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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Protecting Storage Node and Its Communications With Sink in a Two Tier Sensor Network

K.Prashanth[1], J.Praveen Kumar[2]

Student, Department of CSE, Malla Reddy College Engineering and Technology, Hyderabad, India [1]

Assistant Professor, Department of CSE, Malla Reddy College Engineering and Technology, Hyderabad, India [2]

Abstract: In Wireless Sensor Networks where two – tier architecture is used, the storage nodes hold the data collected by sensors acting as mediator between sink and sensors. This will help in efficient query processing in WSN. However, in reality the storage nodes are the center of attraction to attackers. Recently Chen and Liu proposed a protocol that will protect the WSN and support privacy preserving range queries. This protocol uses a novel technique for encoding data, queries and results in such a way that the whole communication is secured. In this paper we implemented a custom simulator which demonstrates the proof of concept. The empirical results revealed that the proposed security approach is effective.

Index Terms: WSN, data integrity, two tier architecture, range queries

I.INTRODUCTION

WSNs are widely used application where human presence is not required or not possible. For instance they can be deployed for earthquake prediction, building safety monitoring, environment sensing and so on. In this paper two-tier architecture is considered for WSN for effective storage and retrieval. The architecture is as shown in fig. 1. The storage node gets data from sensors and it is meant for storing only. The sensor nodes are responsible to sense data from surroundings and send the data to storage node. The sink is privileged to make range queries on storage node and take the required information. This architecture is flexible and ensures efficient storage. Sensors also save power by sending data to nearest node. Sensors are also relieved from storage as the storage takes place in storage node. This kind of architecture is explored in [1], [2], [3], [4], and [5]. There are commercially available known as RISE [6], and StarGate [7].

The inclusion of special storage node causes security problems in WSN. The storage node is subjected to various attacks. Therefore it is important to secure communication in the WSN that is based on two tier architecture. Chen and Liu [8] presented a security protocol that ensures data integrity in WSN. The communication between the storage and sink is encoded thus making is secure. Prior solution to this problem is proposed by Sheng and Li [5] which has two drawbacks. It allows attackers to estimate[9], [10], [11], [12], [13] and [14] the data and the power consumption is more which reduces the lifetime of WSN. In this paper we built a customer simulator the simulates the sensor nodes, storage node and sink with the secure data transfer mechanisms. The experimental results are encouraging and the security mechanisms are reliable.

The remainder of this paper is structured as follows. Section II presents review of literature. Section III presents proposed security mechanisms. Section IV presents custom simulator details. Section V provides experimental results while the section VI concludes the paper.

II.PROPOSED SYSTEM MODEL SECURITY

We consider the two tier architecture for modeling the system and illustrate the mechanism to solve security problems in two tier architecture. Two-tier architecture actually separates the layers. The sensors do not directly communicate with the sink. There is storage node which is specially meant for storing the data collected from sensor nodes. This adds flexibility to the network. The sink can make range queries on the storage node. However, this network causes security problems when storage node is compromised. Security attacks are made on storage node. The typical two tier architecture is as shown in fig. 1.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

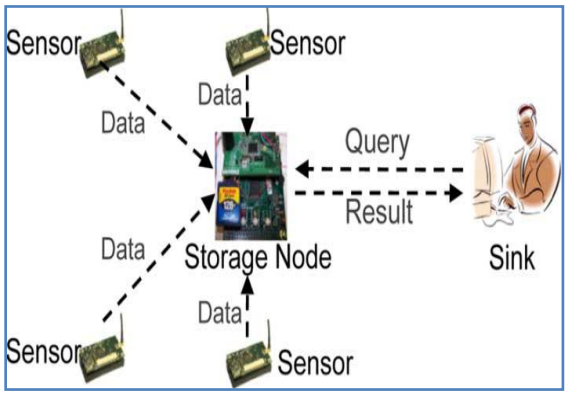

Fig. 1 –WSN in Two – Tier Architecture (excerpt from [8])

As can be seen in fig. 1, there are three different nodes involved in the architecture. They are the sensor nodes, storage node and sink. The sensor nodes are responsible to sense data from their surroundings and send the collected data to storage node. The storage node cannot sense data. However, it can only store data. This data is queried by sink. The sink is having access to storage node and can obtain data required.

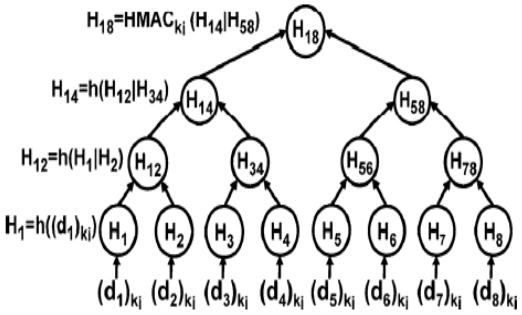

Fig 2 Merkle hash tree for eight data items

As shown in the above figure represents Mrekle hash free of the data items.

