NATIONAL CONFERENCE ON ICT EMPOWERED TEACHING, LEARNING AND EVALUATION (NCICT-2016)

International Journal of Advanced Scientific Technologies in Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) *Volume.2,Special Issue.1Dec.2016*

A reliable and efficient data aggregation technique for privacy preserving in Wireless Sensor Networks based on Hilbert curves

A.L. Sreenivasulu
Associate Professor, ***GATES Institute of Technology, Gooty, Ananthapuramu (Dt)***
E-mail: akula5461@gmail.com

Abstract— In recent years a lot of research has undergone in Wireless sensor networks based on Data aggregation in order to protect the privacy and integrity. There exists a number of Data aggregation techniques for privacy-preserving such as GP2S,SMART,CPDA.However these techniques still suffer from drawbacks, first the communication cost incurred in designing the network topology is high and a so they doesn't uphold data integrity .In this paper a reliable and efficient Data aggregation technique for privacy-preserving has been proposed based on Hilbert curves .In order to minimize the communication cost a tree based topology is used for network construction and for calculating the intermediate Data aggregation. In order to preserve the data privacy a two-fold technique of seed-exchange algorithm and Hilbert-curve data encryption is used. Finally based on simulation results our technique provides better privacy-preserving than existing schemes.

Index Terms— Wireless sensor networks, Data aggregation, Hilbert-curve

I. Introduction

With the proliferation of advanced technologies in mobile devices, wireless sensor networks have drawn increasingly interest from both industry and research institutes [1-3]The Wireless Sensor Network (WSN) is a highly distributed wireless networks consisting of small, lightweight wireless nodes which has got the capability of sensing the human world such as temperature, pressure, sound, vibration and speed etc.WSN plays an important role in military applications and civilian applications.

Mounting efficient in-network data aggregation, while preserving privacy of a sensor node is a challenging problem in WSN. Many such techniques have been proposed such as CPDA, SMART, twin-key based method and GP2S but they suffer from communication cost and energy constraints. So a novel technique for privacy-preserving has been proposed to provide maximum security. It is therefore necessary to design an effective Data aggregation scheme for recent applications of wireless sensor networks such as military applications and environmental monitoring for data privacy and integrity of sensed data.

In this paper, we first propose a seed-exchange algorithm and the seed generated by this algorithm is used to conceal the sensed data for privacy-preserving and we also use Hilbert -curve scheme for data privacy-preservation, with this approach it is not possible for the intruder to retrieve the actual sensed data because the sensed data can only be altered by a unique Hilbert value.

The rest of this paper is organized as follows Section II proposes an reliable and efficient data aggregation scheme for privacy-preservation and Section III provides the performance analysis , Section IV illustrates result analysis of the current system and Section V concludes the paper.

II. DATA AGGREGATION TECHNIQUE TO IMPOSE DATA PRIVACY

In this section we present a Privacy-preserving Data aggregation scheme which uses seed value and Hilbert curve value for privacy preservation. By applying seed-exchange algorithm the total number of messages are minimized during Data aggregation and thereby reducing communication overhead and a Hilbert curve algorithm is used to changed seed value which is encrypted by a unique Hilbert value and difficult for intruder to overhear it.

There are three phases of Privacy-preserving Data aggregation scheme

1 Network build phase,
2 Data encryption phase
3 Data transfer phase.

1. Network build phase: In this phase a tree based topology is used to perform aggregations on the intermediate data. Each node discover its parent node, Sibling nodes and child node. First a sink node sends a HELLO message to all its Sibling nodes based on message flooding algorithm as shown in Fig-1. After receiving the HELLO message each node checks whether the HELLO message is from sink node or not by checking its communication range. If the sink node is located within its communication range then sensor node sets the sink node as parent node by broadcasting a JOIN message. Otherwise it wait for some time until it get a HELLO message from sibling nodes and then chooses one of the sibling node as parent node by transmitting a JOIN message .The sink node transmits the HELLO messages to all its sibling nodes at different level as depicted in Fig 2

