Dr. V. Palanisamy, D. Gandhimathi / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1108-1111

Preservation Of Privacy And Integrity In WSN With Safeg Protocol

Dr. V. Palanisamy, D. Gandhimathi
Professor and Head,, Dept. of CSE, Alagappa University, Karaikudi, Tamilnadu,India.

Abstract

In two-tiered wireless sensor networks, storage nodes play an intermediary role between the sensors and the sink node. These storage nodes store data and processes queries. This technique preserves power and the memory for sensor nodes, as everything is managed by storage nodes including query processing. This importance of storage nodes grabs attackers to intrude storage node in order to affect its integrity and privacy. Thus, there is a need to protect storage node and we propose a new protocol named 'SafeG'. If storage node is protected then, the attacker cannot infer about the data present and also the queries passed by sinks. SafeG provides both privacy and integrity. SafeG encodes both the data and query and so the encoded query acts upon encoded data. SafeG relies on authentication chain to provide integrity.

Index Terms- Integrity, Privacy, Authentication.

I. INTRODUCTION

A wireless sensor network consists of several resource restricted nodes to perform monitoring tasks. Usually, it focuses in tracking mobile objects traversing in different geographical locations. The information collected by 4each sensor is then clubbed together and gets place in storage node.

If the adversary gets access to this storage node, all the information that are needed to be kept secret will be revealed. Using this sensitive information, the adversary can involve in malpractice or in otherwise he can misuse this invaluable information. As WSN is employed to predict earthquake, environmental sensing, it is essential to provide enough security.

This paper concentrates in providing integrity and privacy by using the protocol named SafeG. We use storage nodes here, because of the below mentioned benefits.

Firstly, sensors save power by sending all collected data to their closest storage node instead of sending them to the sink through long routes. Secondly, sensors can be memory-limited because data are mainly stored on storage nodes. Finally, query processing becomes more efficient because the sink only communicates with storage nodes for queries.

The inclusion of storage nodes also brings significant security challenges. As storage nodes store data received from sensors and serve as an important role for answering queries, they are more vulnerable to be compromised, especially in a hostile environment.

A compromised storage node imposes significant threats to a sensor network. First, the attacker may obtain sensitive data that has been, or will be, stored in the storage node. Second, the compromised storage node may return forged data for a query.

Third, this storage node may not include all data items that satisfy the query. Therefore, to design a protocol that prevents attackers from gaining information from both sensor collected data and sink issued queries, which typically can be modeled as range queries, and allows the sink to detect compromised storage nodes when they misbehave. For privacy, compromising a storage node should not allow the attacker to obtain the sensitive information that has been, and will be, stored in the node, as well as the queries that the storage node has received, and will receive.

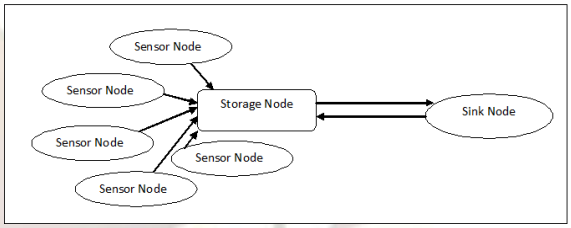

Fig 1: Architecture

Note the queries from the sink as confidential because such queries may leak critical information about query issuers' interests, which need to be protected especially in military applications. For integrity, the sink needs to detect whether a query result from a storage node includes forged data items or does not include all the data that satisfy the query.

There are two key challenges in solving the privacy and integrity- preserving range query problem. First, a storage node needs to correctly process encoded queries over encoded data without knowing their actual values. Second, a sink needs to verify that the result of a query contains all the data items that satisfy the query and does not contain any forged data.

In this work, SafeG, a novel privacy- and integrity-preserving range query Proto-filter for two-

tiered sensor networks. To preserve privacy, SafeG uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their actual values.

In order to provide integrity, we present a scheme that complements existing key distribution schemes for WSNs and protects the communication within a WSN against an attacker who tries to manipulate messages in the network.

This scheme relies on symmetric cryptography by taking the restrictions of sensor nodes into account. It abstains from using public key cryptography or a complete infrastructure of mutually shared symmetric keys and does not require a base station. Nevertheless it allows for reliable communication among any pair of nodes. This scheme is known as canwas. The main objective of this work is to develop a secure and efficient query processing and to achieve data, query privacy and integrity.

II. RELATED WORK

Privacy and integrity-preserving range queries in WSNs have drawn people's attention recently [1], [2], [3]. Sheng and Li proposed a scheme to preserve the privacy and integrity of range queries in sensor networks [1].

This scheme uses the bucket-partitioning idea proposed by Hacigumus et al. in [4] for database privacy. The basic idea is to divide the domain of data values into multiple buckets, the size of which is computed based on the distribution of data values and the location of sensors. In each time-slot, a sensor collects data items from the environment, places them into buckets, encrypts them together in each bucket, and then sends each encrypted bucket along with its bucket ID to a nearby storage node.

For each bucket that has no data items, the sensor sends an encoding number, which can be used by the sink to verify that the bucket is empty, to a nearby storage node. When the sink wants to perform a range query, it finds the smallest set of bucket IDs that contains the range in the query, then sends the set as the query to storage nodes. Upon receiving the bucket IDs, the storage node returns the corresponding encrypted data in all those buckets. The sink can then decrypt the encrypted buckets and verify the integrity using encoding numbers.

The S&L scheme only considered one-dimensional data in [1], and it can be extended to handle multidimensional data by dividing the domain of each dimension into multiple buckets. The S&L scheme has two main drawbacks inherited from the bucket-partitioning technique.

