ISSN No. 0976-5697

Volume 4, No. 2, Jan-Feb 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Protected Multi-tiered Sensor Network Uses Spatiotemporal Feature

M. Adimoolam*, K. Hemachandran, R. Prasanth, N. Prabavathi and Melbin T. Mathew
Information Technology Christ College of engineering and technology
Puducherry, India
m.adimoolam@gmail.com*1, k.hemachandran4@gmail.com, prasi.0604@gmail.com,
prbmarthi@gmail.com, melbinthakidi@gmail.com

Abstract: The reliance on sensor nodes for sending data to the master node raises serious concerns about both data confidentiality & authenticity in hostile environments. In particular an unauthenticated sensor node may exist in the network which leads to various attacks. We target a multi-tier sensor network with resource rich master node at the upper tier and authentication nodes at the middle tier. Master nodes collect data from the sensor nodes and response the queries from the network holder. The proposed scheme offers data confidentiality by providing authentication to sensor nodes which exists in the network (particularly in the cell). The keys which are used for authentication is remains valid only over a session time which makes the sensor network protected. The high efficiency of our approaches is defined by detailed performance evaluations.

Keywords: unauthenticated sensor node; authentication; master node; sensor node; queries; network owner

I. INTRODUCTION

In general, wireless sensor networks (WSNs) has a two-tier architecture, in which it consists of the resource constrained sensor nodes as lower-tier and resource rich sensor master nodes at the upper-tier [1]. In advance we focus an additional tier (i.e. Multi-tier) which consists of resource constrained authentication nodes which is present in the cell and is responsible to recruit the certain sensor nodes to join the network since the environment is unattended like forest areas [2]. By default there are two ways for network owner to access the data generated by the sensor nodes. First, sensor nodes send their data to adjacent master nodes which in turn forward the data instantly along an upper-tier multi-hop, to the network owner. This approach requires a stable repeatedly on communication connection from the master node to the network owner [2]. Push & pull model are the two basic data access methods and in this push model, the data continuously generated by the sensor nodes are sent in real time to an extrinsic data sink hole and various queries resolved in a centralized fashion. More suitable for surveillance and monitoring applications. In the pull model, data which is perceived from the environment through sensors where stored inside the network and abide on-demand queries. That model is suitable for an application which doesn't for live data like military, commercial and scientific applications [2]. This approach may consume unnecessary energy of master sensor nodes if the network owner is only interested in a small portion of the probably huge amount of data composed over time.

The main advantage of this second approach is rapid progress in storage technology and aspects the WSN as a storage system [3]. In considering a multi - dimensional range queries which ask for data with one or multiple attributes falling in specified ranges in sensor networks [4].

An exemplary multidimensional range query is "Return all observed objects with weights between 170 and 220 pounds and moving speeds between 3 and 5 miles per hour" [4]. Event data generated by sensor nodes described generally as a tuple of attribute values and it may be the weight of an observed object, or its location or its speed or its appearance or lingering time. In the experiments on small scale test bed [5], distributed index for multi-dimensional data (or DIM). A GPSR geographic routing algorithm is used for novel geographic embedding of data structure.

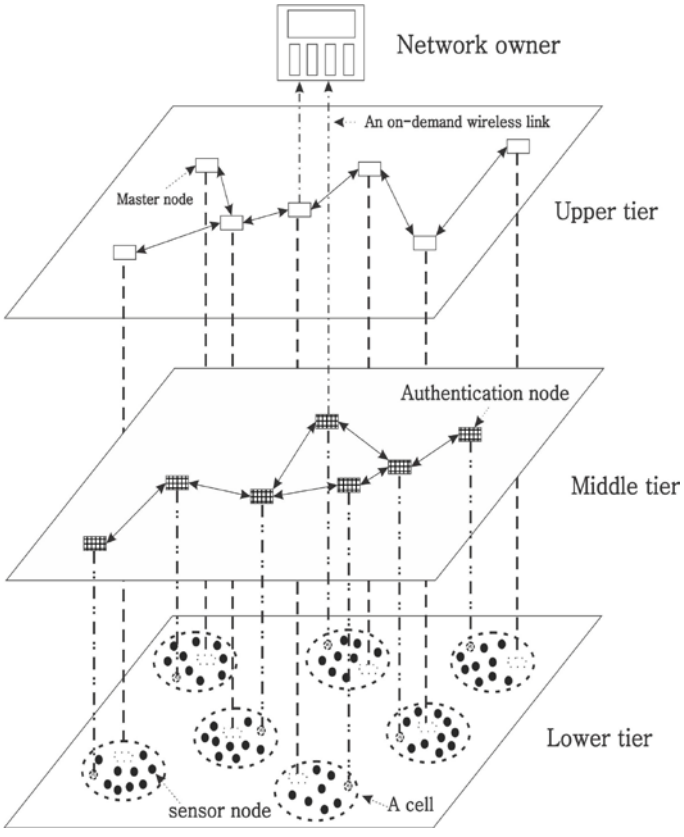

Figure 1. An Abstract Multi-tier Sensor network Architecture

Fig 1 shows the multi-tier model of sensor networks in complement with the Fig 2. An additional tier is added which consists of resource constrained authentication nodes. In each cell at least one authentication node is present in order to authenticate the sensor nodes which are exist in the network. In the prior system [6] architecture framework is followed.

