SEEHPIP: Secure Energy Efficient Homomorphism based Privacy and Integrity Preserving Data Aggregation for Wireless Sensor Networks

H S Annappana\textsuperscript{a}, M Siddappa\textsuperscript{a}

\textsuperscript{a}Department of Computer Science and Engineering, Sri Siddhartha Academy of Higher Education, Tumkur. Contact: Email: hsassit@gmail.com, Email:siddappa.p@gmail.com

In Wireless Sensor Network (WSN), sensor nodes must utilize energy efficiently to increase the lifetime of a sensor node. Existing protocols for achieving data privacy and integrity in WSN introduce high communication and computational overhead which causes high energy and bandwidth consumption. Using data aggregation in WSN reduces the energy consumption at a sensor node. Existing privacy preserving data aggregation protocols do not provide efficient solutions for energy constrained and security required WSNs due to the overhead of power consuming operations at aggregator nodes. This paper proposes a new scheme called Secure Energy Efficient Homomorphism based Privacy and Integrity Preserving Data Aggregation for WSNs (SEEHPIP) that uses additive homomorphism to achieve confidentiality during data aggregation. It achieves non-delayed data aggregation by performing aggregation on encrypted data. The proposed scheme is best suited for time critical, secure applications since it achieves privacy, integrity, accuracy, end to end confidentiality, data freshness and energy efficiency during data aggregation without introducing a significant overhead on the battery limited sensor nodes.

\textbf{Keywords} : Aggregator Node, Base Station, Communication Cost, Data Aggregation, Energy, Homomorphism.

1. INTRODUCTION

WSN consists of large number of resource constrained sensor nodes that are deployed over a geographical area for monitoring physical phenomena like temperature, humidity, traffic seismic events and so on. These sensor nodes collect the data, process and forward it to the central node for further processing. For such sensor nodes more energy is required for data transmission than computation. So sensor nodes must send data to Base Station (BS) with less transmission and computational overhead. Since the data collected by sensor nodes are correlated, direct transmission of data from the sensor node to BS wastes too much energy. There are schemes which try to reduce the transmission overhead from sensor node to BS, thereby reducing the energy required for such transmissions. Data aggregation is one such scheme which gathers the related information from several sensor nodes, aggregates this information and sends the aggregated result to the BS. In the applications like temperature sensing, humidity sensing etc., many sensor nodes are deployed over a specific region. Each sensor node must sense the temperature/humidity in the location where it is deployed and communicate it to the BS which increases the communication cost. Data aggregation techniques can effectively reduce the amount of data transmitted to the BS by aggregating the data using aggregation functions like MIN, MAX, MEAN etc., Data Aggregation increases the lifetime of the network by greatly reducing the number of messages sent in a network which leads to large energy savings. In-network aggregation is an extension of data aggregation that calculates intermediate results along the multi hop path whenever two or more messages are sent along the same path.
5.2.4. Calculation of Energy Consumption in SEEHP/IP Scheme for Data Privacy

For the proposed SEEHP/IP scheme, each node \( i, i=1 \) to \( N \), exchanges only one message for data privacy with a message size of 4 bytes. So, time required for transmitting 4 bytes of data = \( 4 \times 8 \times 10^6 = 0.000032 \) seconds. So, energy required for transmitting and receiving 4 bytes of data by each node is \( 1.055 \times 0.000032 = 0.0000033 \) joules. The energy consumption for a network with 50 nodes is \( 50 \times 0.0000033 = 0.0016 \) joules.

In PEPPDA scheme, if the number of slices increases, then each node must communicate \( m^2 \) bytes of data for data privacy. But in our scheme each node always communicates 4 bytes of data for data privacy. Table 3 shows the comparison of energy consumption for data privacy in PEPPDA and SEEHP/IP schemes with varying number of sensor nodes. Figure 10 depicts the graph for energy consumption by PEPPDA and SEEHP/IP schemes for data privacy. It is evident from the graph that the energy consumption of SEEHP/IP scheme is less than PPAI scheme as it generates less number of messages in the network.

5.3. Computation Cost

Computation cost is measured in terms of number of encryptions, decryptions and other arithmetic operations performed during secure data transmission and secure key establishment. PPAI scheme uses hop by hop encryption for secure data transmission which introduces computational overhead at intermediate nodes. It also introduces computational overhead during secure key establishment. In PEPPDA scheme, leaf node slices its data into \( m \) number of pieces and encrypts each slice with encryption key. So, each leaf node performs \( m \) encryption operations on \( m \) pieces. Aggregator node performs only one encryption operation. SEEHP/IP scheme uses end to end encryption scheme used in PEPPDA scheme which introduces less computation overhead at intermediate nodes to achieve data confidentiality and also during key establishment phase. Table 4 shows the communication cost of all the three schemes for key establishment and for achieving data privacy and integrity.

6. CONCLUSIONS

In this paper, we have presented a new SEEHP/IP scheme to provide privacy and integrity preserving data aggregation for WSNs. It is an energy efficient scheme which reduces the computational overhead associated with PPAI scheme and communication overhead associated with PEPPDA scheme. Performance results show that the performance of our proposed SEEHP/IP scheme is better in comparison with PPAI and PEPPDA schemes. As future work fault tolerance can be included. The proposed scheme assumes that there is no communication link or data packet loss during communication. But in real time scenario link failure or packet loss is common. Thus addressing fault tolerance is also very important for real time data aggregation applications.

REFERENCES

1. Hassan Am, Sunit Ozdemir, Prashant Nair, Devasenapathy Muthuramalingam and H Ozgur Sunil. Energy-Efficient Secure Pattern Based Data Aggregation for Wireless


H S Annapurna is currently working as Associate Professor in the Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur. She has obtained her Bachelor of Engineering from University of Mysore, Mysore. She has received Masters degree in Software Systems from BITS, Pilani. She is currently pursuing Doctoral degree from Sri Siddhartha Academy of Higher Education, Tumkur.

M Siddappa received B E and MTech Degrees in Computer Science and Engineering from University of Mysore, Karnataka, India in 1989 and 1993 respectively. He has completed doctoral degree from Dr. MGR Educational Research Institute Chennai under supervision of Dr. A S Manjunatha, CEO, Manvish e-Tech Pvt. Ltd., Bangalore in 2010. He worked as Project Associate in IISc, Bangalore under Dr. M P Srivanas and Dr. V Rajaraman from 1993/4 to 1995. He has teaching experience of 26 years and research of 10 years. He published 45 Technical Papers in National, International Conference and Journals. He has citation index of 113 till 2015 and
h-index of 3 and i10-index of 1 to his credit. He is a member of IEEE and Life member of ISTE. He is working in the field of Data Structure and Algorithms, Artificial Intelligence, Image Processing and Computer networking. He worked as Assistant Professor in Department of Computer Science and Engineering from 1996 to 2003 in Sri Siddhartha Institute of Technology, Tumkur. Presently, he is working as Professor and Head, Department of Computer Science and Engineering from 1999 in Sri Siddhartha Institute of Technology, Tumkur. He has visited Louisiana university Baton rouge and California university.