ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

Preserving Privacy and Integrity in Sensor Network with Proto-filter

A.S.Balaji[1] S.Roselin Mary[2] R.Femila Goldy[3]

[1]Lecturer, Dept. of CSE, Anand Institute of Higher Technology, Kazhipattur, Chennai, India
[2]Associate Professor, Dept. of CSE, Anand Institute of Higher Technology, Kazhipattur, Chennai, India
[3]Assistant Professor, Dept. of CSE, Anand Institute of Higher Technology, Kazhipattur, Chennai, India

ABSTRACT: **The architecture of two-tiered sensor networks, where storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries, has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. However, the importance of storage nodes also makes them attractive to attackers. SecureQ Proto-filter acts as protocol as well as filter. SecureQ prevents attackers from gaining information from both sensor collected data and sink issued queries. To improve performance, SecureQ will be used to reduce the communication cost between sensors and storage nodes. SecureQ also allows a sink to detect compromised storage nodes when they misbehave. To preserve privacy, SecureQ 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. To preserve integrity, Truth confirmation algorithm to generate integrity verification information so that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query.**

Keywords: Integrity, privacy, range queries, sensor networks

I. INTRODUCTION

Wireless sensor networks (WSNs) have been widely deployed for various applications, such as environment sensing, building safety monitoring, earthquake prediction, etc. Two-tiered sensor network architecture is that in which storage nodes gather data from nearby sensors and answer queries from the sink of the network. The storage nodes serve as an intermediate tier between the sensors and the sink for storing data and processing queries.

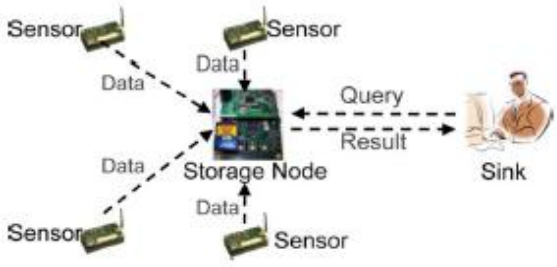

Fig 1.1 Architecture of two-tiered sensor networks

Storage nodes bring three main benefits to sensor networks. First, sensors save power by sending all collected data to their closest storage node instead of sending them to the sink through long routes. Second, sensors can be memory-limited because data are mainly stored on storage nodes. Third, 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. 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

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

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 project, SecureQ, a novel privacy- and integrity-preserving range query Proto-filter for two-tiered sensor networks. To preserve privacy, SecureQ 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.

To preserve integrity, Truth confirmation algorithm to generate integrity verification information so that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query.

Furthermore, a solution to adapt SecureQ for event-driven sensor networks, where a sensor submits data to its nearby storage node only when a certain event happens and the event may occur infrequently. SecureQ provides significantly better security and privacy. While prior art allows a compromised storage node to obtain a reasonable estimation on the value of sensor collected data and sink issued queries, SecureQ makes such estimation very difficult.

Second, SecureQ delivers orders of magnitude better performance on both power consumption and storage space for multidimensional data, which are most common in practice as most sensors are equipped with multiple sensing modules such as temperature, humidity, pressure, etc.

A. Objective

The main objective of the project is to develop a secure and efficient query processing and to achieve Data privacy, Query privacy and Integrity preserving with low communication cost in two tier sensor networks.SecureQ will be used to preserve privacy and to reduce communication cost simultaneously.

B. Scope

The scope of the project is to achieve Confidential communication and secret data storing, Protection of data alteration. 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.

Potential applications of sensor networks include:

- Industrial automation
- Automated and smart homes
- Video surveillance
- Traffic monitoring
- Medical device monitoring
- Monitoring of weather conditions
- Air traffic control
- Robot control.
- Area monitoring
- Environmental/Earth monitoring
- Air quality monitoring
- Environmental magnitudes
- Gas & particle concentration
- Ambient monitoring
- Air pollution monitoring
- Forest fire detection
- Water quality monitoring
- Industrial monitoring
- Machine health monitoring
- Industrial sense and control applications
- Greenhouse monitoring
- Smart home monitoring

But wireless sensor networking has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking.

II. RELATED WORK

A. Privacy and Integrity Preserving in WSNs

Privacy- and integrity-preserving range queries in WSNs have drawn people's attention recently. Fei Chen and Alex X. Liu proposed a scheme to preserve the privacy and integrity of range queries in sensor networks.They introduced SafeQ protocol[2] to preserve privacy, Neighborhood chain and Merkle Hash tree to preserve integrity, Bloom filter has introduced to reduce communication between sensors and storage node.

