International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 39528-39535
© Research India Publications. http://www.ripublication.com

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

H. S. Annapurna

Research Scholar, Dept. of Computer Science & Engg., Sri Siddhartha Academy of Higher Education, Tumkur, India.
Mob: 9448173960, Email: hsassit@gmail. com

M. Siddappa

Professor and Head, Dept. of Computer Science & Engg., Sri Siddhartha Institute of Technology, Tumkur, India.
Mob: 9448077405, Email: siddappa. p@gmail. com

Abstract

In Wireless Sensor Network (WSN), sensor nodes must utilize energy efficiently to increase the life time 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.

Keywords-Aggregator node, Base Station, Communication cost, Data aggregation, Energy, Homomorphism.

I. 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.

If the message to be transmitted from sensor node to BS is confidential, it should be transmitted in a secure manner. If an unauthorized user (adversary) tries to access the secure data it should not be possible for him/her to get the data. Security requirements for data aggregation include confidentiality, integrity, freshness and availability. During data aggregation confidentiality is ensured by applying aggregation functions directly on the encrypted data. Integrity ensures that the content of the message has not been altered either maliciously or accidentally during its transmission. Data freshness ensures that the data are recent and no old messages have been replayed to protect data aggregation schemes against replay attacks. Ensuring availability means that the network is alive and that the data is accessible. Data aggregation security requirements should be carefully implemented to avoid extra energy consumption.

Several data aggregation schemes for WSNs have been proposed to achieve privacy and confidentiality for the data [1], [2], [3], [4], [5], [6]. Some data aggregation schemes [7], [8], [9] for WSNs assume that all sensors are trusted and all communications in the network are secure. However, in reality sensor networks are likely to be deployed in hostile or uncontrolled environment where links can be eavesdropped. Cryptographic keys can be compromised by an adversary and data can be manipulated. In addition, these schemes have not considered data integrity and privacy issues.

In this paper, we introduce a novel scheme to provide privacy and integrity preserving data aggregation for WSNs. It is homomorphism based privacy and integrity preservation protocol and achieves non-delayed data aggregation by performing aggregation on encrypted data. Since aggregator node performs aggregation on encrypted data, it decreases the node compromise attack. So, high chance to get accurate aggregated results at the BS with reduced computation overhead. We show that our scheme achieves data privacy, integrity and confidentiality with less communication and computation overhead and is quite efficient. Rest of the paper is organized as follows: Section II highlights the related work. Section III depicts the system model. Section IV explains the proposed scheme in detail. We analyze the performance of our scheme in comparison with PPAI [3] and PEPPDA [2] schemes in section V before concluding the paper in Section VI.

II. Related Work

Many data aggregation schemes [7], [8], [9] for WSN's assume that all sensor nodes are trusted and all communications in the networks are secure. However, in reality, sensor networks are likely to be deployed in hostile and uncontrolled environment where links can be eavesdropped. Cryptographic keys can be compromised by an adversary and data can be manipulated. In addition, these schemes have not considered data integrity and privacy issues.