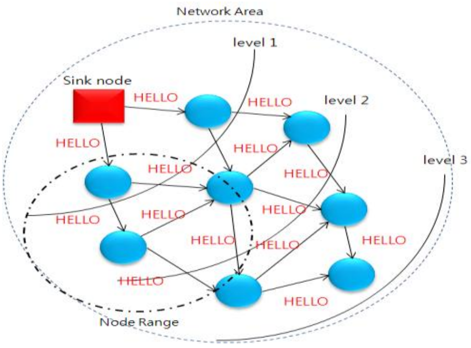


Fig-1 : Message Flooding

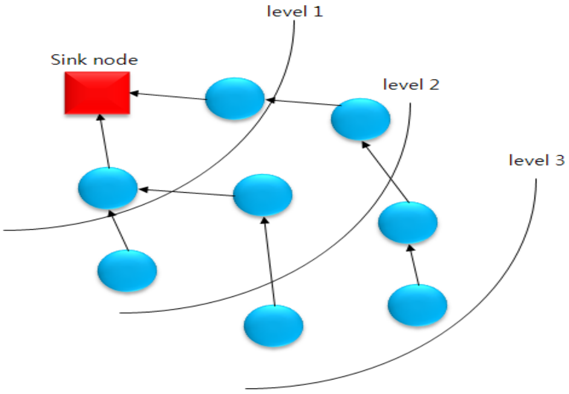


Fig-2 Network construction

In the above phase, initially we must have to decide the maximum number of child nodes so that to reduce the impact of network imbalance. If there is a network imbalance the sensor nodes in that imbalanced area consumes more energy than other areas. The maximum number of child nodes in the above phase is calculated by using the equation

MIN(# of neighbors $[(1+\alpha) \times (1+ER)^2 \times \Pi(CR)^2/NA \times$ # of nodes])

Where

ER = Error Rate (average rate of message loss from as ink node)

α = Density of a sensor network

C = Maximum number of child nodes

CR = Communication range(Communication boundary that can be reachable from a sensor node)

NA = Network Area(Size of the network)

2. Data encryption phase: Upon successful construction of sensor network, each sensor node calculates a seed data for seed exchange algorithm. In order to perform the above the seed exchange we use an elliptic-curve key exchange algorithm which use an public-elliptic curve, arbitrary point and a secret constant key for the exchange of its own seed data.Fig-3 illustrates the flow-diagram of elliptic-curve key exchange algorithm. First, both the source node and destination node initially assign a constant private key , in this scenario pSend and pReceive are the contant private keys for the source and destination respectively. Second, each node calculates a value of R based on arbitrary point, constant private key and public-elliptic curve. Third, each node sends the calculated value of R to the destination node and finally each node calculates seed data seed_S and seed_R by multiplying R with constant private key. The calculated seed data is the sum of x and y coordinates because the elliptic curve is an two-dimensional equation. Since elliptic-curve key exchange algorithm permits the communication between the nodes without any unnecessary messages The sensor data of its own can be protected from an intruder.

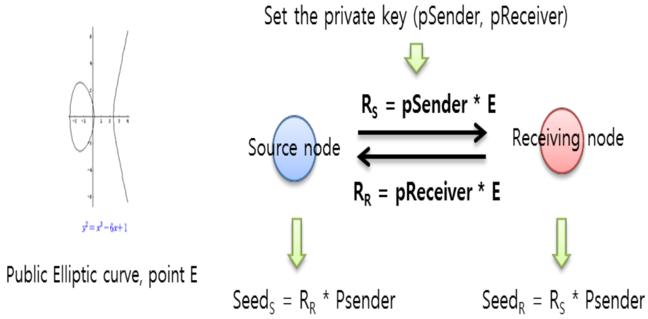
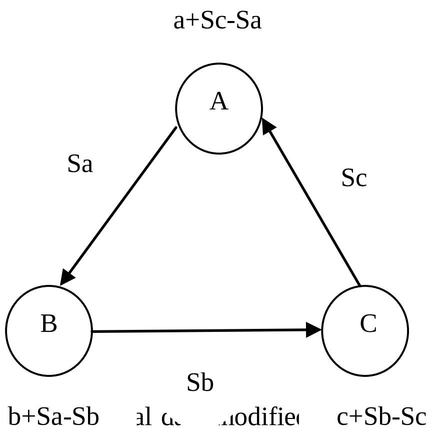

