International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483
Received on: 02.03.2018 Published on: 30.03.2018 Pages : 43-53

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 6, Issue 3, March 2018.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

PROFESSIONAL KEY MANAGEMENT TECHNIQUES AND SECURED MAPPING SCHEMES THROUGH WIRELESS DATA CENTRIC SENSOR NETWORKS

B. Jareena Banu[1a*], D. Sobya[2b], S. Nallusamy[3c]

[1]Lecturer, Department of Instrumentation and Control Engineering, Government Polytechnic College, Udhagamandalam, Nilgiri-641014, Tamilnadu, India
[2] Research Scholar, Department of Adult and Continuing Education and Extension, Jadavpur University, Kolkata-700032, India
[3]Professor, Department of Mechanical Engineering, Dr. M G R Educational and Research Institute, Chennai-600095 Tamil Nadu, India

[a]e-mail: jareenabanu67@gmail.com, [b]e-mail: sobyadevaraj@gmail.com,
[c]e-mail: ksnallu@gmail.com

Abstract

Currently there are many unmanned wireless data centric sensor networks developed for sensing data in different environment conditions facing several security problems, due its unattended nature and its lack of tamper resistance. If the mapping relation between a detector node and a storage node is known to the attacker, the node can be easily compromised. Hence, in this research different data location mapping schemes are utilized to protect against the mapping attack and efficient key management techniques are used to improve the data confidentiality and authentication. Further keyed bloom filter scheme is used to defend against query attack and to optimize the query process. Hashed message authentication code is framed with the established pairwise key and sent several hops down to mobile sink to improve data authentication. Network simulator of NS2 tool is used and from the observed results it was found that, reduced message overhead and message transmission delay and improved privacy level were obtained.

Keywords: WDCS, Security, Mapping Attack, Query Attack, KBF, HMAC

1. Introduction

Wireless networks are broadly classified into cellular, adhoc and sensor networks in which cellular and adhoc networks are manned and sensor networks are unmanned. This unmanned sensor networks are extremely useful in civil and military applications, such as remote surveillance and habitat monitoring, etc [1-5]. Wireless sensor networks are composed of large number of sensors densely deployed in the field of interest to collect data from environment Sensors are connected through wireless channels and each sensor node senses, processes and sends the data to its neighbors or to the sink node. Since the sensor network size and volume of sensed data are increasing nowadays, efficient data dissemination and accessing techniques are necessary [6-10]. To satisfy this requirement Data Centric Sensor (DCS) networks are developed. In DCS, storage events are named, and sensors cooperate locally to detect the named events. When a sensor detects a named event, it determines the

storage sensor responsible for that name, and then stores the data at that sensor by taking a hash of the name, and mapping that hash onto a sensor in the network [10-15]. When a user wishes to query about an event, he can send the query only to the sensor responsible for that data. In this approach, queries are not needed to be flooded throughout the network and the data that the user does not ask is to be sent to the user [16-20]. An example of DCS network is shown in Figure 1.

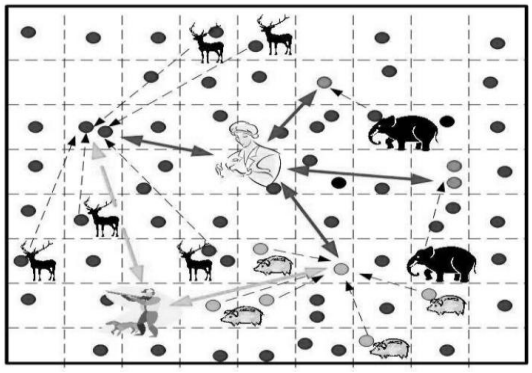


Figure 1 DCS Network for Habitual Monitoring

This DCS network however faces lot of security problems since same type of data are stored at same nodes using a publicly known mapping relation. Once this mapping relation between the nodes is known to the attacker, the nodes can be easily compromised [21-25]. In addition, an attacker can simply send a query to the nodes and easily read all data stored in it. Hence the aim of this paper is to implement secured mapping schemes, efficient key management techniques to protect against the mapping attack and improve the data confidentiality and authentication. Further to implement Keyed Bloom Filter (KBF) scheme and Hashed Message Authentication Code (HMAC) to defend against query attack and to improvise data authentication [26-30].

The salient features of this work are (i) Data location mapping is done based on cryptographic keys instead of publicly known mapping function (ii) Assignment and updating of keys are done to prevent attackers from obtaining the locations of storage cells for the previous sensor data. (iii) Seamless mapping between location keys and logical keys are obtained by updating compromised keys using efficient key management schemes [31-36]. This paper is organized as follows: Section II deals with different secured location mapping schemes, Section III. deals with key management schemes, Section IV discusses about the keyed bloom filter scheme for source authentication and query optimization, Section V discusses the forwarding HMAC for data authentication and finally the conclusion.