Several schemes have been proposed to support end to end encryption[1], [10], [4], [2]. In these schemes, confidentiality is provided by allowing aggregation to be carried out on encrypted data rather than on plain text as in hop by hop encrypted data aggregation protocols[3, [6], [5], [11], [12]. The Energy-efficient Secure Pattern based Data Aggregation for WSNs (ESPDA) [1] improves the energy efficiency by sending pattern code instead of actual data. The privacy is achieved using end to end encryption key of each node. It also provides confidentiality and message authentication for the data. The Concealed Data Aggregation (CDA)[10] uses the end to end encrypted aggregation using DF's (Domingo-FerrorJ) approach [13] to reduce high computational overhead of hop by hop aggregation. All sensor nodes share a common encryption key with the BS. So, compromise of one sensor node leads to loss of privacy between the sensor nodes. But in Efficient Aggregation of Encrypted Data in WSN (EAED) [14], each node shares a unique key with the BS. Thus it achieves data privacy among sensor nodes, but it is not scalable in the large network because BS wants to know the keys of all aggregated packets. So it causes the transfer of nodes' ID. The Recoverable Concealed Data Aggregation for data integrity in WSNs (RCDA) [4] was elliptic curve based additive privacy homomorphism technique to achieve end to end privacy and confidentiality. The recoverability of individual sensing data at the BS helps to overcome the limitation of BS on aggregation function and to verify integrity, authenticity of sensing data using the aggregated signature scheme. In Power Efficient Privacy Preserving Data Aggregation (PEPPDA) scheme[2], leaf node uses the concept of data slicing and assembling to preserve data privacy with end to end encryption to achieve confidentiality. In this scheme each leaf node randomly selects a set of nodes *S* within *h* hops, for dense network *h*=1. Each leaf node splits sensed data into *K* pieces (*K*=*S*), keeps one piece within itself and remaining *K*-1 pieces are sent to randomly selected nodes except to its parent. Data piece for parent node is sent along with aggregation result from leaf node. In this scheme, each node shares symmetric key with BS and uses end to end encryption operation on the sensed data. The Preserving Privacy Assuring Integrity Data Aggregation (PPAI)[3] assures integrity and uses hop by hop encryption used in [6] on modified data by sharing common key between every pair of sensor nodes. Sharing of hop by hop symmetric key introduces high communication and computation overhead using the scheme in [6] PDA[5] provides additive aggregation scheme to protect the privacy in a tree topology. In this scheme each node slices its data into number of pieces and sends it to randomly selected nodes which introduces high communication overhead. The communication cost increases as the number of slices increases. But Energy Efficient and High Accuracy Secure Data Aggregation (EEHA) scheme[11] provides high accuracy data aggregation without releasing private data of a sensor and without introducing considerable overhead on the battery limited sensor nodes. It minimizes the communication overhead associated with PDA scheme by applying a slicing operation only at the leaf nodes, EEHA scheme[11] uses hop by hop encryption which introduces computational overhead at intermediate nodes. In integrity protecting Private Data Aggregation (iPDA) [15], data privacy is achieved through slicing and assembling technique and the integrity achieved through redundancy by constructing a disjoint aggregation tree. PEPPDA scheme [2] is an improvement over the schemes [11], [15] where hop by hop encryption is replaced by end to end encryption and PEPPDA minimizes communication overhead and computational overhead as in EEHA[11] and PDA[5].

The scheme proposed in this paper is a combined approach of PPAI[3] and PEPPDA[2] scheme and minimizes communication and computational overhead of these schemes. Our scheme achieves data privacy by breaking sampled data into two pieces and mixing each piece of data with a unique private seed and performing additive homomorphic encryption on the modified data. Integrity of the aggregated data is assured by sending another copy of the data independently created by breaking and mixing mechanisms.

III. System Model

There are *N* number of resource constrained sensor nodes in a network where *N* is a large positive integer. The nodes communicate with the BS in a multi hop manner. In our proposed schemenodes are organized in the form of a binary tree as in TAG[7] and aggregation is performed on the aggregation tree rooted at the BS. There are 3 types of nodes in the network, BS or sink node, the intermediate node (aggregator node) and a leaf node (normal sensor node). The leaf node performs sensing and forwarding of data to aggregator node. The aggregator node performs sensing, aggregation and forwarding of data from leaf node to upper aggregator or to sink nodedepending on the type of sensor network. The BS processes and derives the meaningful information from the received data. The proposed scheme uses SUM data aggregation function.

The assumptions made by our proposed scheme are:

- Sink is trustworthy and has enough resources. The adversaries can compromise all other nodes except the sink node.
- No message loss during data aggregation.
- Keys are securely preloaded to each node before deployment

Objectives of the proposed scheme are:

- Achieving data aggregation with privacy, integrity, confidentiality, freshness and energy efficiency.

Data privacy: Ensures that the data sensed by each sensor node should be known only to itself, no matter how many nodes have been compromised.

Data Integrity: Ensures that the data received by the sink is not altered on transit by an adversary.

Data Confidentiality: Guarantees that the partially or fully aggregated data is known only to the sink, no matter how many nodes have been compromised. The confidentiality is achieved by the end to end encryption.

Data Freshness: Ensures that the data are recent and that no old messageshave been replayed to protect data aggregation schemes against replay attack.

Energy Efficiency: Data aggregation protocol should be energy efficient while it preserves the privacy and confidentiality of data.

IV. Proposed Scheme

We discuss our proposed scheme in three phases:

1. Key distribution
2. Achieving privacy, integrity and confidentiality
3. SEEHPIP Algorithm

1. Key distribution in proposed SEEHPIP

Asymmetric cryptographic protocols are not suitable for resource constrained sensor nodes as they consume lot of resources. Here we are using energy efficient security protocol of PEPPDA scheme[2] for achieving data confidentiality. Each sensor node is preloaded with a common secret key K, node specific key K_i and an initial seed number S_{i1} and a unique identifier ID_i, i=1, 2,.... *N* before deployment as shown in Fig. 1.