Set the private key (pSender, pReceiver)
R_S = pSender * E
Source node
Receiving node
R_R = pReceiver * E
Public Elliptic curve, point E
$\text{Seed}_S = R_R$ * Psender
$\text{Seed}_R = R_S$ * Psender

Fig-3 Flow diagram of elliptic-curve key exchange algorithm

The generated seed is used to hide original data from an attacker. The process involved in seed-exchange algorithm is as follows : The original data to be transmitted is modified by extracting a part of seed value, which is then transmitted to another nodes. As a result the sensed data can be hidden from other group members. If m is the number of seeds received from another nodes in the sensor network. The following equation gives the final transmitted value from each node for data aggregation.

Final value = original value- seed value + ∑ received seed(i)

Fig-4 shows the result of sensed data encryption of each node after exchanging a seed.



al d modifie ange from three nodes.

For processing a user query, a parent node performs the aggregation on the modified data and all the received from its child nodes. Based on the Hilbert curve technique the parent node transmutes the aggregated result into a two-dimensional encrypted data. The Hilbert curve proposed by peano is a continuous fractional space filling curve that transforms between one dimension and two dimension spaces to preserve locality. To apply Hilbert curve to seed-exchange algorithm we assume that each node transmutes one-dimensional sensed data into an two-dimensional data. Here 1-Dimensional data refers to aggregated value after performing seed-exchange algorithm. The 2-Dimensional data refers to the coordinates of the aggregated value along the Hilbert curve in 2^n x2^n metrics. In Hilbert curve if l is the level and d is the direction, the result of aggregated data is encrypted by 2-Dimensional data (x,y) into a sequence of terms <key(d,l),x,y>.The process of encryption is as follows :

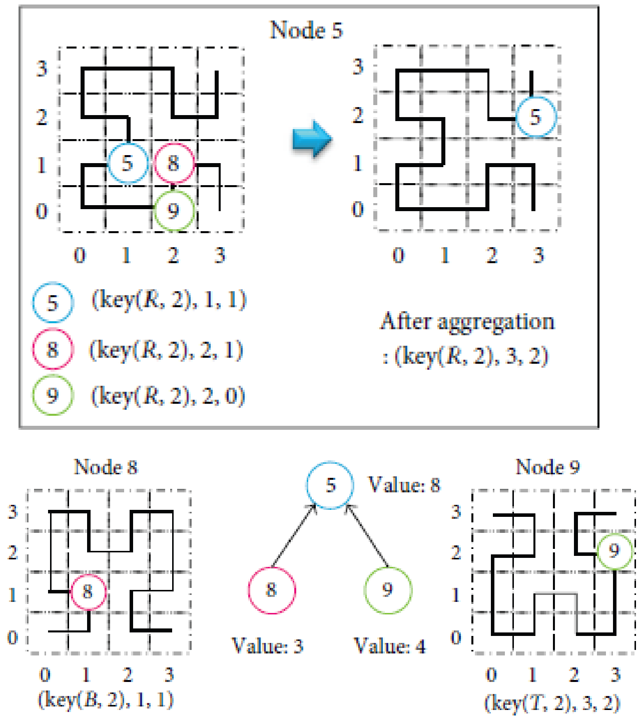


Fig-5 Example of data encryption

Fig-5 shows the example of data encryption for a given set of nodes 5,8,9 the child nodes 8 and 9 sends the encrypted data (key(B,2)1,1) and (key(T,2)3,2) to the parent node. By considering the level and direction of node 5 the encrypted received from child nodes are changed to (key(R,2)2,1) and (key(R,2)2,0) then node 5 performs aggregation on their data and sends the aggregated data to the parent node.