The main issues,there is separate entities for each and every operartion and the cost of bloom filter is high.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

III. MODELS AND PROBLEM STATEMENT

A. *System Model*

A Two-tired sensor network consists of three types of nodes: sensors, storage nodes, and a sink. Sensors are inexpensive sensing devices with limited storage and computing power. They are often massively distributed in a field for collecting physical or environmental data, e.g., temperature. Storage nodes are powerful wireless devices that are equipped with much more storage capacity and computing power than sensors. Each sensor periodically sends collected data to its nearby storage node. The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then disseminates the queries to the corresponding storage nodes, which process the queries based on their data and return the query results to the sink. The sink unifies the query results from multiple storage nodes into the final answer and sends it back to the user.

B. Threat Model

For a two-tiered sensor network, we assume that the sensors and the sink are trusted, but the storage nodes are not. In a hostile environment, both sensors and storage nodes can be compromised. If a sensor is compromised, the subsequent collected data of the sensor will be known to the attacker, and the compromised sensor may send forged data to its closest storage node. It is extremely difficult to prevent such attacks without the use of tamper-proof hardware. However, the data from one sensor constitute a small fraction of the collected data of the whole sensor network. Therefore, we mainly focus on the scenario where a storage node is compromised. Compromising a storage node can cause much greater damage to the sensor network than compromising a sensor. After a storage node is compromised, the large quantity of data stored on the node will be known to the attacker, and upon receiving a query from the sink, the compromised storage node may return a falsified result formed by including forged data or excluding legitimate data. Therefore, attackers are more motivated to compromise storage nodes.

C. . Problem Statement

The fundamental problem for a two-tired sensor network is the following: How can we design the storage scheme and the query protocol in a privacy- and integrity-preserving manner? A satisfactory solution to this problem should meet the following two requirements.

1) Data and query privacy: Data privacy means that a storage node cannot know the actual values of sensor collected data. This ensures that an attacker cannot understand the data stored on a compromised storage node. Query privacy means that a storage node cannot know the actual value of sink issued queries. This ensures that an attacker cannot understand, or deduce useful information from, the queries that a compromised storage node receives.

2) Data integrity: If a query result that a storage node sends to the sink includes forged data or excludes legitimate data, the query result is guaranteed to be detected by the sink as invalid. Besides these two hard requirements, a desirable solution should have low power and space consumption because these wireless devices have limited resources.

IV. MODULE DESCRIPTION

A. 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.

B. 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.

C. SecureQ Module

SecureQ is a Proto-filter that prevents attackers from gaining information from both sensor collected data and sink issued queries. SecureQ also allows a sink to detect compromised storage nodes when they misbehave. To preserve privacy, SecureQ 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. To preserve integrity, Truth confirmation algorithm to generate integrity verification information so that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

Operations Of SecureQ Proto-filter as a Protocol

1) Select any one of the value from the original data, which is already stored into the storage node.
2) Selected data will be computed (any basic arithmetic operation and it will be selected randomly) with remaining data.
3) Finally, generating new encoded data set, which will be viewed by the Unauthorized user

Operations Of SecureQ Proto-filter as a filter

1) Identify the different types of sensor.
2) Dynamically observe the number of active sensors in the sensor networks
3) Based on the user request, Dynamically Storage nodes stimulate the filter to rearrange the data according to the sensor id.
4) Dynamically SecureQ filter rearrange the data based on the value of the data.
5) Dynamically storage node sends the accurate response data to the user with the help of Proto-filter.

Truth confirmation algorithm

After the sink receives Query Result and Verification Object , it verifies the integrity of Query Result as follows. First, the sink verifies that every item in Query Result satisfies the query. Second, the sink verifies that the storage node has not excluded any item that satisfies the query. Let $\{(E_{n1-1}|E_{n1})k_{i,\ldots,}\ (E_{j-1}|E_j)k_i\ _{,\ldots,}\ (E_{n2-1}|E_{n2})k_i\ \}$ be the correct query result and Query Result be the query result from the storage node.

We consider the following four cases.

1) If there exists n1<j<n2 such that ,$(E_{j-1}|E_j)_{ki} \notin$ QUERY RESULT, the sink can detect this error because the items in QUERY RESULT do not form truth information.
2) If $(E_{n1-1}|E_{n1})_{ki} \notin$ QUERY RESULT, , the sink can detect this error because it knows the existence of E_{n1} from $(E_{n1}|E_{n1+1})_{ki}$ and E_{n1} satisfies the query.
3) If $(E_{n2-1}|E_{n2})_{ki} \notin$ QUERY RESULT, the sink can detect this error because it knows the existence of En_2 from the item $(E_{n2}|E_{n2+1})_{ki}$ in VERIFICATION OBJECT and E_{n2} satisfies the query.
4) If QUERY RESULT=$\emptyset$, the sink can verify this fact because the item $(E_{n2}|E_{n2+1})_{ki}$ in VERIFICATION OBJECT should satisfy the property $E_{n2} < a \leq b < E_{n2+1}$

D. Sink Module

The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then disseminates the queries to the corresponding storage nodes, which process the queries based on their data and return the query results to the sink. The sink unifies the query results from multiple storage nodes into the final answer and sends it back to the user. Sink can detect compromised storage nodes when they misbehave.