2. Secured Mapping Schemes

Data centric sensor networks have security threats like eavesdropping or injecting of faulty information by attackers, Node compromise or node capture. These threats are due to insecure radio links, lack of tamper resistant and their unattended nature. Generally the security attacks on the DCS network are classified as follows,

Passive Attack: Eavesdropping of message transmissions by an attacker. The solution to this is encryption of message with keys of sufficient length.

Query Attack: Passing a query into the network by an attacker to obtain the sensor data of his interest. The solution for this is source authentication.

Readout Attack: Sensor nodes are captured and data are read directly by the attacker.

Mapping Attack: The attacker try to know about the mapping relation between the detector and storage nodes is called mapping attack.

We divide our DCS network into a grid of detector cells and storage cells. The detector cells are used to sense the data from the surrounding environment and to pass them to the storage cells where they are stored Each Cell is identified by a unique ID and each sensor is aware of its own Cell ID. Pair of

nodes from neighboring cells can directly communicate with each other. Trusted Mobile Sink enters the network and controls data collection and key management. The authorized mobile sink is assumed to haves the ability to broadcast messages and each node in the network can verify that. Also the cell is assumed to be compromised if at least one node in the cell is compromised. Once a node is compromised means all the keys possessed by it are obtained by the attacker.

The sensor data is handled in the following manner. The detector cell (p) determines the storage cell (q) using keyed hash function, encrypts the data with cell key, forwards data to storage cell 'q' where it is stored. An authorized MS sends a query to 'q' and decrypts the collected data. If an attacker comes to know the mapping relation between the storage cell and detector cell (p & q), he can launch various attacks. But without knowing the mapping key, he cannot get the mapping relation between them. Since storage cell does not possess decryption key and MS only does the decryption, the readout attack is made difficult even though a node in storage cell p is compromised. Hence the main aim of the design is to secure the mapping function to prevent mapping attack. Necessary requirements for addressing mapping and readout attacks are defined as follows:

1. Event data Privacy. Even after an attacker compromised a sensor node and obtained all its keys, he must be prevented from knowing the event data stored in the compromised node.
2. Backward and Forward event privacy. An attacker should be prevented from obtaining the previous as well as future sensor data for an event of his interest even if he has compromised some nodes.
3. Query privacy. An MS query should not reveal any information about the location of the sensor data.
4. Network wide flooding and public key operations should be avoided

We discuss about three types of secure mapping schemes in the order of increasing privacy and before that the following general assumptions are made,

- N -- Number of cells
- Nr -- Number of cells in row
- Nc -- Number of cells in a column
- Every cell is uniquely identified by L (i, j) where $0 \leq i \leq Nr-1$ and $0 \leq j \leq Nc-1$
- 'm' independent detection cells for event E are identically distributed over N cells
- Attacker is capable of compromising's' cells.
- Event privacy level (EPL): Probability that an attacker cannot obtain both sensor data and encryption key for an event of his interest
- Larger the EPL, higher the privacy

Scheme I: Group Key Based Mapping

In this scheme, based on a group wide shared key, all nodes store same event E in location (Lr, Lc)

Lr = H (0|K|E) mod (Nr)
Lc = H (1|K|E) mod (Nc)

A cell should not store its own data to avoid stand alone readout attack. MS can send a query in the form what is information about event E? MS determines the location of the storage node based on group key K and event E. All m detection cells are mapped to one storage location. An Attacker can randomly compromise a node to get group key and locate storage cell based on group key. Since the data stored is encrypted using individual cell key, the attacker has to first get cell-ID randomly from m detection cells. Assume attacker compromise up to s cells and if the first compromised cell is storage cell with probability (1/N) then the attacker will randomly compromise (s-1) cells from (N-1) cells. If first compromised cell is not a storage cell with probability (N-1)/N then he compromise storage cell first and randomly compromise (s-2) cells from remaining (N-2) cells. Assume the attacker compromised i out of m detection cells then. The Backward Event Privacy Level (BEPL) of this scheme is given by

$$P_b^1(m,s) = 1 - \frac{1}{N}\sum_{i=1}^{B_1} \frac{\binom{i}{m}\binom{N-1-m}{s-1-i}\binom{m}{i}}{\binom{N-1}{s-1}} - \frac{N-1}{N}\sum_{i=1}^{B_2} \frac{\binom{i}{m}\binom{N-2-m}{s-2-m}\binom{m}{i}}{\binom{N-2}{s-2}}$$

and also the Forward Event Privacy Level (FEPL) is given bye is

$$P_f^1(m,s) = 1 - \frac{\binom{ms}{N}}{m} = 1 - \frac{s}{N}$$

Scheme II: Time Based Mapping

Node stores event E occurring in same time interval T into the same location (Lr, Lc) using group wide shared key Kt

Lr = H (0|KT|E|T) mod (Nr)
Lc = H (1|KT|E|T) mod (Nc)

Every sensor node maintains timer which periodically at T interval derives next group key Kt as function of H(Kt). An MS can raise a type of query "what event E at timer interval T?". MS determines location of storage cell based on Kt, E and T. Attacker cannot get old group key from current group key of captured node because of the one way hash function. Hence it is difficult to find out the previous data storage locations. BEPL p_b^2 (m, s) for this scheme is higher than scheme I and is given by

$$P_b^2(m,s) = 1 - \left(\frac{s}{N}\right)\left(\frac{s}{N}\right) = 1 - \left(\frac{s}{N}\right)^2$$

Since storage cells vary over time T for same Event E, FEPL is same as BEPL

Scheme III: Cell Based Mapping

All nodes of same cell L (i, j) store in the same location (Lr, Lc) the same type of event E at time T.

