Security Challenges of Sensor Network Query Processor in Wireless Sensor Network

Muhamad Erza Aminanto* and Kwangjo Kim*

*School of Computing, KAIST.

Abstract

Recently, the use of the database paradigm has emerged as a feasible solution to manage data in Wireless Sensor Network (WSN) environments. Various Sensor Network Query Processors (SNQPs) implements in-network declarative query processing that provide data reduction, aggregation, logging, and auditing facilities. These SNQPs view the WSN as a distributed database over which declarative query processor can be used to program WSN applications with much less effort. This paper discusses novel approaches of SNQP in WSN from the point of security. We discuss security requirements, attack models and unique features of SNQP in WSN. Finally, we suggest security challenges of SNQP in WSN.

I. Introduction

A Wireless Sensor Network (WSN) is an *ad-hoc* network of a large number of sensor nodes interconnected wirelessly which collect environmental data, such as temperature, vibration, pressure, sound, *etc* [1]. WSN has broad implementations such as military, environmental, health, and home applications.

In WSN, a former approach was analyzed the data in the warehousing approach which the whole raw data is pushed out of network to Base Station. It leads to expensive load on network channel and sometimes impossible [2]. In contrast to warehousing approach, the in-network processing approach aims to reduce large amount of data transmission by injecting more complex processing into the node [2].

In in-network processing approach, WSN are constructed as distributed database system. This conception of sensor networks has led to the approach of retrieving data from a sensor network by declarative query. Declarative queries allow users to specify what data they want from a sensor network without the details how to retrieve the data [2], but, it is difficult to implement declarative query such as Structured Query Language (SQL) in WSN. Thus, Madden *et al.* [3] and Yao and Gehrke [4] proposed that WSNs can be programmed with Sensor Network Query Processors (SNQP) which implementing in-network declarative query processing over WSNs such as TinyDB [3] and Cougar [4]. This allows for low-cost programmability, since rather than reprogramming the network, users only need to pose a different query to the SNQP.

In WSN, sensors are operated in an open environment which make them vulnerable to different kinds of attacks. These sensors could be attacked physically and logically. Furthermore, the data managed by the sensors may be compromised. Thus we need security techniques to ensure that the sensor data is protected. We must also ensure that the data is not maliciously corrupted. However, there is virtually no research on security for SNQP. In this paper we examine security issues for SNQP in WSN in accordance to security challenge as Huang *et al.* [5] and Kumar *et al.* [6].

II. Threat Model

SNQP in WSN has unique features will be explained in Section 3 that make it difference with wide impact of attacks in conventional networks. Thus, we would describe the security requirements and attack models for SNQP in WSN only as follows.

2.1. Security Requirements

- *Confidentiality*. The confidentiality principle in case of WSN must be achieved when we can ensure to aggregate encrypted data securely [6].
- *Integrity*. We must be able to maintain the information has not been altered along query process. Especially, there should not be alterations in aggregated data [6].
- *Availability (Freshness)*. We must ensure that SNQP can accurately perform as its intended [6]. Freshness term means that sometime we need recent data from sensors. There are several challenges for maintain freshness such as hardware sensor errors, queuing in network, etc.
- *Authentication*. It means we should ensure the correctness of claimed entity [6].
- *Authorization*. After authentication completed, we need to ensure permission granted for actions performed by any entity. The SNQP need to manage granularity of data items.
- *Non-Repudiation*. Any entity in database should not deny of committing query or updating the attributes of any tuples [7].
- *Anonymity*. All private credentials should be keep securely. Anonymity in WSN can be assured by using authentication protocol which has temporary identity from Certificate Authority [7].

2.2. Attack Models

Several attack models can be considered in WSN systems. However, in this paper, we only interested in attack models to SNQP in WSN. Therefore, besides attack models listed below, there are several attack models in WSN such as eavesdropping, hijacking [8], packet or signal destruction, wormhole, and false routing [9].

- *Disruption*. The goal of this attack is to disrupt the sensor application, thus the sensor reading result would be disrupted. There are two types of disruption [8]. This attack also known as stealthy attack [10].
- *Sybil Attack*. The adversary node makes multiple entities. These entities could be fabricated or stolen entities [9].
- *Replay Attack*. The adversary committed previous query repeatedly which affects the freshness of sensor data. Furthermore, the Base Station can't get most recent data from each sensor node[10].
- *Denial of Service (DoS)*. Any action that prevents any part of a WSN functioning correctly or in a timely manner.

III. SNQP Unique Features

In this section, we briefly describe the main distinctions that lead to new challenges in security.

- **P1: Tree-Structured Topology**. Most recently WSN adopted tree-structured topology which locate the base station at the root [8]. Because of this topology, data aggregation is needed in WSN.
- **P2: Dynamic Network and Environments**. In WSN, we need to cope with network layer dynamics. Among the most important dynamic events are those that cause the network topology to change (such as nodes failure, packet collision, *etc*

[2]). Furthermore, the arrival rate of tuples is often prone to more severe fluctuation because of system conditions such as congestion, link quality, and node workload [2]. Also, the surrounding environments might be fluctuate such as extreme weather, intended harmed by adversaries, *etc*.

- **P3: Distributed Data.** WSN is distributed platforms, therefore, each node is only aware of that part of event region that is within its sensing range. Due to resource constraints, no node can assume to have complete information. Thus, complete information regarding event region is distributed throughout the WSN [2].
- **P4: Sensor Noise**. WSN has a significant proportion of noise and uncertainty. Noise is usually unwanted faulty measurements reported by sensor nodes due to several reasons such as hardware/software fault, extreme environment, *etc*. Thus, while considering all these challenges associated with WSN, it is required for SNQP to have separate data models, query languages, and query semantics, *etc* [2].

