ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (369-371), Month: April - June 2015, Available at: www.researchpublish.com

Privacy and Integrity Preserving In Three Tier Architecture Using Symmetric Key Sharing Method and MAC Address

[1]Manasa .D.S., [2]Mrs Shruthi. G

[1]Mtech final year, [2]Assistance professor, Dept of CSE, DonBosco institute of technology, Kumbalagodu, Bangalore, India

Abstract: **In sensor network the master nodes are responsible for storing the data sensed from environment and these are the nodes which are always the target of attackers, because of this the master node may return incomplete or fake results. To overcome this we propose a simple method by using symmetric key sharing method and unique address(MAC).**

Keywords: **Sensor network, privacy, integrity, WSN.**

I. INTRODUCTION

Wireless sensor network: are spatially distributed sensors to monitor environmental changes temperature, sound, pressure etc. and pass them to the main location or to main storage node. Sensors: sensors are then devices used to detect physical changes like light, temperature, sound pressure, etc. and store them and respond by taking some measures. Top-k: query asks for data whose attributes are among k- highest values. Example: Return top-5 paths with minimum kilometers from Bangalore to Delhi.[5]

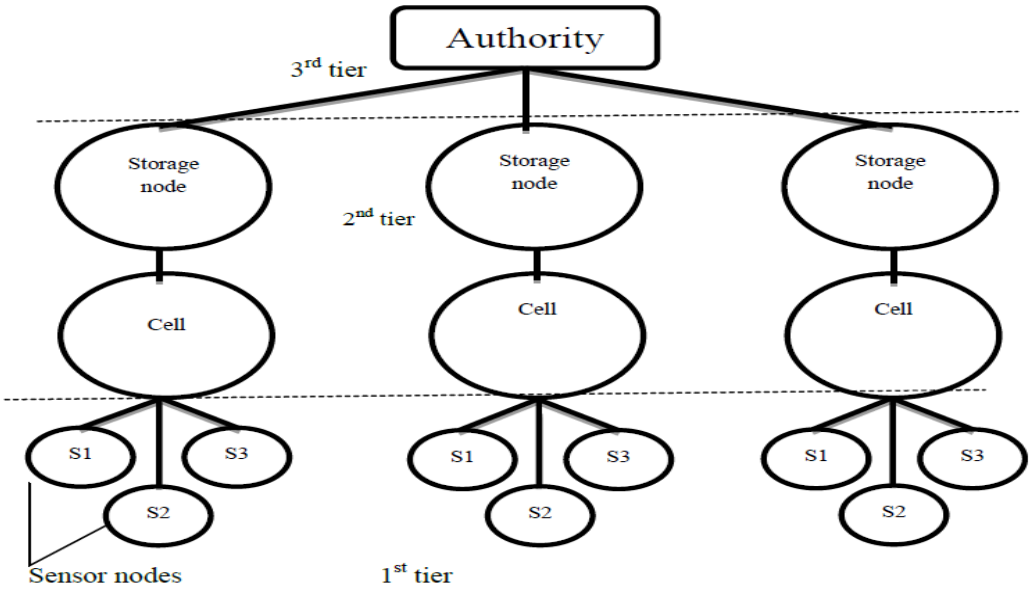

Fig.1 Three Architecture of WSN

The three tier architecture looks like fig1, first layer consist of normal sensor nodes which senses the environment and collect the data, sensor nodes are grouped based on distance and form cell, second layer consist of node which stores all data collected from the sensor nodes is called as storage node and third layer consist authority which is responsible for distributing keys and issuing the queries.

II. RELATED WORK

Top-k result integrity was addressed in "secure query processing via untrusted location-based service provider" [1], where distributed data sources generate and forward the sensed data to a proxy node. Their network model differ from our because in "secure query processing via untrusted location-based service provider" it is a trusted single proxy node that generates the integrity verification materials whereas in our consideration there is no trusted central authority like proxy for such responsibility.