K	K_i	S_{i1}	ID_i

Fig. 1: Keys stored in sensor node.

The sink is assigned with a secret key K a session key K_s, initial seed S_{i1} of all the nodes and the pairs (ID_i, K_i) of all nodes in the network, i=1, 2,....... *N*. The contents are shown in Fig. 2

K	K_s	S_{i1}	(ID_i, K_i)

Fig. 2: Keys stored at sink node.

The sink node generates the session key K_s for each session and broadcasts to all the nodes in the network using the common secret key K. Upon receiving, each node decrypts and gets the session key K_s by using the common secret key K. Then each node i generates its own encryption key K_{ei}, i=1 to *N* by XORing the session key and node specific key.

$K_{ei} = K_i \oplus K_s$, for i=1 to *N*

Whenever the sink node receives the partially aggregated encrypted data from the aggregator, it first determines K_i of the sensor node i, i=1 to *N* by using ID's of aggregator and the sender. Then generates decryption key by XORing node specific key K_i with session key K_s transmitted by the sink node. The encryption key K_{ei} of node i, i=1 to *N* is changed for each session providing data freshness. Fig. 3 shows key distribution in the proposed scheme.

K, K_s, S_{i1}, ID_i, K_i

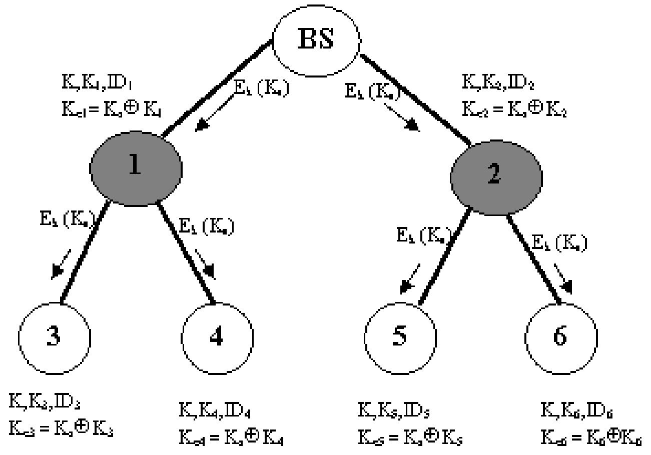


Fig. 3: Key distribution in SEEHPIP

2. Achieving privacy, integrity and confidentiality in SEEHPIP

The new privacy homomorphism based scheme uses privacy preserving scheme used in PPAI scheme [3] to reduce communication overhead and end to end data encryption used in PEPPDA scheme [2] to reduce computation overhead. At the same time, it can check data integrity of the aggregated data at the sink node. The new SEEHPIP scheme is a general approach because it can be applied to any WSN with arbitrary tree topology. It consists of 4 steps:

a. Aggregation Tree Construction

Aggregation tree is constructed using TAG[7] protocol. Here BS is assumed to be the root node and it assigns level 0 to itself, broadcasts the message that contains its level number and node ID. Nodes within the energy region of BS receive broadcast message and increment the level number by one and use the node ID of BS as their parent ID. Nodes rebroadcast the message that contains updated level number and their node ID and nodes within the energy range receive message, increment level number by one and use node ID as their parent ID. Same procedure continues until every node is assigned with level number and parent. If a node receives message for the second time, then that node discards the message. Fig. 4 shows the tree constructed using the above procedure.

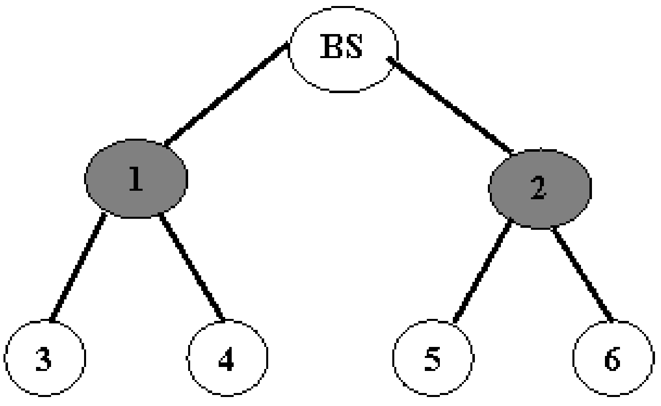


Fig. 4: Data Aggregation tree.