Lr = H (0|i|j|E|Kij|T) mod (Nr)
Lc = H (1|i|j|E|Kij|T) mod (Nc)

A Cell key Kij is shared among all nodes in cell L (i, j). Kij is updated periodically such that Kij = H(kij) and erases old keys for backward privacy Since cell key is used for encryption, data is encrypted using different keys over period of time. MS can raise a query in the form "has event E happened in cell L (i, j) at time T". Attacker cannot get old cell keys from new keys and hence offers highest BEPL (p=1) and FEPL is same as scheme II.

3. Comparison among Different Mapping Schemes

After simulation in NS2 with N=100 and with different values of m and s, BEPL is plotted and shown in Figure 2. The results show that BEPL increases with increasing m and decreased with increasing.

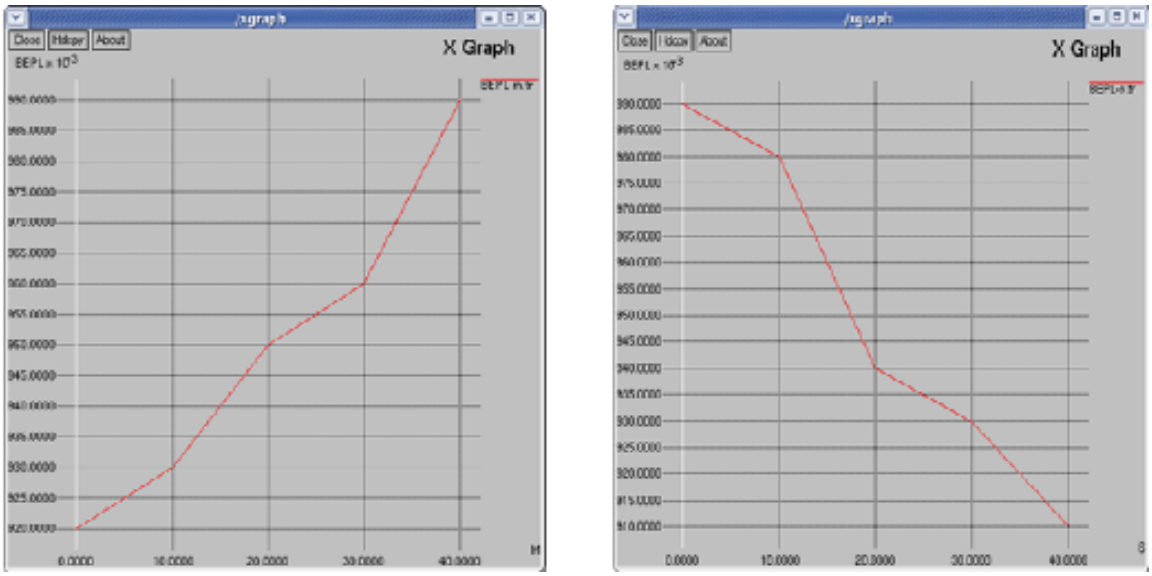


Figure 2 Backward Event Privacy Level Vs m and s

Keeping the Overall memory requirement to store sensed data to be same in all 3 schemes the Message overhead which is the total number of hops of all the messages from detector to storage cells for different mapping schemes is plotted as in Figure 3. It shows that the message overhead linearly increases with number of events. Cell based scheme has slightly more overhead

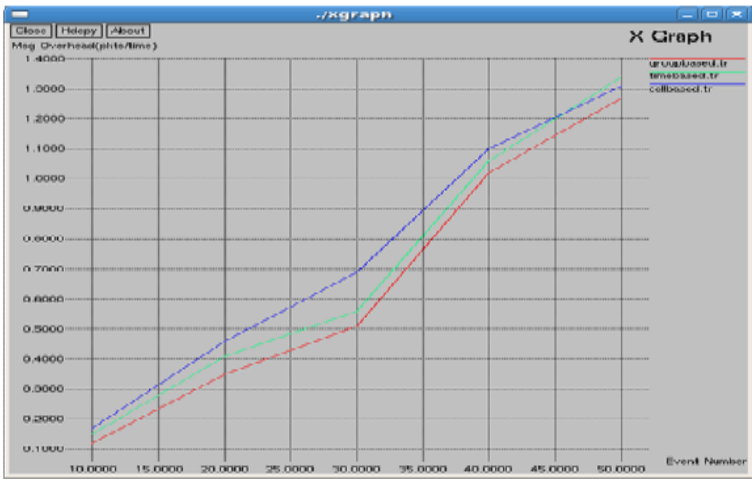


Figure 3 Overhead Comparison of Mapping Schemes

4. Efficient Key Management

4.1 Keys Generated

The list of keys generated for our data centric sensor networks to achieve data confidentiality and their efficient management schemes to achieve improved authentication are given below:

Master Key: Every node u has a master key Kp shared only with MS. It is necessary to secure the communications between the MS and individual sensors. For example, if any node wants to report about the malfunction of another node to MS, it may use the this key to calculate a message authentication code over the report, or when MS distributes a new cell key to a cell with a node to be revoked, the master keys of other nodes can be used to encrypt the new cell key for secure key distribution.