First, as pointed out in [5], the bucket-partitioning technique allows compromised storage nodes to obtain a reasonable estimation on the actual value of both data items and queries. In SafeQ, such estimations are very difficult.

Second, for multidimensional data, the power consumption of both sensors and storage nodes, as well as the space consumption of storage nodes, increases exponentially with the number of dimensions due to the exponential increase of the number of buckets.

In SafeG, power and space consumption increases linearly with the number of dimensions times the number of data items. Shi et al. proposed an optimized version of S&L's integrity preserving scheme aiming to reduce the communication cost between sensors and storage nodes [2], [3].

The basic idea of their optimization is that each sensor uses a bitmap to represent which buckets have data and broadcasts its bitmap to the nearby sensors. Each sensor attaches the bit maps received from others to its own data items and encrypts them together. The sink verifies query result integrity for a sensor by examining the bitmaps from its nearby sensors.

In our experiments, we did not choose the solutions in [2] and [3] for side-by-side comparison for two reasons. First, the techniques used in [2] and [3] are similar to the S&L scheme except the optimization for integrity verification.

The way they extend the S&L scheme to handle multi dimensional data is to divide the domain of each dimension into multiple buckets. They inherit the same weakness of allowing compromised storage nodes to estimate the values of data items and queries with the S&L scheme.

Second, their optimization technique allows a compromised sensor to easily compromise the integrity verification functionality of the network by sending falsified bit maps to sensors and storage nodes. In contrast, in S&Land our schemes a compromised sensor cannot jeopardize the querying and verification of data collected by other sensors.

III. PROPOSED WORK

In Sensor Module, Sensor nodes are responsible to collect the data from environment The collected data are stored into the storage node. Sensor node has limited storage capacity.

All the sensor nodes should have capability to collect and store the data at the same time.

In Storage Node Module, Storage nodes are powerful wireless devices that are equipped with much more storage capacity and computing power than sensors. The storage node collects all data from the sensor nodes.

The storage node allows only the Authorized user to view the actual value of sensor node data. If any unauthorized user trying to view the sensor node data, sink detect misbehave of storage node and the unauthorized user can able to view the encoded data only.

In SafeG Module, SafeG is a Proto-filter that prevents attackers from gaining information from both sensor collected data and sink issued queries. SafeG also allows a sink to detect compromised storage nodes when they misbehave. To preserve privacy, SafeG uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their values.

The Canwas Scheme is used to preserve integrity and it consists of three phases. The task of the first phase is key pre-distribution. It is carried out before the sensor network is deployed. At the end of this phase, an arbitrarily chosen pair of nodes is (with high probability) able to establish a secret shared key (a suitable approach is described in [11]).

The second phase follows immediately after deployment, when the distribu- tion of the sensor nodes has been fixed. (We do not consider mobile nodes in this paper.) Each node establishes a separate secret shared key with each of its immediate (1-hop) and indirect (2-hop) neighbours. We assume that only such nodes can participate in this process, which also participated in the first phase.

This prevents an attacker from joining the network with his own nodes.After the second phase, there exists at least one path between any two nodes in the network (if the network is connected) with the characteristics shown in Fig 1.

Apparently, an attacker can manipulate messages on such a path if he controls two adjacent nodes. Single nodes under the attacker's control are not capable of disrupting the communication path. The third and last phase is the operational phase of the sensor network.

Nodes exchange messages with remote peers by "authenticating" them with their neighbour keys along the transmission path. This will be explained in detail below. Note that we assume a suitable routing scheme.

IV. Conclusion

Thus, this work provides both privacy and integrity by using SafeG protocol. The Canvas scheme achieves data integrity at very low cost for sensor node communication. It relies on symmetric cryptographic operations and a low number of keys that have to be stored; it is therefore well-suited for resource- constrained sensor networks. We hope that it has become clear that in a large distributed system, such as a WSN, end-to-end security is not always necessary, and data integrity can be achieved with less effort. SafeG encodes both the data and query and so the encoded query acts upon encoded data. SafeG relies on authentication chain to provide integrity.

REFERENCES

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

[2] *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.*

[3] *P. Desnoyers, D. Ganesan, H. Li, and P. Shenoy, "Presto: A predictive storagearchitectureforsensornetworks,"inProc.HotOS,2005,p.23.*

[4] *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. 31–44.*

[5] *B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensor net- works," in Proc. ACM MobiHoc, 2006, pp. 344–355.*

[6] *B.Sheng,C.C.Tan,Q.Li,andW.Mao,"Anappr oximationalgorithm for data storage placement in sensor networks," in Proc. WASA, 2007, pp. 71–78.*

[7] *B.ShengandQ.Li,"Verifiableprivacy-preservingrangequeryintwo- tiered sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 46–50.*

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

[9] *W. A. Najjar, A. Banerjee, and A. Mitra, "RISE: More powerful, en- ergy efficient, gigabyte scale storage high performance sensors," 2005 [Online]. Available: http://www.cs.ucr.edu/~rise*

[10] *S. Madden, "Intel lab data," 2004 [Online]. Available: http://berkeley. intel-research.net/labdata*

[11] *J. Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor networks," in Proc. IEEE INFOCOM, 2009, pp. 945–953.*

[12] *R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional range queries in sensor networks," in Proc. ACM MobiHoc, 2009, pp. 197–206.*

[13] *H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proc. ACM SIGMOD, 2002, pp. 216–227.*

[14] *B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proc. VLDB, 2004, pp. 720–731.*

[15] *R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD, 2004, pp. 563–574.*

[16] *D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE S&P, 2000, pp. 44–55.*

[17] *P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. ACNS, 2004, pp. 31–45.*

[18] *D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. TCC, 2007, pp. 535–554.*