b. Splitting

For data confidentiality, we use end to end data encryption scheme using additive privacy homomorphism which was used in PEPPDA scheme [2]. On sensed data d at node i, we perform additive homomorphic encryption using encryption key k_{ei}that is generated by XORing node specific key K_i with session key K_s received from BS, i=1, 2... *N*

$C_i = E_{K_{ei}}(d), \text{for } i = 1, 2, \ldots. N$

$((R_1, R_2), (R_3, R_4))||ID_3||ID_4||ID_1$

Here, we use the concept of data splitting used in PPAI scheme[3] for achieving data privacy. Each node splits its encrypted data C_i into c_1 and c_2 and again independently splits same data C_i into c_3 and c_4. For each data piece we add private seeds which are preloaded in each node. Seeds are some random numbers which are different for each sensor node and every node stores initial seed and other seeds are generated using pseudo random generators. Every node i maintains four seeds. First twoi. e., S_{i1}, S_{i2} for data privacy and next two i. e., S_{i3}, $S_{i4}$for data integrity. Now, we add c_1 with seed S_{i1}, c_2 with S_{i2}, c_3 with $S_{i3}$and c_4 with S_{i4}, i. e., $M_{i1}=c_1+S_{i1}$, $M_{i2}=c_2+S_{i2}$, $M_{i3}=c_3+S_{i3}$, $M_{i4}=c_4+S_{i4}$. These four computed values are grouped into two pairs <M_{i1}, M_{i2}> and<M_{i3}, M_{i4}> and are sent to upper level node by attaching node ID of the sender. The first pair <M_{i1}, M_{i2}> is used for data privacy and the second pair <M_{i3}, M_{i4}> for data integrity. This mechanism provides high level of data privacy because the sampled data can be known to neighboring trusted nodes only if they have information of at least two private seeds of a sensor node. By increasing the ranges (the numerical space between lower bound integer and upper bound integer) of private seeds, the level of privacy can further be improved. Fig. 5 shows homomorphic encryption and data splitting.

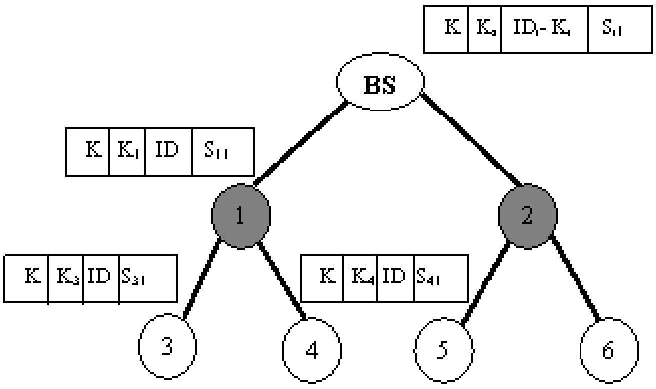
Data sensed at node i is d for i=1, 2, …*N*

$C = E_{K_{ei}}(d)$

$C=c_1, c_2$ $C=c_3, c_4$

$M_{i1} = c_1+S_{i1}$ $M_{i2} = c_2+S_{i2}$

$M_{i3}=c_3+S_{i3}$ $M_{i4}=c_4+S_{i4}$

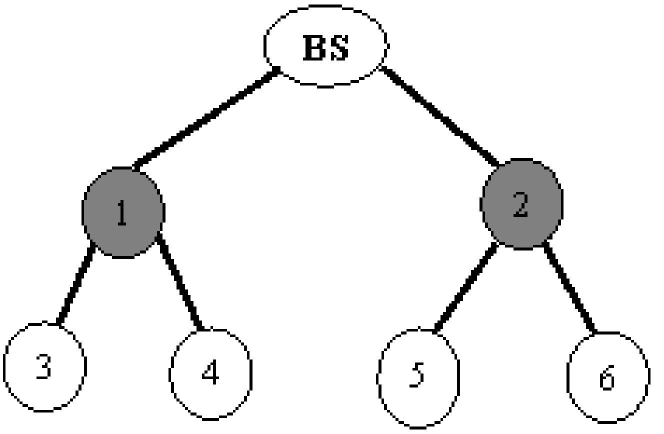


$((M_{31}, M_{32}), (M_{33}, M_{34})) \mid\mid ID_3 \, ((M_{41}, M_{42}), (M_{43}, M_{44})) \mid\mid ID_4$