Pairwise Key: Neighboring nodes in the network share a pairwise key which is used for secure distribution of keys, and to provide authentication between neighboring cells or between MS.

Cell Key: A cell key is generated for each cell for encrypting sensed data to be stored in a storage cell and to achieve cell-to-cell mapping.

Row Key: A row key is generated to private mapping between a row to cell or delivering group key among cells in a secured manner.

Group Key: A group key is generated for secure group to-cell mapping or when MS sends a secure query or instruction to all the nodes.

4.2 Keys Organisation

All Keys except pair wise keys are organized into a Logical Key Tree (LKH) with the hierarchy as shown in Figure 4. The root of the tree is group key, followed by row key (column key) and cell key. Here the group members share pair wise keys which reduce the bandwidth overhead of group re-keying when a node is revoked in a group

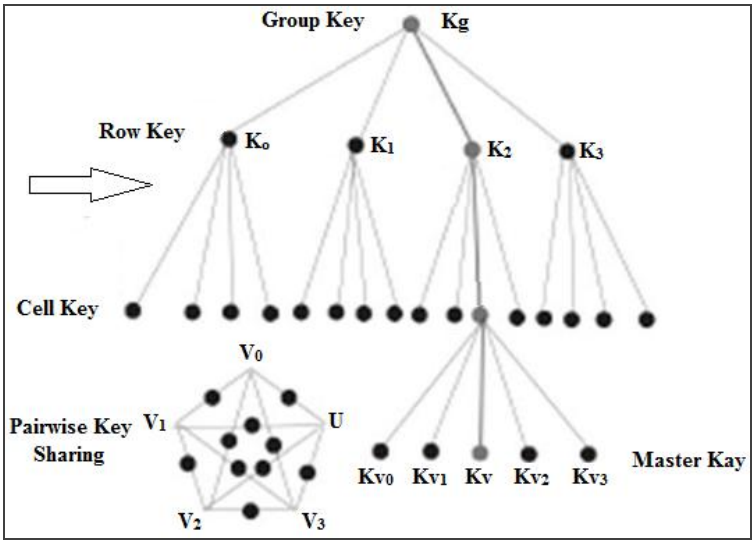


Figure 4 Logical Key Tree

4.3 Key Assignment

Pairwise keys are established using existing schemes by trusted base station, Group keys and Master keys are pre-loaded prior to deployment of the network. But Row and Cell keys are established after deployment. We assume that during the initial key assignment, a node will not be compromised before it finds its location. Every node is first loaded with same network key Ki for computing the cell key using the function H(Ki,i|j) based on cell location (i, j) and after this Ki to be erased. Similarly row key is also computed using H (ki, i)

4.4 Key Updates on Node Revocation

If a node u in cell L (2, 2) is compromised, all other nodes in the cell report this to MS. Nodes use master key to compute MAC. Since node u compromise keys k_{22}, k_2 and kg these keys are updated to new. The new group key K_g is encrypted by K_0, K_1, K_2 and K_3. K_2 is encrypted by K_{20}, K_{21}, K_{22} and K_{23}. K_{22} is encrypted by Kv_0, Kv_1, Kv_2 and Kv_3. Based on LKH, MS will encrypt each key with its child keys (new keys if updated) and broadcast. In general Nr + Nc + Nij-1 encrypted keys will be broadcast to the network.

Performance Analysis: We define performance overhead C as the average number of keys that traverse each cell during a rekeying event

$$C = \sum_{i=0}^{N_r-1} \sum_{j=0}^{N_c-1} \frac{sij}{(N_r N_c)}$$

Where sij is number keys traversed cell L(i,j). Assume a sensor network of square field with hundred nodes then Nr= Nc and hence C=2.5 better than Nr+Nj+Nij-1 keys to be broadcasted.

4.5 Improvement to Rekeying

When a new encrypted key is to be communicated, send it to only one in the group and allow the recipient to propagate to others using pair wise keys. But this increases communication If a node u in cell L(i,j) is revoked then

- For nodes in row r{r≠i) they only need new group key Kg' encrypted by its row key Kr. MS sends only one encrypted key to cell (r,0). Keys are propagated to other cells in row r.
- For nodes in row i, if nodes in column (n ≠ j) they only need new group key Kg' encrypted by Ki' and Ki' encrypted with cell key Kin. If nodes are located in same cell as node u then each need to receive Kij' encrypted with its own mater key.
- MS sends Nc+Nij-1 keys to cell (i,0) and keys are propagated in row i.

