assistant Professor, Department of Computer Science and Engineering of
BTIRT Sagar M.P., India[1 & 2]
Professor and Head, Department of Computer Science and Applications,
BTIRT, Sironja, Sagar[3]
prashantsen@yahoo.com, pimpu123@rediffmail.com, drjayantdubey@gmail.com

Keywords: WSN-Wireless Sensor Networks,

Abstract

A wireless sensor network (WSN) is an ad-hoc network composed of small sensor nodes deployed in large numbers to sense the physical world. Wireless sensor networks have very broad application prospects including both military and civilian usage. They include surveillance, tracking at critical facilities, or monitoring animal habitats. Sensor networks have the potential to radically change the way people observe and interact with their environment. With current wireless sensor network technology, people will gain advanced knowledge of physical and social systems, and the advent of a ubiquitous sensing era is coming. In-network processing or data aggregation is an essential function of WSNs to collect raw sensory data and get aggregated statistics about the measured environment, and help queries capture the major feature or changes of the measured systems. As more and more applications of WSNs collect sensitive measurements of people's everyday life, privacy and security concerns draw more and more attention. If privacy of sensory content is not preserved, it is not feasible to deploy the WSNs for information collection. On the other hand, if integrity of the collected sensory information is not protected, no queries or users can trust and/or use the collected information. Hence, two important issues should be addressed before wireless sensor network systems can realize their promise in civilian applications: (1) protect data privacy, so the deployment of the wireless sensor network systems is feasible; (2) enforce integrity, so users can trust the collected or aggregated information.

1. Introduction

Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN.

Information based on sensed data can be used in agriculture and livestock, assisted driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance. Five key features need to be considered when developing WSN solutions: scalability, security, reliability, self-healing and robustness. The required strength of each of these features depends on the application in question. Current trend of networked embedded computing technology is to involve humans as part of the sensing, data collecting and computing. In this way, public and professional users are able to gather, analyze and share local information to form advanced knowledge about the surrounding physical or social world. Instead of dedicated infrastructure or special designed networks, it is more convenient and efficient to collect commonly interested information and knowledge through wireless sensor networks. The emerging applications with wireless sensor networks involve human as a part of sensing, data collecting, and computing. These applications announce the advent of a new era of ubiquitous computing and communication.

2. Motivation

In publicly accessible wireless sensor networks (e.g. the above mentioned advanced metering systems), to encourage information sharing between users who may not trust each other, privacy and integrity are two important properties in information collection. Because in the civilian applications of wireless sensor networks, the data we deal with and the environments we interact with are not only about trees in the forest and animals in habitat, rather they may be critical to our properties, health and even lives, such systems will never succeed without adequate provision for data privacy and integrity.

3. Technology

WSNs form a particular class of ad hoc networks that operate with little or no infrastructure. WSNs are gaining momentum as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally low-priced, very small devices. They typically consist of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment. We cannot assume that sensor nodes will be tamper-resistant, although we will consider the availability of such tamper-resistant nodes for future applications. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable.

4. Threat Models and Their Relevance in WSNs

Typical functions in a WSN include sensing and collecting data, processing and transmitting sensed data, possibly storing data for some time, and providing processed data as information e.g. to a so called sink node. A particular kind of processing that is essential, as will be explained later, is aggregation of data in the sensor nodes. Securing such functions turns out to be very challenging. The Dolev-Yao threat model assumes that the two communicating parties, say A(lice) and B(ob), communicate over an insecure channel. If an intruder gains control over the communication network, she/he can overhear messages between the partners, intercept them and prevent their delivery to the intended recipient. But this threat model also assumes that the end-points, Alice and Bob, are not themselves subject to attack. A WSN adapted threat model should reflect that the channel is assumed to be insecure and the end-points cannot in general be trusted. An attacker may physically pick up sensor nodes and extract sensitive information.