3.Data transmission phase : In this phase the parent node after receiving the encrypted data from its child node examines the data based on key, curve level and curve direction. If the curve level and curve direction of the child node are different from its own curve level and direction, the node should transmute the received sensed value based on curve level and direction. Hence the sink node performs the aggregation on all the encrypted data from the hierarchy nodes. Here we use Time Division Multiplexing Access method for transmission of data in order to avoid the communication loss in WSN.

III. Performance ANAYSIS

In this section we present simulation results of our new aggregation scheme with the existing Data aggregation schemes in terms of communication overhead, propagation delay and lifetime. In our experiment we make us eof TOSSIM simulator running on TinyOs and a GCC compiler and we use 100 sensor nodes randomly distributed in a dense are of 100x100 m with a transmitting power of 660 mW and receiving power of 395 mW. The environment setup for the above environment requires a CPU(inter Core2 Duo), Memory(2G),Language (nesC), Simulator(TOSSIM) and Compiler(GCC ver 4.0.3).

There are 3 types of sensor node distributions for the experiment such as Skewed, Random and Grid.

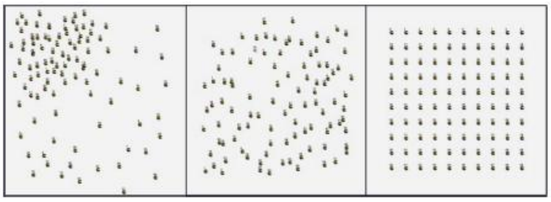


Fig-6 Three types of sensor node distributions

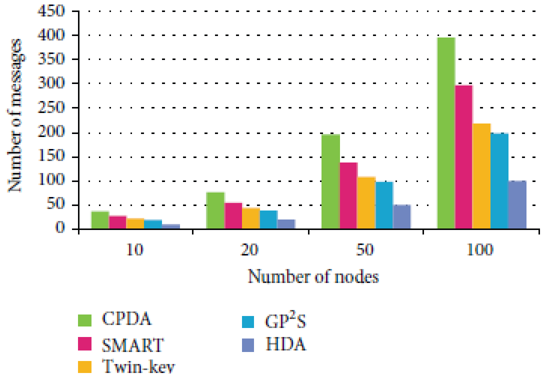


Fig-7 Transmission of messages with respect to varying number of nodes

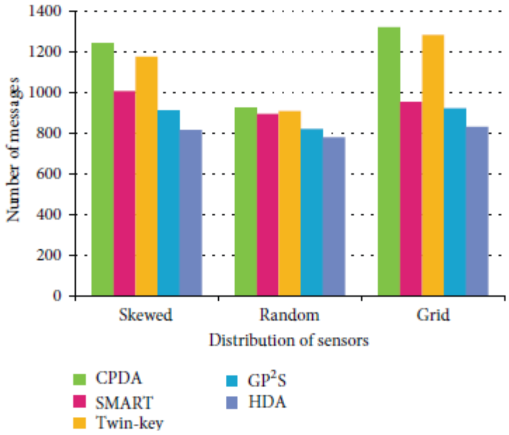


Fig-8 Transmission of messages with respect to distribution of sensor nodes

IV. Result analysis

In this Section we compare HDA(Hilbert Curve Data aggregation) with the existing schemes in terms of communication overhead and the average lifetime of the sensor node. Where the total number of sensor nodes ranges from 10 to 100 .Fig-7 depicts the communication overhead with respect to increasing number of sensor nodes. In the existing schema as the number of sensor nodes increases the transmission of messages also increases because in a huge network, each node has got the capability of sensing the data which in turn transmitted to the parent node. However our HDA schema need not generate unnecessary messages during data aggregation Since each sensor node ca transmute its own data whereas in existing schemas additional messages are required for privacy-preservation. Fig-8 depicts transmission of messages in terms of three distribution of sensor nodes.Fig-9 depicts the transmission of messages in term of communication boundary by considering the number f sensor nodes to 100.In both the above figures our HDA schema need not generate the unnecessary messages when compared to existing schemas. In general HDA, SMART and GP^{2}S present consistent performance irrespective of the type of distributions and communication range because they are less influenced by the location of sensor nodes pertaining to the use of tree topology where as CPDA and twin-key are strongly affected by the communication range and type of distributions because they use clustering technique.