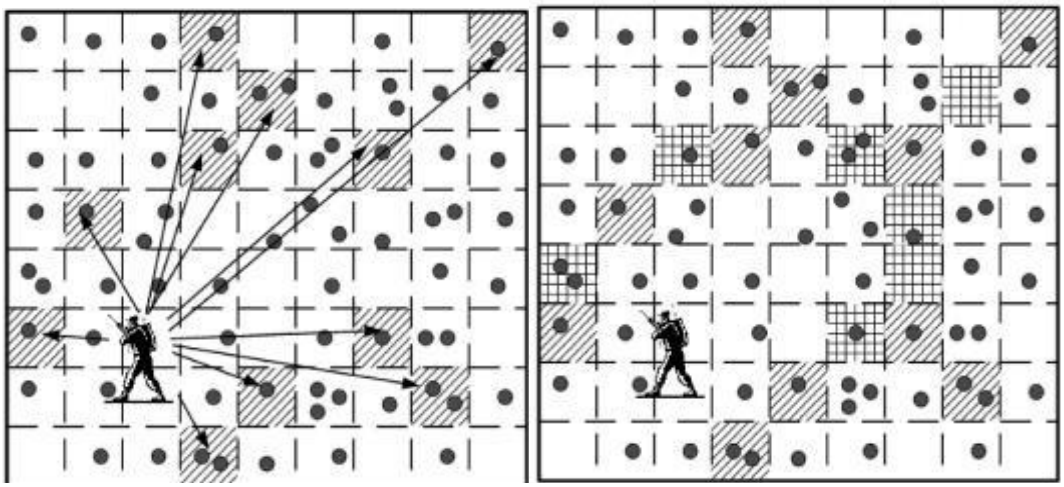
5. Keyed Bloom Filter Scheme

An attacker can easily send a query to read the data of his interest from the network. Source authentication is the solution for the query attack. That is the storage cell should verify that the query arises from the authenticated mobile sink. To achieve this and improvising query process, we consider the bloom filter scheme. Before that we discuss about the basic query process.

Basic Scheme of Querying: MS sends one query message to each cell using routing protocol like GPRS. Each message contains query and storage cell ID. This type of query gives high message overhead as well the query privacy is measured as probability that attacker cannot get storage cell ID. For this scheme since cell ID is part of message the probability of privacy is P1=0. The process is illustrated in Figure 5a.

Keyed Bloom Filter Scheme: Bloom filter is data structure used for membership queries. It represents a set $S=s_1,s_2,..,s_n$ using k independent hash functions $h_1,h_2,..,h_k$ and string of m bits each set to 0 initially. For each s subset of S, all k hash functions are hashed to obtain hi(s) (1<=i<=k). The bits corresponding to this value are set to 1 in the string. Multiple hash values may map to same bit yielding false positive i.e. an element not in S but its bits hi(s) are marked by elements in S.

An attacker could still easily check if the cell ID is that of storage cells though there are high false positive rates In KBF. Cell key is used to encrypt cell ID .Encrypted Cell ID is then concatenated with cell key of its parent in Euclidean Steiner Tree (EST) before inserting into Bloom Filter based query message. Thus the attacker has a very small chance to derive cell ids from this BF. When a query message arrives at a cell, the cell concatenates its own cell key with the ID of each neighboring cell that is not a neighbor of its own parent node, and determines whether the neighbor is in the Bloom Filter. But it cannot verify membership of other cells. Then the storage node forwards message only if it is in BF. The KBF scheme is illustrated in Figure 5b. It offers much better query privacy compared to other schemes.