Threat Model

The sensor and sink involved in two tier architecture of WSN are assumed to be trusted. They do not cause any security problems to the network as per our assumption. When the storage node is compromised the data will be lost. We focus on protecting the storage node from malicious attacks. The proposed solution ensures data and query privacy, and data integrity.

Security Model

The security mechanism we have implemented is influenced by the approach proposed by Chen and Liu [8]. A secret key is associated with every sensor in the WSN. Each sensor shares it with the sink. The data sensed by the sensor is encrypted using the secret key which is shared with sink. The encrypted data and associated information is sent to storage node. The protocol we implemented takes care of secure communication among the three parties such as sensor node, storage node and sink. When the sink makes query, the storage node involves in the security mechanism and finally sends requested data to sink after authenticating the sink. The sink will be able to decrypt the data with the shared key of the sensor from which the data has been collected.

III.CUSTOM SIMULATOR

We have built a custom simulator in Java programming language which models a network among the storage node, sensors and sink. The environment used for developmentincludes a PC with 2GB RAM, Core 2 Dual processor running Windows 7 OS. The NetBeans IDE (Integrated Development Environment) is used to build application. Java SWING API is used to model the sensor, storage node and sink with Graphical User Interface (GUI). The three representations are presented here. Fig. 1 shows a typical sensor node which can send data to storage node.

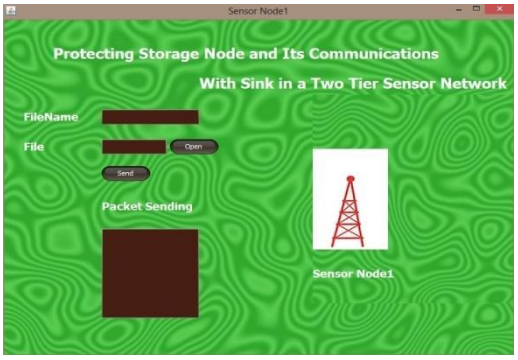

Fig. 3– A typical sensor node representation

As can be seen in fig. 3, the GUI encapsulates the sensor node. It simulates sensor node behavior. The data it senses is sent to storage node. The communication between the storage node and sensor nodes is for data transfer only. The sensor nodes do not send data directly to sink.

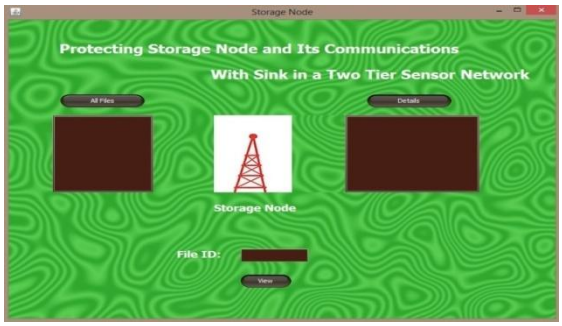

Fig. 4– A typical storagenode representation

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

As can be seen in fig. 4, the GUI encapsulates the storage node. It simulates storage node behavior. The data sent by sensor nodes is stored here. In turn it communicates with the sink. The sign takes required data from the storage node as per the two-tier architecture illustrated in fig. 1.

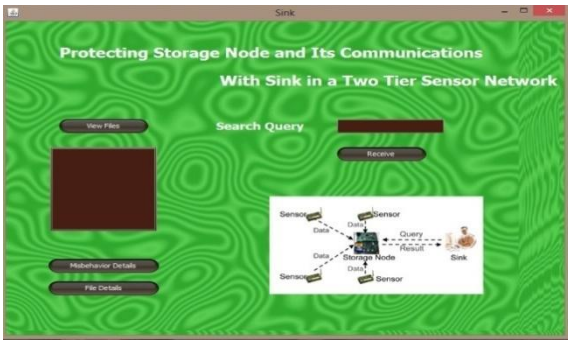

Fig. 5– A typical Sink node representation

As can be seen in fig. 5, it encapsulates the sink node behavior. It is responsible to collect data from storage node as and when required. In fact it can make privacy and integrity preserving range queries to storage node to obtain required information.

IV.EXPERIMRNTAL RESULTS

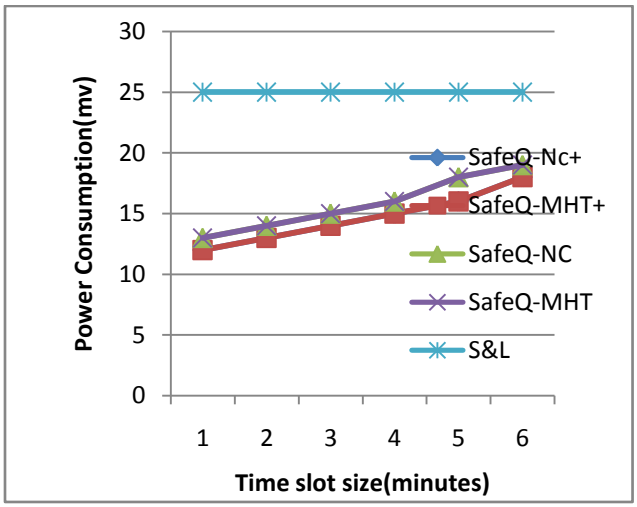

Fig 6Average power consumption per submission for a sensor. Three-dimensional data

As shown in the above figure represents the horizontal axis represents time slot size while vertical axis represents power consumption.