V. CONCLUSION

We make three key contributions in this paper. First, we propose SecureQ, a novel and efficient Proto-filter for handling range queries in two-tiered sensor networks in a privacy- and integrity-preserving fashion.SecureQ significantly strengthens the security of two-tiered sensor networks.SecureQ prevents a compromised storage node from obtaining a reasonable estimation on the actual values of sensor collected data items and sink issued queries. In terms of efficiency, our results show that SecureQ significantly outperforms prior art for multidimensional data in terms of both power consumption and storage space. Second, we propose an single entity,which acts as protocol as well as filter to preserve privacy and communication cost respectively Third, we propose a solution to adapt SecureQ for event-driven sensor networks.

ACKNOWLEDGMENT

First and foremost I thank and praise Almighty for giving me wisdom and courage to take over this paper. I take the privilege to express hearty thanks to my parents for their valuable support and effort to complete. I take this chance to express my deep sense of gratitude to my Management, Principal Dr.T.A.Ragavendiran M.E., Ph.D, Director Prof J.R. Balakrishnan and Mrs. S. Roselin Mary M.Tech (Ph.D), Head of the Department, Department of Computer Science and Engineering, for providing an excellent infrastructure and support.

REFERENCES

[1] Kamran Tirdad, Pedram Ghodsnia, J. Ian Munro, and Alejandro," COCA Filters: Co-Occurrence Aware Bloom Filters", NSERC of Canada,2011

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, January 2013

[2] F. Chen and A. X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," in *Proc. IEEE INFOCOM*, pp. 1–9., 2010
[3] 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.*, VERIFICATION OBJECTl. 8, no. 4, pp. 427–442, 2003.
[4] P. Desnoyers, D. Ganesan, H. Li, and P. Shenoy, "Presto:A predictive storage architecture for sensor networks," in *Proc. HotOS*, p. 23,2005,
[5] 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*, pp. 31–44.
[6] B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensor networks,"in *Proc. ACM MobiHoc*, 2006, pp. 344–355,2005,
[7] B. Sheng, C. C. Tan, Q. Li, and W. Mao, "An approximation algorithm for data storage placement in sensor networks," in *Proc. WASA*, pp. 71–78,2007.
[8] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in two tiered sensor networks," in *Proc. IEEE INFOCOM*, pp. 46–50,2008
[9] W. A. Najjar, A. Banerjee, and A. Mitra, "RISE:More powerful, energy efficient, gigabyte scale storage high performance sensors," 2005
[10] J. Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor networks," in *Proc. IEEE INFOCOM*, 2009, pp. 945–953.
[11] R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional range queries in sensor networks," in *Proc. ACM MobiHoc*, pp.197–206,2009.
[12] H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in *Proc. ACM SIGMOD*,pp. 216–227, 2002.
[13] B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in *Proc. VLDB*, 2004, pp. 720–731.
[14] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD*, pp.563–574, 2002.
[15] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE S&P*, pp. 44–55, 2000.
[16] H. Pang and K.-L. Tan, "Authenticating query results in edge computing,"in *Proc. ICDE*, p. 560, 2004.
[17] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in *Proc. ACM SIGMOD*, pp. 407–418, 2005.
[18] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," in *Proc. DASFAA*,pp.420–436, 2006.
[19] W. Cheng, H. Pang, and K.-L. Tan, "Authenticating multi-dimensional query results in data publishing," in *Proc. DBSec*, pp. 60–73, 2006.
[20] H. Krawczyk,M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," RFC 2104, 1997.
[21] R. Rivest, "The md5 message-digest algorithm," RFC 1321, 1992.
[22] D. Eastlake and P. Jones, "Us secure hash algorithm 1 (sha1)," RFC 3174, 2001.
[23] B. Bloom, "Space/time trade-offs in hash coding with allowable errors,"*Commun. ACM* vol. 13, no. 7, pp. 422–426, 1970.

BIOGRAPHY

Balaji.A.S is presently doing Master degree (M.E-CSE) as a part time course in Anand Institute of Higher Technology,Chennai.Currently working as a Lecturer in Anand Institute of Higher Technology,Chennai.His area of interest includes Computer networks,Wireless sensor networks and Software Engineering etc.

S. Roselin Mary is an Associate professor and HOD In charge of the Department of Computer science and engineering, Anand Institute of Higher technology at Chennai. She has 9 years of teaching experience. Her area of interest includes Software architecture, Digital image processing and wireless sensor networks. She guided many Master degree level projects and published variety of papers in many conferences and journals.

Femila Goldy.R is presently working as a Assistant Professor in Anand Institute of Higher Technology, Chennai. She had published many papers in conferences and journals. Her area of interest includes Image Processing, Pattern Recognition and Wireless sensor networks etc.