Fig. 5: Data Splitting

c. Partial data aggregation at aggregator

Each aggregator node i, receives data <<M_{i1}, M_{i2}><M_{i3}, M_{i4}>> along with ID from its child nodes 2i+1 and 2i +2, for i=1 to n/2-1 and adds each encrypted component of sensor node to respective encrypted component of other sensor node including its own. In the existing PPAI scheme[3], each pair of nodes shares common key for hop to hop encryption[14] which consumes lot of resources at aggregator node. In the proposed scheme, we use end to end encryption using additive homomorphic encryption. Here, aggregator node performs SUM aggregation on encrypted data without decryption, which saves computation cost at aggregator nodes thereby saving energy. Fig. 6 shows partial sum aggregation at node 1 and sending aggregated data to BS.



$((M_{11}, M_{12}), (M_{13}, M_{14}))||ID_1$

$((M_{31}, M_{32}), (M_{33}, M_{34})) \mid\mid ID_3 \, ((M_{41}, M_{42}), (M_{43}, M_{44})) \mid\mid ID_4$

At node 1

$((R_1=M_{31}+M_{41}+M_{11}, R_2=M_{32}+M_{42}+M_{12}), (R_3= M_{33} + M_{43} + M_{13}, R_4 = M_{34} + M_{44}+ M_{14}))$

Fig. 6: Partial data aggregation

d. Final sum aggregation at BS

When partially aggregated data reaches the sink node, it adds first and second data parts, then third and fourth data parts. To check data integrity, the sink node performs the following operations when it receives ((R_1, R_2), (R_3, R_4)) from aggregator nodes as shown in Fig. 6:

$R_{privacy}$= (R_1+R_2)
$R_{integrity}$= (R_3+R_4)

$$\mathrm{Sum}_1 = \mathrm{R}_{\mathrm{privacy}} - (S_{31} + S_{41} + S_{11} + S_{32} + S_{42} + S_{12}) - (E_{K_{e3}} + E_{K_{e4}} + E_{K_{e1}})$$

$$\mathrm{Sum}_2 = \mathrm{R}_{\mathrm{integrity}} - (S_{33} + S_{43} + S_{13} + S_{34} + S_{44} + S_{14}) - (E_{K_{e3}} + E_{K_{e4}} + E_{K_{e1}})$$

If Sum_1==Sum_2
Return Sum_1 or Sum_2 // data not corrupted
else
Reject Sum_1 and Sum_2 // data has been corrupted

3. SEEHPIP Algorithm

Step1: Construct aggregation tree using TAG[7] protocol.

Step2: The BS broadcasts the session key K_s by encrypting using common secret key in the network.

Step 3: Each node i generates the encryption key K_{ei}as follows: K_{ei} =K_i⊕ K_s, for i=1 to *N*

Step 4: Each node i, for i=1 to *N* Sense d // data sampling C= $E_{K_{ei}}$ (d)// encrypt sensor reading using encryption key. Split (C) C=c_1, c_2// divide encrypted reading C into two unequal data pieces. Split (C) // divide d into two unequal data pieces. C=c_3, c_4; for j= 1 to 4 //combine each data piece with a seed. M_{ij}= c_i + S_{ij}; Msg=<<M_{i1}=c_1+S_{i1}, M_{i2}=c_2+S_{i2}>, <M_{i3}=c_3+S_{i3}, M_{i4}=c_4+S_{i4}>> Transmit (Msg); // Append the node ID and sendto its parent.

Step 5: Generate partially aggregated data at aggregator nodes for every data aggregator. For all received modified data from children Sum up respective results received from child nodes with its own encrypted data. Append the intermediate node ID with the aggregated data and send to its parent.

Step 6: Compute aggregation result at the sink node. Receive partial aggregated data from each aggregator node. Add data privacy parts, it results in $R_{privacy}$, i. e., M_{i1}, M_{i2}, first and second part. Add data Integrity parts, it results in $R_{integrity}$, i. e., M_{i3}, M_{i4}, third and fourth part. Generate decryption key for each contributed sensor node. Subtract decryption key and seeds from $R_{privacy}$ and $R_{integrity}$It results in Sum_1 and Sum_2. Check for integrity If Sum_1== Sum_2 Accept data //Data not modified Else Reject data //Data has been modified.