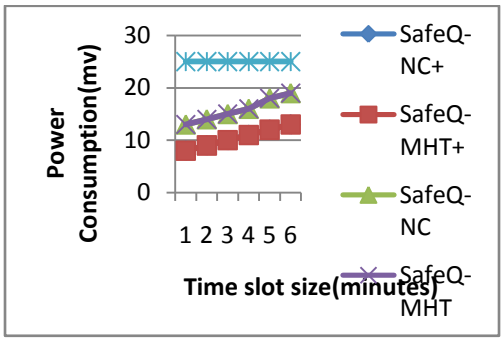

Fig 7 Average power consumption per submission for a sensorTwo-dimensional data.

As shown in the above figure represents the horizontal axis represents time slot size while vertical axis represents power consumption.

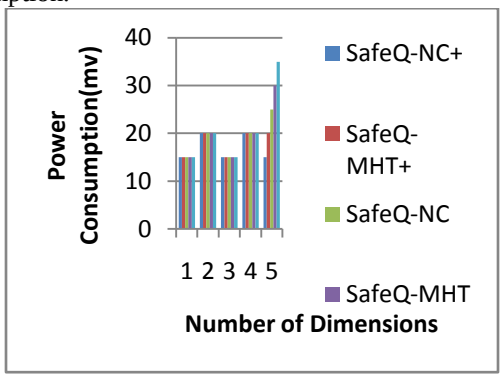

Fig 8 Average power consumption per submission for a sensor For 10 min.

As shown in the above figure represents the horizontal axis represents Number of Dimensions while vertical axis represents power consumption.

V.CONCLUSION

In WSN two tier architecture causes security attacks as the data is stored in storage node. The storage node is vulnerable as the attackers make exclusive attacks on the storage node only. Therefore it is inevitable to have a robust security mechanism that can prevent the security problems in WSN that uses two tier architecture. We implement a novel protocol proposed by Chen and Liu [37]. The protocol ensures encoded communication among the storage node and sinksto ensure data integrity. We also build a custom simulator of WSN where the sensor, storage node and sink are simulated with their respective behavior. We applied the protocol in order to test the network. The experimental results revealed that the proposed security mechanism is robust to attacks.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

REFERENCES

[1] P. Desnoyers, D. Ganesan, H. Li, and P. Shenoy, "Presto:A predictivestorage architecture for sensor networks," in *Proc. HotOS*, 2005, p. 23.
[2] D. Zeinalipour-Yazti, S. Lin, V. Kalogeraki, D. Gunopulos, and W. A.Najjar, "Microhash: An efficient index structure for flash-based sensordevices," in *Proc. FAST*, 2005, pp. 31–44.
[3] B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensor networks,"in*Proc. ACM MobiHoc*, 2006, pp. 344–355.
[4] B. Sheng, C. C. Tan, Q. Li, and W. Mao, "An approximation algorithmfor data storage placement in sensor networks," in *Proc. WASA*, 2007,pp. 71–78.
[5] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in twotieredsensor networks," in *Proc. IEEE INFOCOM*, 2008, pp. 46–50.
[6] W. A. Najjar, A. Banerjee, and A. Mitra, "RISE:More powerful, energyefficient, gigabyte scale storage high performance sensors," 2005[Online]. Available: http://www.cs.ucr.edu/~rise
[7] Xbow, "Stargate gateway (spb400)," 2011 [Online]. Available: http://www.xbow.com
[8] Fei Chen and Alex X. Liu" Privacy- and Integrity-Preserving Range Queries in Sensor Networks". IEEE/ACM TRANSACTIONS ON NETWORKING.
[9] S. Madden, "Intel lab data," 2004 [Online]. Available: http://berkeley.intel-research.net/labdata
[10] J. Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensornetworks," in Proc. IEEE INFOCOM, 2009, pp. 945–953.
[11] R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional rangequeries in sensor networks," in Proc. ACM MobiHoc, 2009, pp.197–206.
[12] H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL overencrypted data in the database-service-provider model," in Proc. ACMSIGMOD, 2002, pp. 216–227.
[13] B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index forrange queries," in Proc. VLDB, 2004, pp. 720–731.
[14] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preservingencryption for numeric data," in Proc. ACM SIGMOD, 2004, pp.563–574.

BIOGRAPHIES

K.Prashanth is student of Malla Reddy College of Engineering and Technology, Hyderabad, AP, INDIA. He has received B.Tech Degree in Information Technology and M.Tech degree in Computer Science and Engineering. His main research interest includes Networking.

J.Praveen Kumar is working as assistant professor in CSE department at Malla Reddy College of Engineering and technology and having 5 years experience in teaching field. Received Post Graduation M.Tech from the stream of Computer Science Engineering from Bharath University Chennai. His main research interest includes Networking and WSN.