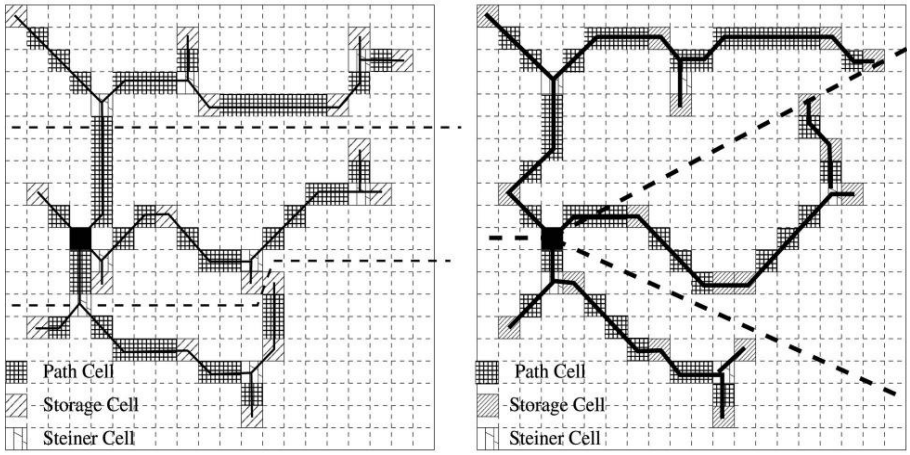


(a)Basic Scheme (b) KBF Scheme

Figure 5 Keyed Bloom Filter Scheme

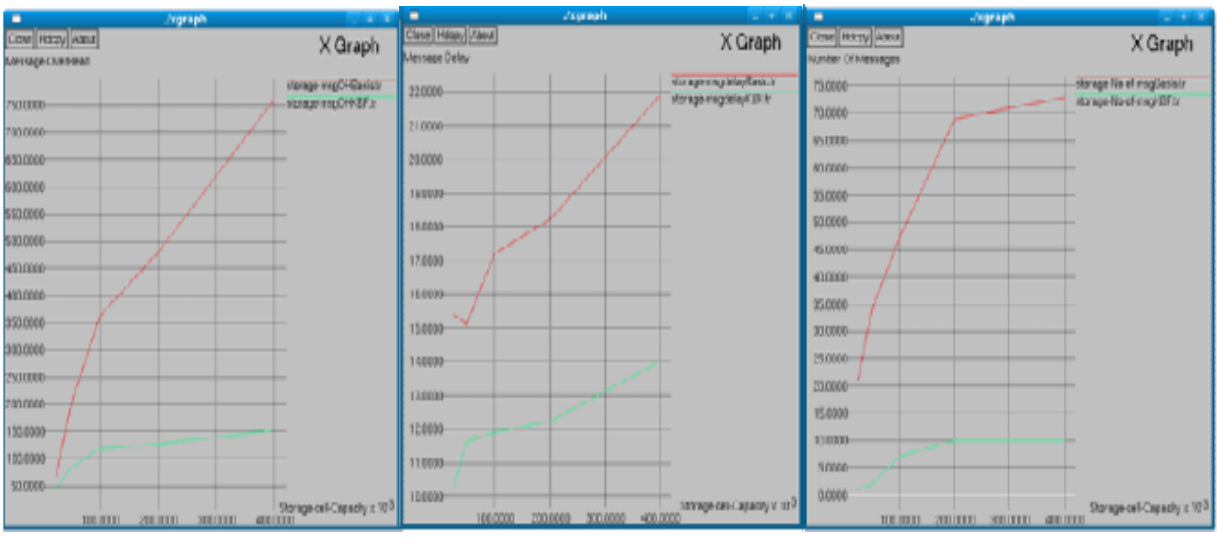
But this scheme increases the size of the messaged. Since the storage capacity of sensors are limited, the number of cell ids included in the query message to be limited. To achieve this scheme the area of sending a query to be reduced. Hence instead of using plane partition of the network, different partition method called fanlike partition may be adopted. Scheme has the same partitions and builds the same sub-EST trees. Here the Cartesian coordinates are changed to polar coordinates. In this partition the storage cells are within the area [–π, π]. The partition algorithm scans the plane from _π to π and collects enough storage cells into each partition. Figure 6 shows the example of dividing the plane into three partitions using the Fanlike partition method. After the partition the MS sends a query to each partition at the same time. In this way, the message size can be reduced. Further, since multiple queries are sent out at the same time, the average query delay is also reduced.

Performance and Analysis: The performance against message overhead, query delay and number of messages used after implementing KBF scheme with fanlike partition is compared with basic scheme of querying. We observe better results and they are shown in Figure 7.



(a) Plane partition (b) Fanlike partition

Figure 6 Storage Cells are partitioned into Three Parts



(a) Message Overhead (b) Message delay (c) No. of messages

Figure7 Performance Comparisons between KBF with Fanlike Partition and Basic Scheme of Querying

6. Data Authentication using HMAC

When an event occurs in the sensing area, the detector cell p will first detect this event and will create a report. Before this sensor sending the report to storage node or to sink, our approach requires each report includes up to m MACs attached. To collect those MACs, the reporting node p broadcasts a message to all its neighbors. Here we employ Hashed Message Authentication Code to improve the

data authentication between neighboring cells. The pairwise key shared between the neighboring cells are first hashed and then included in the MAC message. This will be then forwarded to neighboring nodes or to mobile sink. The implementation of HMAC SHA-1 in our simulation brought better results in data authentication and better performance. The performance analysis after HMAC implementation is shown in Figure 8.