In accordance with the security concerns that the unauthenticated or malicious sensor node may be attached to the network which results in sending unwanted data to the master node which lead to the traffic overhead during communication or intentionally provide misleading information to other nodes. For that a pairwise key management protocol for heterogeneous multi-tiered wireless sensor network [7] can be deployed. In the field of WSN a novel random key algorithm [8] can be utilized. Since the resource consumption of the sensor devices is less but the key can be identified by the adversary when it compromises a few sensor nodes. This paper is fully focused on providing authentication to the sensor nodes at the lower tier and to support multi-dimensional range query processing.

II. EXISTING SYSTEM

In the existing system, the bucketing technique is used to store encrypted data at the master sensor nodes and also ensure the range-query efficiency. The encryption algorithm used is a OCB-like authenticated encryption which can ensure query-result authenticity and data confidentiality over an extent and it uses the spatiotemporal approach to verify the query result, which is the combination of spatial crosscheck (SC) and the temporal crosscheck (TC) based on two-tier architecture. The lower sensor tier comprises a large number of sensor nodes with constrained resources, while the resource-rich master nodes are in the upper tier.

Master nodes are involved in computation and communication tasks from the data which are received from the sensor nodes. Therefore master nodes are resource-rich in nature respectively. The key idea of the spatial crosscheck is to embed some relationship among data generated by nodes during each epoch.

Single-attribute in the sense, the network owner can able to attain query results corresponding to any one of its attribute for comparison with other attributes the owner needs additional computational algorithms to manipulate the results. For example queries like "List all events that have weight more than 200lbs". If the network owner needs to find the habitats with a certain speed and weight owner must be able to pass queries with a single attribute individually and in most cases a manual evaluation will be required to filter the results.

A. Multidimensional Range queries:

Event data generated by sensor nodes can generally be described by the attribute values, where $d \geq 1$ depends on concrete sensor network applications. Each attribute $\{A_j\}_{j=1}^{d}$ represents a sensor reading or an aspect of the event such as weight of an observed object, location, speed and its moving direction, or appearance of lingering time [4]. For the sake of simplicity, we will focus on the following types of primitive multidimensional range queries [4].

$$(\text{Cell} = C) \wedge (\text{Epoch} = t) \bigwedge_{j \in [1,d]} (l_j \leq A_j \leq h_j),$$

Where C and t denote the cell ID and the interested epoch, respectively, and [lj,hj] is the interested range of attribute Aj.

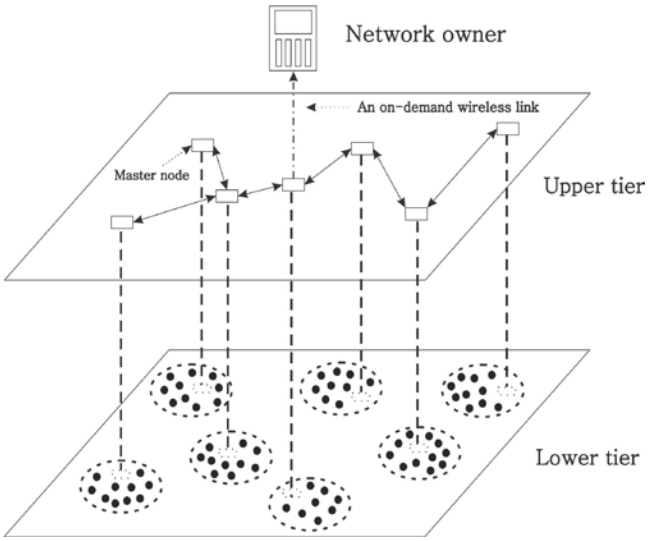

Figure 2. Two-Tier Sensor Network Architecture

Fig 3 illustrates the communication procedure followed in the two tier architecture which the sensor nodes are responsible to sense the environment and conveys to the master node through encrypted form and the master node is involved in storing the data through the bucketing technique. Since it is pull model, data are stored inside the network. Symmetric key encryption is used therefore the same key has been used for both encryption and decryption, encryption is done in the sensor node where decryption is done by the network owner.