V. Performance Evaluation

We analyze the performance of our scheme to show its resource efficiency and compare it with PPAI and PEPPDA schemes in terms of communication cost, energy efficiency and computational cost. We then discuss the performance results.

5. 1 Communication Cost

Communication cost is measured in terms of number of messages generated by sensor node for achieving data privacy, integrity and for secure key establishment for data confidentiality. In our scheme, we use the concept of data splitting to achieve data privacy and integrity which requires very less communication overhead. We use end to end encryption to achieve data confidentiality which requires very less communication overhead for secure key establishment. So, one message needs to be exchanged for data privacy and integrity and one message is required for key establishment for each node. Therefore communication cost for achieving data privacy and integrity is *N* and communication cost for key establishment is *N* where *N* is the number of nodes in the network. PPAI scheme [3] achieves data privacy and integrity without any message exchange. Only one message is sent to upper level node for aggregation with privacy protection. So communication cost for achieving data privacy and integrity is *N*. PPAI scheme[3] uses hop by hop encryption protocol for data confidentiality. Each sensor node exchanges minimum five messages for key establishment with its single predecessor in the best case, seven messages in the average case and twelve messages in the worst case. In PEPPDA scheme only leaf node uses slicing operation for data privacy. Each leaf node slices its data into m number of pieces and one piece is kept in the node itself and remaining m-1 slices are securely distributed to set of randomly selected h hop neighbor nodes. Communication cost in this scheme is *m*L*for the leaf node and *N-L* for the intermediate node for data privacy where *L* is the number of leaves and *N-L* is the number of aggregators. For key establishment each node exchanges one message, so the communication cost is *N*. Table I shows the communication cost of all the three schemes for key establishment and for achieving data privacy and integrity. Fig. 7 (a) and 7 (b) show the graphs for communication cost for key establishment and for achieving data privacy and integrity respectively. It is clear from the graphs that SEEHPIP scheme is more efficient than PPAI scheme[3] for key establishment and PEPPDA scheme[2] for achieving data privacy.

Table I: Communication cost of PPAI, PEPPDA and SEEHPIP schemes

Scheme	Communication cost for key establishment		Communication cost for privacy and integrity
PPAI	12×*N*, *N*>=5		*N*
PEPPDA	Leaf	*N*	*m*×*L*
	Aggregator		*N-L*
SEEHPIP	*N*		*N*

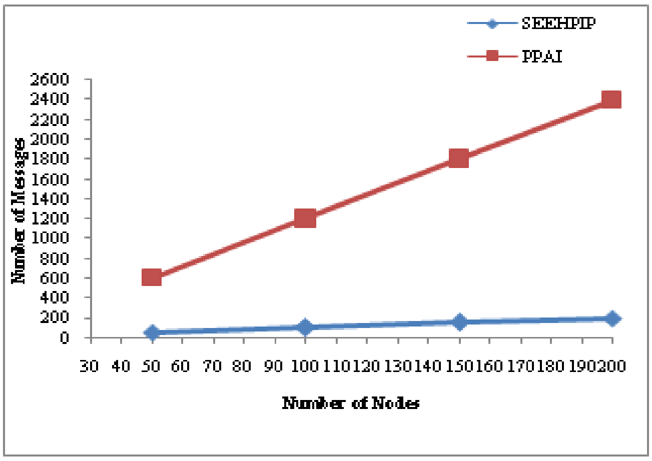


Fig. 7 (a) Communication cost for key establishment

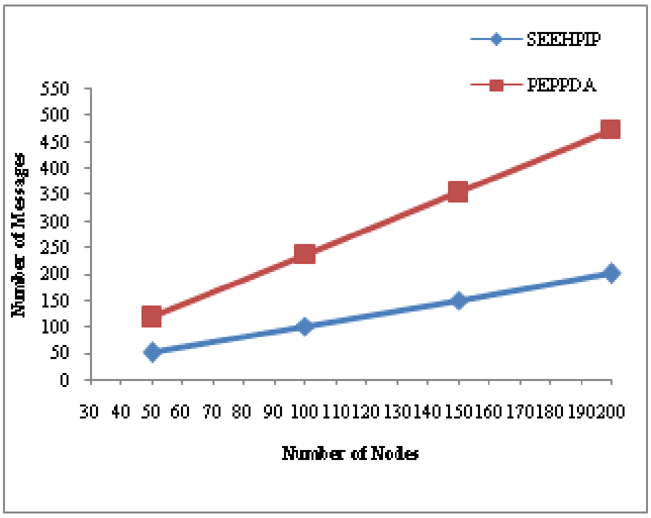


Fig. 7 (b) Communication cost for data privacy

5. 2 Energy Efficiency

For calculating energy consumption, we consider a total available battery power as *100J* receiving power dissipation as *395mW*, transmitting power dissipation as *660mW*, data rate as 1*Mbps*and transmission range as *50m*.