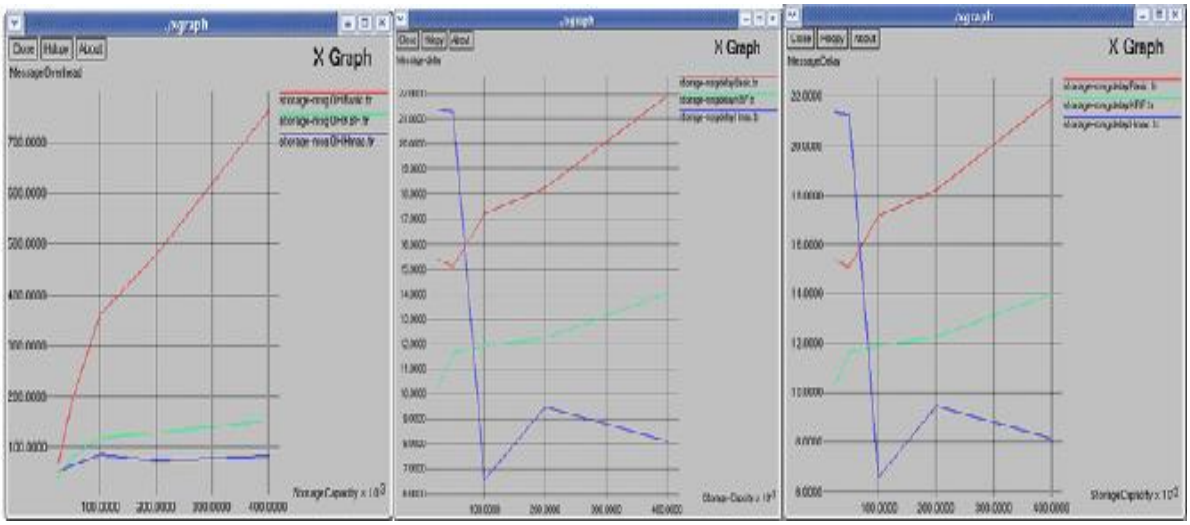


Figure 8 Performance Comparisons with HMAC

7. Conclusion

A security scheme for data centric wireless sensor networks that combines different mapping schemes to avoid mapping attack was presented. Efficient key management system for improved data confidentiality and keyed bloom filter scheme with fanlike portion of the network to improve source authentication and query optimization. HMAC is also implemented to achieve better data authentication. We achieved reduced message overhead and message transmission delay and improved privacy level. But for lower values of storage capacity, number of messages to be handled is more compared to higher values of storage capacity.

8. References

[1]. H. Lee, K. Shin and D.H. Lee, "PACPs: practical access control protocols for wireless sensor networks", Consumer Electronics, IEEE Transactions, 58(2), 2012, 491-499

[2]. D. Sobya, S.K. Muruganandham, S. Nallusamy and P.S. Chakraborty, "Wireless ECG monitoring system using IoT based signal conditioning module for real time signal acquisition", Indian Journal of Public Health Research and Development, 9(2), 2018, 296-301

[3]. S.K. Muruganandham, D. Sobya, S. Nallusamy, Dulal Krishna Mandal and P.S. Chakraborty, "Study on leaf segmentation using k-means and k-medoid clustering algorithm for identification of disease", Indian Journal of Public Health Research and Development, 9(2), 2018, 291-295

[4]. D. Sobya, SK. Muruganantham, S. Nallusamy and P.S. Chakraborty, "A proposed model for public distribution system through IOT", International Journal on Recent Researches in Science Engineering and Technology, 6(2), 2018, 67-74

[5]. Debnath, Singaravelu and Verma, "Privacy in wireless sensor networks using ring signature", Journal of King Saud University Computer and Information Sciences, 26(2), 2014, 228-236

[6]. D. Sobya, "Discrete wavelet transform for image compression and reconstruction via VLSI", International Research Journal in Advanced Engineering and Technology, 1(1), 2015, 31-35

[7]. SK. Muruganantham, D. Sobya, S. Nallusamy, Dulal Krishna Mandal and P.S. Chakraborty, "Development of policy based security application to enhance the security of software defined network", International Journal on Recent Researches in Science Engineering and Technology, 6(2), 2018, 58-66