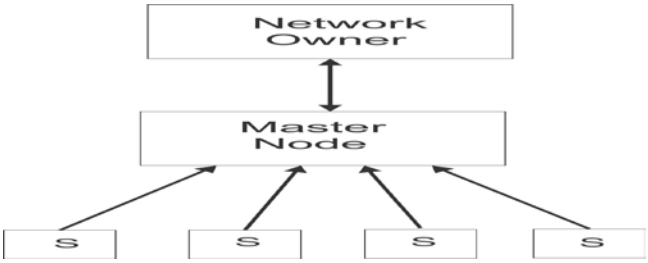

Figure 3. Block Diagram of Prior System

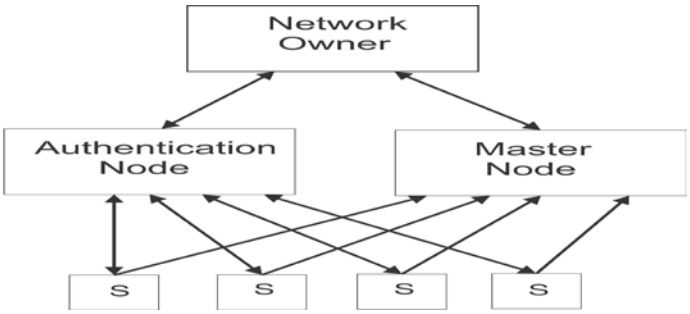

Figure 4. Block Diagram of Proposed System

III. PROBLEM IN THE EXISTING SYSTEM

Since the key idea of the spatial crosscheck is to embed some relationships to the and to send data index of the certain node to other nodes in the cell which has the capability to provide data confidentiality but when an unknown sensor node exists in a cell can able to receive the data index so that the node can be easily identified and compromised and it encourages the adversary to eavesdrop the communication.

Let us consider an arbitrary number of sensor nodes are present in a cell $\{S_k\}_{k=1}^{N}$. Assume that one sensor node in the cell has been compromised and the adversary has the control over it, now the adversary can able to overload the communication among other sensor nodes by increasing the traffic. In an extreme case the adversary able to collapse the network over a cell.

IV. PROPOSED SYSTEM

In our system multi-dimensional queries are resolved according to [3]. In complementary to the existing system which is a two-tier architecture where the unknown sensor nodes can eavesdrop the network for that an additional authentication node is provided which is responsible for authenticating the sensor nodes in a cell by evaluating the source key(which is from network owner)S_k with the sensor nodes key SN_k in a cell, which the SN_k is generated over a cell is the same among other nodes because it is infeasible for the network owner to generate more number of S_k keys to authenticate for a large system.

Here the separate key generation algorithms are used in a random manner. Here the function of authentication node is to generate $key_{S,SN}$ by performing EX-OR operation on both the keys S_k and SN_k

$$key_{S,SN} = S_k \oplus SN_k$$

Where the network owner and the sensor nodes sends the S_k and SN_k to the authentication node then the sensor nodes are authenticated by verifying the keys. Since HSC technique is used in the prior system which embeds the data index to the other sensor nodes in a cell in order to verify the query authenticity for that a sensor node must be authenticated, if the network owner needs to verify the sensor node, it is done by,

$$S_k \rightarrow S_k = key_{S,SN} \oplus SN_k$$

In this authentication mechanism, the key generated by both the network owner and the sensor node are valid only for a certain time. The key pool is stored in the authentication node for future verification. When the validation time t=0, a new key is generated, for sending data from sensor node to master node it uses OCB-encryption method, which is the process of integrating a Message Authentication Code (MAC) into the operation of block cipher.

V. IMPLEMENTATION AND PERFORMANCE EVALUATION

In this section, we illustrate the performance of the proposed algorithm. The proposed algorithm is implemented using NS2.35 Simulator in Ubuntu 12.04. The area considered is 600x600 and the algorithm is evaluated from 25 to 150 nodes. The proposed scheme is performed by 3o simulations with different simulation time and the simulation result concentrates on communication ration which is the number of actual communication and the number expected communication. By varying the number of nodes different communication ratios are obtained. Fig 4 shows that increase in communication ratio with the increase in the number of nodes