5. Applications

A wide range of applications of wireless sensor networks is anticipated in the following areas: public/community health monitoring, vehicular and transportation control, urban infrastructure management/planning, etc. Let's consider an advanced metering system as an example to explain our proposed protocols, and design simulation scenarios. Utility companies are expecting millions of the wireless meters in the coming years. Besides automatic reading, the great potential of advanced metering systems is the ability to implement innovative rate policies. The wireless metering systems can provide real-time utility consumption that will help customers decide when they should increase their electricity usage to take advantage of cheaper power prices during low-demand periods or reduce usage when demand rises. Advanced metering accommodates this by collecting power consumption information hourly or even in smaller intervals.

The major characteristics of civilian wireless sensor networks are summarized as follows.-

5.1 Data Aggregation: The dominant traffic is data traffic. Usually people desire to get high level statistics rather than to learn individual behavior to capture the major feature of the surrounding systems. For example, in advanced metering systems, in order to determine pricing policies, real-time aggregated utility consumption information indicates whether or not it is the peak time of utility usage. For this purpose, utility consumption of individual households is not important. This means data aggregation is an important function in wireless sensor networks. On the other hand, information collection in such a system with fine granularity and over a large population will introduce a huge bandwidth demand, so it requires efficient means to get the aggregated statistics of utility consumptions. Hence, in network aggregation is needed.

5.2 Resource Constraints: Advances in miniaturization and nanotechnology enable us to reduce the size and cost of embedded devices for sensing, computation and wireless communication in physical world. However, small-size and low-cost devices usually have limited power, computation and storage. Also, the shared medium nature and interferences of multi-hop wireless communications imply limited bandwidth among low-power embedded devices.

5.3 Privacy & Integrity Concerns: Privacy and integrity are major concerns in collection of utility consumption information. If your neighbors or people around your house know the utility consumption information of your household, they can easily infer when you are on vacation, when you go to work, when you are taking shower, etc. On the other hand, integrity of the aggregated statistics about the utility consumption is a prerequisite to ensure correct pricing, appropriate load balancing, and in general avoid chaos in advanced metering systems.

5.4 Large Scale: The proliferation of embedded devices and the advances of the networked embedded systems provide means to gather data on large scales. In the advanced metering example, millions of advance meters are involved in a certain area. We anticipate that large-scale, on-line data collection and processing paradigms will make great impact on both physical systems and social behaviors. Hence, scalability is one of the major design concerns.

6. Challenges

Providing efficient data aggregation while preserving data privacy and integrity is a challenging problem in wireless sensor networks due to the following factors:

- Trust management in WSN is very challenging. Users in the wireless sensor networks can be very curious to learn others' private information, and the communication is over public accessible wireless links, hence the data collection is vulnerable to attacks which threaten the privacy. Without proper protection of privacy, the communication of privacy-sensitive data over civilian wireless sensor networks is considered impractical.

- During in-network aggregation, adversaries can easily alter the intermediate aggregation result and make the final aggregation result deviate from the true value greatly. Without protection of data integrity, the data aggregation result is not trustworthy.

- Data collection over wireless sensor networks does not rely on dedicated infrastructure. In many cases, the number of nodes answering a query is unknown before the data aggregation is conducted.

- Resource limited portable devices cannot afford heavy computation and communication load.

- The requirement on accuracy of information collection (i.e., aggregated result) makes the existing randomized privacy-preserving algorithms not suitable. Besides the above mentioned factors, it is very challenging to protect privacy and integrity of data aggregation simultaneously, because usually privacy-preserving schemes disable traffic peer monitoring mechanisms, which reduces the availability of information in a neighborhood to verify data integrity.

7. Design Objective

The overarching goal of this dissertation is to design novel network protocols for privacy-preserving and integrity-protecting data aggregation, make the proposed protocols robust against *eavesdropping*, and capable of detecting *data pollution*. Our desired data aggregation schemes will satisfy the following criteria:

Privacy-preservation: Privacy concern is one of the major obstacles to apply the wireless sensor networks to civilian applications, where curious individuals may attempt to determine more detailed information by eavesdropping on the communications of their neighbors. It is increasingly important to develop privacy-preserving data aggregation schemes to ensure data privacy against eavesdropping.