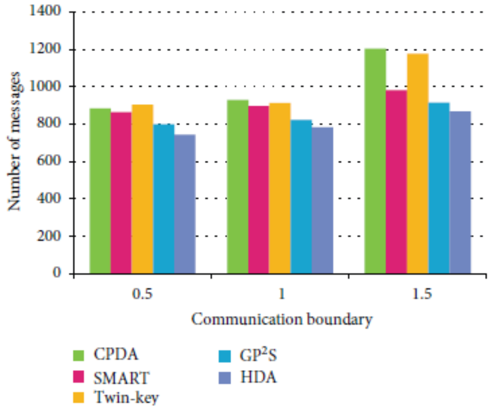


Fig-9 Transmission of messages with respect to communication boundary

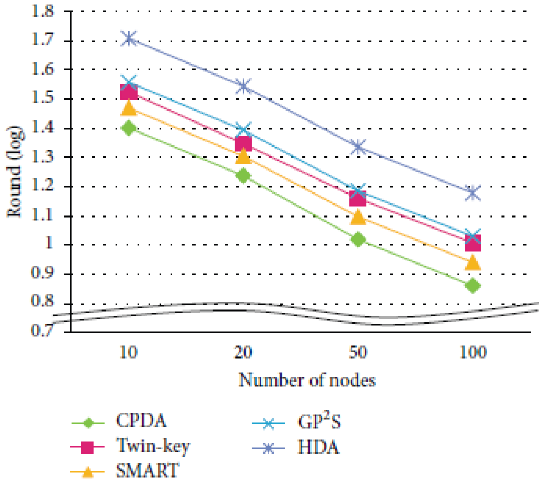


Fig-10 Average lifetime of sensor node with increasing number of sensor nodes

Fig-10 depicts the average lifetime of sensor network with increasing number of sensor nodes in WSN. Here we analyze the time as a measure of total number of sensor nodes whose energy is completely consumed with other nodes is greater than 50% of all sensor nodes. Therefore it is clear that the lifetime of all existing schemas decreases as number of sensor nodes increases because the total number of message generated is proportional to the number of messages required for Data aggregation. But the lifetime of HDA increases by 100-125% longer than those of all existing schemas.

V. CONCLUSION

This paper proposes a novel data aggregation technique for privacy preserving in WSN. This technique uses an seed- exchange algorithm to reduce the message overhead for privacy preserving in sensor networks. Based on the simulation our technique accomplish 100-300% longer network lifetime and 10% better participation rate when compared to the existing privacy preserving schemas.

REFERENCES

[1] “James reserve microclimate and video remote sensing,” 2008,http://www.cens.ucla.edu/.

[2] The firebug project,” 2008, http://firebg.sourceforge.net

[3] “Habitat monitoring on great duck island,” 2008, http://www.greatduckisland.net/.

[4] S. R. Madden, . M.R.Franklin, J.M.Hillerstein and W.Hong“TinyDB;an acquitional queryprocessing system for sensor networks,” ACM Transactions on Database Systems,vol. 30, no 1, pp. 122-173,2005

[5] K. Du, J. Wu, and D. Zhou, “Chain-based protocols for Data broadcasting and gathering in sensor networks,” in Proceedings of the International Parallel and Distributed Processing Symposium, April 2008

[6] Http://www.tinyos.net/tinyos-2.x/tos/lib/tossim/.

[7] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks,” Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM’07), pp. 2045-2053, Anchorage, Alaska, USA,May-2007.

[8] M. Acharya, J. Girao, and D Westhohh, “Secure Comparision of encrypted data in wireless sensor network”, Proceedings of the 3rd International Symposium on Modelling and Optimization in Mobile-Adhoc, and Wireless Networks (WIOPT),PP. 47-53, Washington, DC,USA, 2005.

[9] J. Girao, D. Westhoff , and M. Schneider, “ CDA : Concealed data aggregation for reverse multicast traffic in wireless sensor networks”, Proceedings of the 40th IEEE Conference on Communications