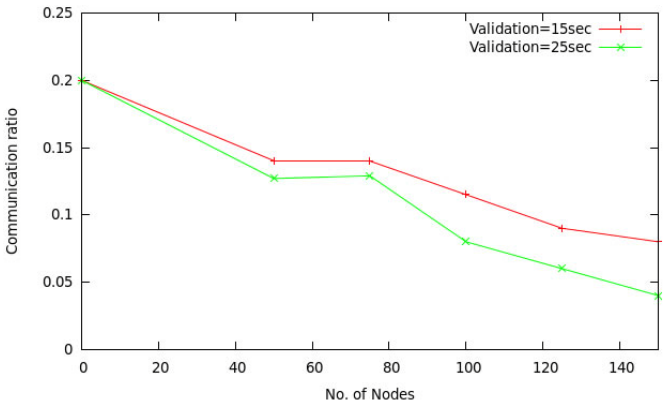

Figure 5. Communication Ratio with Different Validation Time

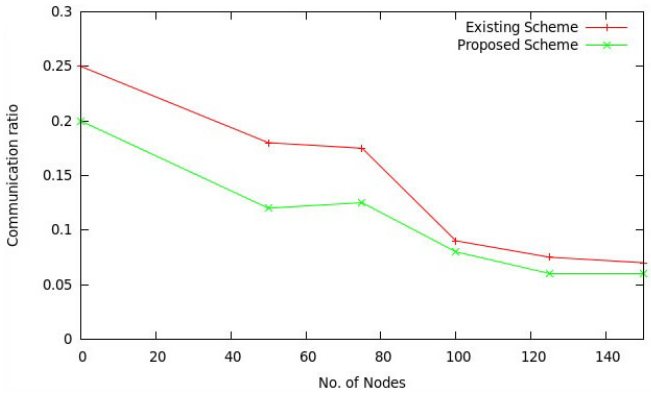

Figure 6. Comparison of proposed scheme with existing scheme

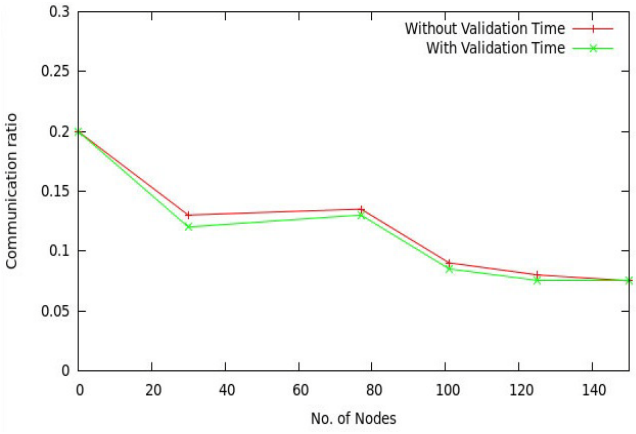

Figure 7. No Validation time vs Validation time.

Fig 6 shows that the proposed scheme is suited for smaller areas with lesser number of nodes deployed. Validation time is considered as the parameter in fig 7. This shows the difference between the existing algorithms with the proposed scheme.

VI. CONCLUSION

The proposed scheme is advantageous over the existing scheme that it does not affect the use of the OCB - encryption method also the key is valid only after a session time, which makes the system more secure by authenticating the existing sensor nodes in the network. The simulation results showed that the proposed scheme is suited for smaller areas which have lesser number of nodes. In the proposed scheme in order to authenticate the message OCB is used and to authenticate the sensor nodes public key encryption is used. Therefore the sensor nodes are robust against attacks.

VII. ACKNOWLEDGEMENT

Our thanks to the experts who have reviewed our paper and given valuable suggestions .We also thank our students Gunashanthi, Arulkumar and Adhavan for their support in the constant development and contribution to this project. We also thank our college management for providing the necessary infrastructure and constant support

VIII.REFERENCES

[1] J. Shi, Y. Zhang, R. Zhang, "A Spatiotemporal approach for secure Range queries in tiered Sensor Networks" in IEEE transactions on wireless communications, VOL 10. NO1 JAN 2011.

[2] J. Shi, Y. Zhang and R. Zhang "Secure range Queries in tiered Sensor Networks" in IEEE INFOCOM'09, Rio de Janeiro, Brazil, Apr.2009.

[3] N. Subramanian, C. Yang and W. Zhang "Secure distributed Data Storage and retrieval in Sensor Networks" in IEEE Percom'07, White Plains, NY, MAR 2007.

[4] R. Zhang, Y. Zhang and, J. Shi "Secure Multidimensional range queries in Sensor Networks" in Proc. ACM MobiHoc'09, New Orleans, LA, MAY 2009. PP 197-206.

[5] X. Li, Y. J. Kim, R. Govindan and W. Hong "Multidimensional range queries in Sensor Networks" in Proc. ACM SenSys'03, Los Angeles, California, USA, NOV 2003. PP63-75.

[6] O. Gnawali, K. Y. Jang, J. Peck, M. Viera, R. Govindan, B. Greensteinm, A. Joki, D. Estrin and E. Kohler, "The Tenet architecture for tiered Sensor Networks" in ACM Sensys'06, Boulder, Colorado, USA Oct. 2006. PP153-166.

[7] Manel Boujelben, HYoussef "Establishing Pairwise keys in Heterogeneous two-tiered Wireless Sensor Networks" in SENSORCOMM.2009

[8] J. Chao, Ren Xiuli, "A Novel Random Key Algorithm in Wireless Sensor Networks" in IEEE , PACIIA 2008.