Data Integrity: Since data aggregation results may be used to make critical decisions, a base station needs to attest the integrity of the aggregated result before accepting it. Therefore, it is important that data aggregation schemes can protect the aggregation results from being polluted by attackers.

Efficiency: Data aggregation achieves bandwidth efficiency through in-network processing. In integrity-protecting private data aggregation schemes, additional communication overhead is unavoidable to achieve the additional features. However, we must keep the additional overhead as small as possible.

Accuracy: An accurate aggregation result of sensor data is usually desired. Therefore, we take accuracy as a criterion to evaluate the performance of integrity protecting private data aggregation schemes. When accurate aggregation results are needed, schemes based on randomization techniques are not applicable.

In the dissertation, we adopt the above discussed metrics to explore the space and tradeoff among the performance of the proposed algorithms. These metrics include communication and computation overhead, efficacy of privacy and integrity protection, and accuracy of aggregated result.

8. Related Work

Data aggregation has the benefit to achieve bandwidth and energy efficiency in resource-limited wireless sensor networks. Previous work addresses data aggregation in various application scenarios with the assumption that all sensors are working in trusted and friendly environments. However, in reality, sensor networks are likely to be deployed in a entrusted environment, where links can be eavesdropped and messages can be altered. An adversary may manipulate the sensory data in wireless sensor networks. Le May et al. summarize the functional characteristic of wireless metering sensors and categorizes attackers in, where both privacy and security are concerns in the given scenarios. Wireless sensor networks are operated in an open, publicly accessible, and entrusted environment Therefore, integrity of data aggregation is a big concern. As a result, existing research addresses the integrity of data aggregation in wireless sensor networks. Previous work investigates secure data aggregation against adversaries who try to tamper the intermediate aggregation result. To reinforce security in sensor networks, communications are usually encrypted and authenticated. Przydatek, Song and Perrig proposed *SIA* protocol. *SIA* addresses data integrity by constructing efficient random sampling mechanisms and interactive proofs. There are three stages in the *SIA* protocol: computation of the result, committing to the collected data and reporting back the aggregation result, and proving the correctness of the result. *SIA* is the first work on secure information aggregation in sensor networks that can handle malicious aggregators and sensor nodes. The drawback of this protocol is that the statistical security property is achieved under the assumption of a single-aggregator model, where sensor nodes send their data to a single-aggregate node. In this way, the interactive verification procedure results in additional bandwidth consumption. When the sample size is large, the additional communication overhead can be large.

9. Contributions and Dissertation Outline

In the dissertation, we focus on network protocol design for privacy-preserving and integrity protecting data aggregation. We extensively study the trade-offs between efficiency and functionality of protocols. We also investigate factors which affect the performance of the protocols, and discuss the trade-offs between privacy preservation and integrity protection. Achieving both data privacy and integrity simultaneously in data aggregation was considered very challenging in the past. This dissertation explores privacy and integrity of data aggregation in wireless sensor networks. First, I present privacy-preserving data aggregation schemes for additive aggregation functions, and show that the additive aggregation functions can serve to estimate the aggregation results for more general aggregation functions. The first scheme, Private Data Aggregation Using Cluster, leverages clustering protocol and algebraic properties of polynomials. It has the advantage to enable peer monitoring within a cluster. The second scheme, Slicing Data Aggregation, builds on slicing techniques and the associative property of addition. It has the advantage of incurring less computation overhead for privacy-preserving data aggregation. Then, I address both privacy of individual sensory data and integrity of aggregation result simultaneously. It is very challenging to achieve the synergy of privacy and integrity, because privacy-preserving schemes try to hide or interfere with data, while integrity protection usually needs to enable peer monitoring or public access of the data. To show the efficiency and efficacy of the proposed schemes, I present simulation results of our schemes and compare their performance to a typical data aggregation scheme, Tiny Aggregation Protocol, where no privacy preservation and integrity protection is provided. We explore multiple dimensions in design space, and investigate the trade-offs in protocol design.