Verifiable query processing also considered in the context of range query. In "verifiable privacy-preserving range query in two tiered sensor network"[2] bucketization to mix the data for a range, use message encryption for data integrity, and employ encoding numbers to prevent the storage nodes from dropping data. In this approach, the value domain is divided into multiple buckets and each bucket is assigned with a tag. There is no overlap or gap between consecutive buckets, i.e., every value is covered by exactly one bucket. Sensors and the sink have agreed on the same range partition, which is unknown to storage nodes.

When sending data to the storage nodes, sensors attach the corresponding tag to every encrypted data based on which bucket the data falls into. The data values assigned with the same tag can be encrypted as a block.

The query result completeness is achieved by requiring sensors to send cryptographic one-way hashes to the storage node even when they do not have satisfying reading.

In "Secure Range Queries in Tiered Sensor Networks" and "Secure Multidimensional Range Queries in Sensor Network" [3][4]crosscheck was also utilized to secure range query. By converting the verification of whether a number is in a range to several verification of whether two numbers are equal.

III. PROBLEM STATEMENT

When the network owner receives the top-k query, the main aim is to receive top-k query result, it must fulfill following requirements

1) Privacy: the sensor reading sent from the sensor must not be read by others.
2) Integrity: data must be as it is sent from the sensor nodes.
3) The obtain data must be complete and it must not be fake.

IV. PERFORMANCE METRICS

1. Communication cost.
2. Storage space.

V. PROPOSED METHOD

The model we consider here is fig1, in the above model we consider 3teir, 1st tier consist of ordinary sensors which collect the data from environment, based of distances sensor nodes are grouped to form cells, second tier consist of storage node which store the data and respond to the query from the authority, third tier consist of authority which issues the query.

The method used is symmetric key sharing and assigning unique address (MAC address) for each sensor node, initially the authority will issue the public keys to all the sensor nodes, the sensor nodes will encrypt data using symmetric secret keys and then the encrypted data will be forwarded to the storage node.

Description Parameter used in algorithm

D1, D2, D3…… Dn----------> Data collected from environment

D1^, D2^……Dn^ + secret key ----------> Encrypted data

Algorithm at the sensor is

Sensor nodes MAC address must be present in authority to send data

Step1: Collect the data from the environment.

D1, D2, D3…… Dn

Step2: Encrypted using secret key.

Encryption (D1^, D2^, D3^…… Dn^+ secret key)

Step3: Forward data to storage node.

Algorithm at the authority:

Step1: Issues the Top-1 query

Step2: Receive the Top-1 query result from the storage node.

Step3: Decrypt the data received

Decrypt (D1^, D2^, D3^…… Dn^ +) + secret key (same secret key is used as in sensor node)

Decrypted data = D1, D2, D3…… Dn

Step4: Check the unique address of Node from where the data is come from, if it is from of sensor node which is in that range then data is accepted.

Step5: If the received data is as expected and if even more appropriate results are needed then issue another top-1 query.

VI. CONCLUSION

By using simple symmetric secret key the architecture require less space to store keys since it must store single, and less space to store data. Using this method the data can be saved in the nearest storage node so communication cost can be reduced. This method will provide security by using MAC address so that no other nodes can send data except those nodes whose MAC address stored in authority.

REFERENCES

[1] R. Zhang, Y. Zhang, and C. Zhang, "Secure top-k query processing via untrusted location-based service providers," in Proc. 24th IEEE Conf. Comput.Commun., Mar. 2012, pp. 1170–1178.

[2] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in two-tiered sensor networks," in Proc. 24th IEEE 27th Conf. Comput.Commun., Apr. 2008, pp. 743–766.

[3] J. Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor networks," in Proc. 24th IEEE Conf. Comput. Commun., Jan. 2009,pp. 1–9.

[4] R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional range queries in sensor networks," in Proc. ACM Int. Symp. Mobile Ad Hoc Netw.Comput., 2009, pp. 197–206.

[5] C.-M. Yu, G.-K. Ni, I.-Y. Chen, E. Gelenbe, and S.-Y. Kuo, "Top-k query result completeness verification in sensor networks," in Proc. IEEE Int. ICC Workshops, Jun. 2013, pp. 1026–1030.