ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

Comparative Assay of the Overhead of Efficient Version of CPDA Protocol to Original CPDA Protocol

A.L.Sreenivasulu *, Dr.P.Chenna Reddy **
* Assistant Professor, Department of Computer Science & Engineering, IEC, Anantapur
** Professor, Department of Computer Science & Engineering, JNTUCEP, Pulivendula

Abstract— ***Data aggregation plays a vital role in Wireless sensor network which can be applied at aggregator nodes for effective bandwidth and energy. However in-network data aggregation presents a problem to the secrecy of sensor data because each individual sensor node data must be known to the aggregator before the aggregation process can be carried out. Providing efficient data aggregation while preserving data secrecy is a challenging problem in wireless sensor networks research. Therefore a number of Privacy-preserving data aggregation protocols have been proposed and one among them is CPDA [3] which is based on algebraic properties of polynomials. It suffers from vulnerable attack and is not energy efficient. A modified version of CPDA [2] has been proposed and it is more secure and energy efficient. In this paper, we present a brief comparative study of the overhead of modified version of CPDA to the existing privacy preserving CPDA version. Our study is based on two classifications of overheads in terms of communication and computation i) Overhead due to message transmission in the network ii) Computational overhead at the sensor node***

Keywords: **Wireless Sensor Network, Data Aggregation, Cluster-Based Private Data Aggregation (CPDA), Privacy.**

I. INTRODUCTION

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 and one among them is CPDA which has still drawbacks of security and energy constraints. So a new version of CPDA has been proposed to provide maximum security.

In this paper, we first compare the communication overhead of three protocols - TAG, CPDA and modified version of CPDA and show that modified CPDA provides less communication overhead compared to other protocols. Next we compare the computational overhead of the original CPDA to the modified CPDA and show that modified CPDA exhibits less computational overhead compare to the original CPDA.

The rest of this paper is organized as follows. Section II provides a brief discussion on communication overheads of original CPDA to modified CPDA protocol. Section III presents a computational overhead incurred in the original CPDA to the modified CPDA protocol. Section IV concludes the paper.

II. COMMUNICATION OVERHEAD

First we compare the communication overhead of three protocols – *the tiny aggregation protocol* (TAG), the original CPDA protocol and efficient version of CPDA protocol. In TAG each sensor node perforce to send 2 messages for the data aggregation protocol to travail. One HELLO message from each sensor node is communicated which require the formation of aggregation tree and one message for data aggregation. However this protocol performs only data aggregation and doesn't provide any security for the sensor node.

In original CPDA protocol, each cluster leader node transmits 4 messages and each cluster member node transmits 3 messages for assuring that the aggregation protocol works fine in privacy-preserving manner

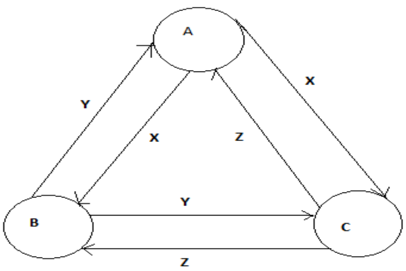

Fig. 1. Nodes *A*, *B* and *C* transmit their distinct and non-zero public value *x*, *y* and *z* respectively.

Consider the example cluster shown in Fig. 1.The cluster leader node A transmits 4 messages one HELLO message for the creation of cluster, one message for transmitting its public seed x, and one message transmitting v_B^A and v_C^A to cluster member nodes B and C respectively and one message for transmitting the aggregated result from the cluster. Similarly the 3 messages transmitted by cluster member node B are one message for transmitting its public seed y, one message for transmitting v_A^B and v_C^B to cluster leader node A and cluster member node C respectively and one message for transmitting the aggregate result F_B to the cluster leader node A.

In contrast to the original CPDA protocol, the modified version of CPDA protocol involves 3 message transmissions from cluster leader node and 2 message transmissions from each cluster member node. The 3 messages transmitted by

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

cluster leader node A are, One HELLO message from each sensor node is communicated which require the formation of aggregation tree and one message for transmitting its public seed x, and one message for transmitting the final aggregated result. It is worth noting that in this protocol the cluster leader node A need not transmit v_B^A and v_C^A to the cluster member node B and C respectively. Each cluster member node needs to transmit 2 messages. For example the cluster member node B needs to transmit its public seed y, and also needs to transmit v_A^B to the cluster leader node A. In the modified CPDA protocol the cluster member node B need not transmit F_B to the cluster leader A. Similarly the cluster member node C doesn't transmit F_C to the cluster leader A.

In a cluster consisting of 3 members the original CPDA protocol would comprise 10 messages (4 messages from cluster leader node A and 3 messages from each cluster member node B and C respectively). The modified CPDA protocol would comprise 7 messages (3 messages from cluster leader node A and 2 messages from each cluster member node B and C respectively). Therefore in a cluster of 3 nodes, modified CPDA will comprise 3 less messages transmissions. If we consider a large-scale WSN the number of clusters will be more which leads to perceptible abatement in the communication overhead.

In terms of secure version the modified CPDA protocol presents the same communication overhead to the original CPDA protocol. However if the sensor select higher values for its public seed value, then the secure version of the modified CPDA will comprise 2 extra messages from each of the associated sensor nodes. Therefore, for a cluster with 3 nodes, the secure version of modified CPDA protocol will comprise 6 extra messages in the worst case when compared with the original CPDA protocol.