IV. SNQP Security Challenge

In order to protect SNQP in WSN against the attacks outlined in Section 3 and to fulfill the security requirements also outlined in Section 3, SNQP system designers must be aware of the security properties that belong to SNQP (explained in Section 4). Below, we take a first step towards establishing a comprehensive set of security challenges for SNQP in WSN.

C1: Secure Query

WSN has tree-structured topology (**P1**) which leads to adoption of two-tiered sensor networks are very common. The two-tiered sensor networks has a large number of resource constrained sensor nodes in the lower tier and fewer relatively resource-rich storage (or master) nodes in the upper tier. Also, the storage nodes collect data from the sensor nodes and answer the queries from the base station. Thus it leads security drawbacks where once storage nodes are compromised, it may disclose the stored sensor data to the adversary and send a wrong query result to base station. Then, Huang *et al.* [5] proposed secure multiparty query in WSN without two-tiered structure. The authors adopted homomorphic privacy and secure multi-party computation techniques. Unfortunately, this scheme still have several drawbacks such as once malicious party involved, it may be damage the network. Thus there is a need for re-verifying the identifications of underground parties during the top k-query [5]. Also, Jabeen *et al.* [2] claimed that existing WNS SNQP assume that all nodes are co-operative and trustworthy. Thus, authentication scheme is needed in query process. **C1** is to develop novel cryptographic approaches in query process.

C2: Secure Data Aggregation

We know from **P1** that WSN needed data aggregation at intermediary nodes. From the point of security, end-to-end secure transmission from sensors to base station is needed. Although several cryptosystem proposed, those still have performance drawbacks [8] since those scheme should be done in each node (because of **P3**, each node should be able to compute with the data). Also, Guo *et al.* [10] claimed that majority of secure data aggregation protocols use tree-based structures which are fixed structure instead of dynamic structure.

Meanwhile, the trend of WSN s going to dynamic topology [10] for preserving power consumption. Thus, C2 is to develop novel cryptographic approaches that allow secure data aggregation in recent state of WSN.

C3: Adaptability

Node and network failure may lead to network partitions, topology change, delay, packet corruption, *etc* [2]. These situation represent P2. Thus, SNQP must provide comprehensive support for adaptability (also known as availability). As an example, to find a new path because of packet loss and to reschedule the Query Execution Plan (QEP) fragment. C3 is to develop query scheme that ensure adaptability in WSN.

C4: Integrity

P4 may lead to integrity problem since data from sensors might be disrupted by noise. If several sensors can't maintain their integrity, it will give incorrect result after aggregation (P3). C4 is to develop query scheme that ensure integrity in WSN.

C5: Weak Audit Trail

WSN constitute a distributed environment (P3) and hence there is no central clock to regulate activities of the network. However, each clock of the sensor node may not be accurate and may drift over time [2]. It lead to unsynchronized timestamps. C5 is to develop time synchronization time that ensure strong audit trail in WSN.

V. Conclusion and Future Work

This paper highlighted some of the major security issues of SNQP in WSN. We describe security requirements and attack models of SNQP in WSN. Also, we discussed unique features of SNQP. Last, we listed 5 security challenges came from SNQP unique features to protect SNQP in WSN against the attacks and to fulfill the security requirements. Thus, the significant unexplored research must be discussed in this field.

References

[1] K. Sunitha and H. Chandrakanth, "A Survey on Security Attacks in Wireless Sensor Network," Int. J. Eng. …, vol. 2, no. August, pp. 1684 – 1691, 2012.

[2] F. Jabeen and S. Nawaz, "In-network wireless sensor network query processors : State of the art , challenges and future directions," Inf. Fusion, Elsevier, vol. 25, pp. 1 – 15, 2015.

[3] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TinyDB: an acquisitional query processing system for sensor networks," ACM Trans. Database Syst., vol. 30, pp. 122 – 173, 2005.

[4] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," ACM SIGMOD Rec., vol. 31, no. 3, p. 9, 2002.

[5] H. Huang, Y. Dou, J. Chen, J. Feng, and X. Qin, "Secure Query in Wireless Sensor Network Using Underground Parties," J. Networks, vol. 7, no. 12, pp. 2063 – 2069, 2012.

[6] K. Mukesh and K. Dutta, "A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks," Intell. Comput. Commun. Devices. Springer, pp. 1 – 15, 2015.

[7] B. Vidhya and Et.al., "Environment Based Secure Transfer of Data in Wireless Sensor Networks," arXiv Prepr. arXiv1503.03215, 2015.

[8] M. Anand, E. Cronin, M. Sherr, M. Blaze, and I. Lee, "Sensor network security: more interesting than you think," USENIX Work. Hot Top. Secur., 2006.

[9] A. Tayebi, S. M. Berber, and A. Swain, "Sensing Technology: Current Status and Future Trends III," Sens. Technol. Curr. Status Futur. Trends III. Springer Int. Publ., vol. 11, pp. 201 – 221, 2015.

[10] J. Guo, J. Fang, and X. Chen, "Survey on secure data aggregation for wireless sensor networks," Proc. 2011 IEEE Int. Conf. Serv. Oper. Logist. Informatics, pp. 138 – 143, 2011.