[8]. D. Sobya, SK. Muruganantham, S. Nallusamy and P.S. Chakraborty, "A proposed model for smart farming in rural areas using IoT advanced technologies", International Journal on Recent Researches in Science Engineering and Technology, 6(1), 2018, 61-67
[9]. P. Zeng, K.K.R. Choo and D.Z. Sun, "On the security of an enhanced novel access control protocol for wireless sensor networks", Consumer Electronics, IEEE Transactions, 56(2), 2010, 566-569
[10]. D. Sobya, SK. Muruganantham, S. Nallusamy, Dulal Krishna Mandal and P.S. Chakraborty, "Study on mobile adhoc networks routing protocols to enhance the end-user experience", International Journal on Recent Researches in Science Engineering and Technology, 6(1), 2018, 54-60
[11]. S. Nallusamy and Gautam Majumdar, "Enhancement of overall equipment effectiveness using total productive maintenance in a manufacturing industry", International Journal of Performability Engineering, 13(2), 2017, 01-16
[12]. D. Sobya, S.K. Muruganandham, S. Nallusamy and Partha Sarathi Chakraborty, "Optimization of bit error and data transmission rate for different modulation scheme using MIMO diversity technique", International Journal on Recent Researches in Science Engineering and Technology, 5(8), 2017, 06-13
[13]. S. Sicari, L.A. Grieco, G. Boggia and A. Coen Porisini, "DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks", Journal of Systems and Software, 85(1), 2012, 152-166
[14]. D. Sobya, S. Nallusamy, Partha Sarathi Chakraborty and S.K. Muruganandham, "Design of multi functional electronic energy meter enabled with zigbee protocol intended for industrial applications", International Journal of Current Advanced Research, 6(10), 2017, 7029-7033
[15]. S. Nallusamy, R. Balaji and S. Sundar, "Proposed model for inventory review policy through ABC analysis in an automotive manufacturing industry", International Journal of Engineering Research in Africa, 29, 2017, 165-174
[16]. Y. Yao, J. Liu and N.N. Xiong, "Privacy preserving data aggregation in two-tiered wireless sensor networks with mobile nodes", Sensors, 14(11), 2014, 174-194
[17]. D. Sobya, S K. Muruganandham, S. Nallusamy and Partha Sarathi Chakraborty, "Development of bluetooth based smart meter reading system for residential power monitoring," International Journal on Recent Researches in Science Engineering and Technology, 5(12), 2017, 39-47
[18]. S K. Muruganandham, D. Sobya, S. Nallusamy, P.S. Chakraborty and D K Mandal, "Development of framework to enhance the lifetime of wireless network in mobile power sharing networks," International Journal on Recent Researches in Science Engineering and Technology, 5(12), 2017, 28-38
[19]. X. Liu, "A survey on clustering routing protocols in wireless sensor networks", Sensors, 12(8), 2012, 113-153
[20]. S. Nallusamy, G.B. Dinagaraj, K. Balakannan and S. Satheesh, "Sustainable green lean manufacturing practices in small scale industries-A case study", International Journal of Applied Engineering Research, 10(62), 2015, 143-146
[21]. D. Sobya, S. Nallusamy and Partha Sarathi Chakraborty, "A proposed remote monitoring system by global system for mobile communication and internet technology," International Journal on Recent Researches in Science Engineering and Technology, 5(11), 2017, 07-14
[22]. Ismail Mansour, Gerard Chalhoub and Pascal Lafourcade, "Key management in wireless sensor networks", Journal of Sensor and Actuator Networks, 4, 2015, 251-273
[23]. D. Sobya, Partha Sarathi Chakraborty and Dulal Krishna Mandal, "Design and development of IoT based residential automation security system with bluetooth technology", International Journal of Application or Innovation in Engineering & Management, 6(6), 2017, 62-72
[24]. J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy", Journal of Network and Computer Applications, 33, 2010, 63-75
[25]. D. Sobya, Arvind Kumar and Vicky Kumar, "Smart IoT based energy monitoring and controlling household appliances", International Innovative Research Journal of Engineering and Technology, 2, 2017, 94-97

[26]. I. Mansour, G. Chalhoub and P. Lafourcade, "Evaluation of secure multi-hop node authentication and key establishment mechanisms for wireless sensor networks", Journal of Sensor and Actuator Networks, 3, 2014, 224-244
[27]. D. Sobya, R. Varshni and P. Albinia, "MEMS based hand gesture wheel chair movement control with emergency alert", International Innovative Research Journal of Engineering and Technology, 2, 2017, 90-93
[28]. S. Chattopadhyay and A.K. Turuk, "A Scheme for key revocation in wireless sensor networks", International Journal of Advanced Computer Engineering and Communication Technology, 1, 2012, 16-20
[29]. D. Sobya, "Data compression analysis of rocket engines with vector quantization based on FCM algorithm", Int. Journal of Engineering Research in Africa, 22, 2016, 135-140
[30]. P. Chuang, S. Chang and C.A. Lin, "Node revocation scheme using public key cryptography in wireless sensor networks". Journal of Information Science and Engineering, 26, 2010, 1859-1873
[31]. D. Sobya, "Lab view based multi-input fuzzy logic controller of DC motor speed control", International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(1), 2015, 55-60
[32]. M. Saravanakumar, D. Sobya and B. Sathis kumar "Design and development of new technique for testing of field programmable gate arrays", International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(4), 2016, 139-147
[33]. K. Balakannan, S. Nallusamy, P.S. Chakraborty and Gautam Majumdar, "Selection and evaluation of supplier by decision model of hybrid data envelopment analysis", International Journal of Applied Engineering Research, 10(62), 2015, 123-127
[34]. S. Nallusamy, Sri Lakshmana Kumar, K.Balakannan and P.S.Chakraborty, "MCDM tools application for selection of suppliers in manufacturing industries using AHP, Fuzzy Logic and ANN", International Journal of Engineering Research in Africa, 19, 2015, 130-137
[35]. D. Sobya, "Design and implementation of FPGA based wave-pipelining for digital signal processing circuits", International Research Journal in Advanced Engineering and Technology, 1(2), 2015, 36-42
[36]. G.N. Purohit and Rawat, A.S., "Revocation and self-healing of keys in hierarchical wireless sensor network", International Journal of Computer Science and Information Technology, 2, 2011, 2909-2914