If the probability of sensor node designating itself as cluster leader is p_c then the average number of messages transmitted by sensor node in the original CPDA is : $4p_c+3(1-p_c)=3+p_c$. Thus the message overhead in the original CPDA is 3 less than double as that in TAG. Compare to the modified CPDA protocol the average number of messages transmitted by a sensor node is : $3p_c+2(1-p_c)=2+p_c$. In CPDA protocol the cluster size should be as large as possible in order to avoid collision attack in sensor nodes. This proves that valve of p_c should be small and hence it is understood that the message overhead in the modified CPDA protocol is similar to that of TAG and is still less (one message less for each sensor node) compared to that of original CPDA protocol.

In secure mode of the modified CPDA protocol [4][5] the communication overhead in the average case will be similar to that of original CPDA protocol. But in worst case the number of messages transmitted by a sensor node in this protocol will be $6p_c+5(1-p_c)=5+p_c$ which is 2.5 times the average communication overhead in TAG and 1.67 times the average communication overhead in the original CPDA protocol. Therefore the secure protocol will comprise 67% more overhead in the original CPDA protocol in the worst case scenario (Where a malicious sensor node select higher values for public seed as well as for random numbers).

III. COMPUTATIONAL OVERHEAD

In this section we summarize comparative assay of the computational overhead incurred by the sensor node in the existing CPDA protocol to the efficient version of CPDA protocol.

Computational overhead of the existing CPDA protocol:

In the original CPDA protocol the computational overhead can be divided into four categories:

i) Calculations of variables at sensor nodes: In a cluster consisting of three sensor nodes, each sensor node calculates 3 parameters. For example the cluster leader node A calculates v_A^A, v_B^A, *and* v_C^A. Similarly the cluster member node B computes v_A^B, v_B^B , *and* v_C^B. First we calculate the overhead due to these computations.

Since $v_A^A = a + r_1^A x + r_2^A x^2$, the operations involved in calculating v_A^A for node A are 2 additions, 2 multiplications and 1 exponentiation. Similarly for calculating v_A^A, v_B^A, *and* v_C^A the operation required are 6 additions, 6 multiplications and 3 exponentiation operations. Therefore for a cluster consisting of three nodes, calculation of all the variables in the original CPDA protocol requires 18 additions, 18 multiplications and 9 exponentiation operations.

ii) Calculations involved in encrypting messages: In CPDA protocol, nodes in the cluster perform encryption techniques which involves computation overhead. For example node A performs encryption of v_B^A,v_C^A before transmitting to node B and C respectively. Therefore, 2 encryption operations are needed at cluster leader node A. For a cluster consisting of 3 nodes the protocol requires 6 encryption operations.

iii) Calculation of aggregate results: In a cluster of 3 nodes A, B and C each node calculates its aggregate results F_A,F_B and F_C respectively for the calculation of final aggregate result. Since $F_A = v_A^A + v_A^B + v_A^C = (a+b+c) + r_1 x + r_2 x^2$ and $r1 = r_1^A + r_1^B + r_1^C$, for computing F_A node, A requires 4 addition operations. Therefore 3 nodes in a cluster require 12 addition operations.

iv) Calculation of final aggregate result at cluster leader node: For calculating final aggregate result in a privacy-preserving manner, the cluster leader node A requires one matrix inversion operation and one matrix multiplication operation.

Type of operation	No of operations
Addition	30
Multiplication	18
Exponentiation	3
Encryption	6
Matrix multiplication	1
Matrix inversion	1

Table 1. Operations in the CPDA protocol

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

Computational overhead of the efficient CPDA protocol:

The overhead incurred in the modified CPDA protocol are due to

i) Calculations of variables at sensor nodes: In the modified version of CPDA protocol, nodes A, B and C need to calculate v_A^A, v_B^A, *and* v_C^A respectively. As shown earlier each node requires only 2 additions, 2 multiplications and 1 exponentiation operations leading to a total of 6 additions, 6 multiplications and 3 exponentiation operations.

ii) Calculations involved in encrypting messages: In a cluster of 3 nodes A,B and C, Where A is the cluster leader node, the nodes B and C need to encrypt only v_A^B and v_A^C respectively before transmitting to cluster leader A. Therefore a total of 2 encryption operations are needed.

iii) Calculation of aggregate results: Unlike in the original CPDA protocol, the cluster leader node A will only compute F_A in modified version whereas node B and C need not compute F_B and F_C. As discussed earlier, for computing F_A 4 addition operations are needed.

iv) Calculation of final aggregate result at cluster leader node: Finally for calculating the aggregate function at cluster leader 2 integer division and 2 subtraction operations are needed.

Type of operation	No of operations
Addition	10
Subtraction	2
Multiplication	6
Division	2
Exponentiation	3
Encryption	2

Table 2. Operations in the modified CPDA protocol

By comparing Table 1 and Table 2 it is clear that the modified version of CPDA has less number of operations involved when compared to that of original CPDA protocol and thereby computational overhead is maximally reduced.

IV. CONCLUSION

In-network data aggregation is an important technique which saves energy and communication bandwidth and thereby increasing the lifetime of sensor node for data collection in wireless sensor networks. Here we made a comparative assay of communication and computational overhead of the original CPDA to the modified version of CPDA and found that the modified version of CPDA involves less message transmission overheads in the network and computational load on participating sensor nodes.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol.38, no.4, pp. 393-422, March 2002.

[2] J Sen “Secure and Energy-Efficient Data Aggregation in Wireless Sensor Networks”.

[3] 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.

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

[5] 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 (IEEE ICC’05), vol. 5, pp. 3044–3049, Seoul, Korea, May 2005.