10. Conclusion:

Accordingly, I will focus on two aspects of such systems, privacy preservation and integrity protection. My objective is to design protocols for (1) protecting sensory content privacy to make the deployment of WSNs more applicable to people; (2) enforcing integrity of collected sensory information, so users can trust it. Therefore, we focus on privacy-preserving and integrity-protecting data aggregation protocol design. We can anticipate trustworthy wireless sensor networks in the future.

11. References:

- B. Lai, S. Kim, and I. Verbauwhede, “Scalable session key construction protocol for wireless sensor networks.” *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*, December 2002.
- B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” *In Proc. of ACM SenSys*, 2003.
- C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient Aggregation of Encrypted Data in Wireless Sensor Networks,” *Mobiquitous*, 2005.
- D. Liu and P. Ning, “Establishing pair-wise keys in distributed sensor networks,” in *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS03)*, October 2003, pp. 52–61.

- F. Delgosha and F. Fekri, “Threshold key-establishment in distributed sensor networks using a multivariate scheme.” *Proceedings of 25th IEEE INFOCOM*, April 2006.
- H. Chan, A. Perrig, and D. Song, “Random key pre-distribution schemes for sensor networks,” in *IEEE Symposium on Research in Security and Privacy*, 2003, pp. 197–213.
- H. Chan, A. Perrig, and D. Song, “Secure Hierarchical In-Network Aggregation in Sensor Networks,” in *Proceedings of 13rd ACM Conference on Computer and Communications Security (CCS06)*, October 2006.
- J. Girao, D. Westhoff, and M. Schneider, “CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks,” in *40th International Conference on Communications, IEEE ICC*, May 2005.
- J.Y. Chen, G. Pandurangan, and D. Xu, “Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis,” *IPSN*, 2005.
- K. Krizman, T. E. Biedka, and T. Rappaport, “Wireless position location: fundamentals, implementation strategies, and source of error,” in *Proceedings of IEEE 47th Vehicular Technology Conference*, 1997.
- M. LeMay, G. Gross, C. A. Gunter, and S. Garg, “Unified architecture for large-scale attested metering,” in *proceedings of HICSS-40*, January 2007.
- M. Li and Y. Liu, “Underground structure monitoring with wireless sensor networks,” in *6th International Symposium on Information Processing in Sensor Networks (IPSN)*, Cambridge, Massachusetts, USA, April 2007.
- Q. Huang, H. J.Wang, and N. Borisov, “Privacy-preserving friends troubleshooting network,” in *Symposium on Network and Distributed Systems Security (NDSS)*, San Diego, CA, February 2005.
- S. Camtepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks,” in *Proceedings of 9th European Symposium On Research in Computer Security (ESORICS 04)*, 2004.
- T. Abdelzaher, T. He, and J. Stankovic, “Feedback Control of Data Aggregation in Sensor Networks,” *43rd IEEE Conference on Decision and Control*, December 2004.
- W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pair-wise key pre-distribution scheme for wireless sensor networks,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, October 2003, pp. 42–51.
- B. Karp and H. T. Kung, GPSR: Greedy Perimeter Stateless Routing for Wireless Sensor Networks,IEEE Mobicom, August 2000.
- P. Levis and D. Culler, Mate: A Tiny Virtual Machine for Sensor Networks, Int. Conf. on Architectural Support for Programming Languages and Operating Systems, October 2002.

- J. Liu, M. Chu, J.J. Liu, J. Reich and F. Zhao, State-centric Programming for Sensor and Actuator Network Systems, IEEE Pervasive Computing, October 2003.
- C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, RAP: A Real-Time Communication Ar-chitecture for Large-Scale Wireless Sensor Networks, IEEE Real-Time Applications Symposium, June 2002.
- L. Luo, T. Abdelzaher, T. He, and J. Stankovic, EnviroSuite: An Environmentally Immersive Pro-gramming Framework for Sensor Networks, ACM Transactions on Embedded Computing Systems, to appear.

* * * *