5. 2. 1 Calculation of energy consumption in PPAI scheme for key establishment

A network with *N* nodes requires *12*N* messages to establish a key between each node i and its parent, for i = 1 to *N*. Each message contains key splits and it is of size 2 bytes, so time required to transmit 2 bytes of data is 2*8/10^6 = 0. 000016 seconds. Energy consumption for both transmitting and receiving 2 bytes of data is 1. 055*0. 000016 = 0. 0000168 joules. Energy consumption for transmitting and receiving 12 messages is 12* 0. 0000168 = 0. 000202 joules. Thus energy consumptionfor a network with 50 nodes is 50*0. 000202 = 0. 0101 joules.

5. 2. 2 Calculation of energy consumption in SEEHPIP scheme for key establishment

A network with *N* nodes requires *N* messages for key establishment with the base station. Each message contains encrypted session key of size 2 bytes. So, energy consumption for a network with 50 nodes is 50*0. 0000168 = 0. 00084 joules.

Table II shows the comparison of energy consumption for key establishment in PPAI and SEEHPIP schemes with varying number of sensor nodes. Fig. 7 (c) depicts the graph for energy consumption by PPAI and SEEHPIP schemes for key establishment. As expected, the dissipated energy in both the schemes increases when the number of sensor nodes increases. It is evident from the graph that SEEHPIP scheme is more energy efficient than the PPAI scheme as it generates less number of messages in the network.

Table II: Comparison of energy consumption for key establishment in PPAI and SEEHPIP schemes

Number of Nodes	Energy consumption in Joules	
	PPAI	SEEHPIP
50	0. 0101	0. 00084
100	0. 0202	0. 00168
150	0. 0303	0. 00252
200	0. 0404	0. 00336

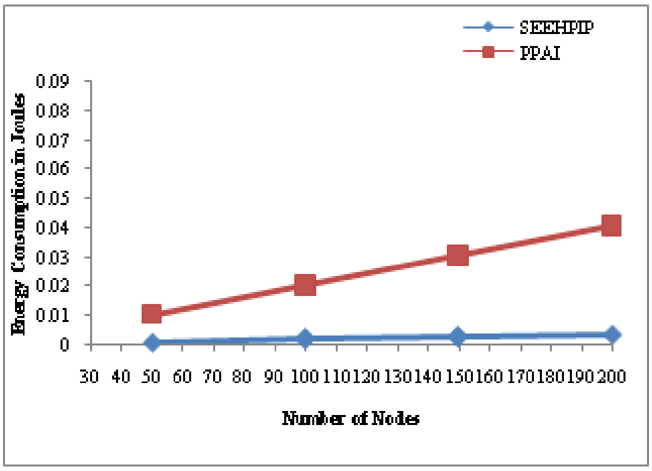


Fig. 7 (c) Energy consumption for Key establishment

5. 2. 3 Calculation of energy consumption in PEPPDA scheme for data privacy

For PEPPDA scheme we consider m=3, number of data slices for achieving data privacy at leaf nodes. So each leaf node must communicate a total of 6 bytes of data for data privacy. Thus transmission time for 6 bytes of data is 6*8/10^6 = 0. 000048 seconds. For a network with 50 nodes, there are 34 leaf nodes and 16 non-leaf nodes and total energy consumed by each leaf node for data privacy is 1. 055*0. 0000048 = 0. 0000506 joules. For 34 leaf nodes, total energy consumed is 34*0. 0000506 = 0. 00172 joules. Non-leaf nodes do not use slicing and mixing mechanism for data privacy, instead they take advantage of SUM aggregation function. So, each aggregator node exchanges only 2 bytes of data and the time required is 2*8/10^6 = 0. 000016 seconds. Energy consumption for each non-leaf node to achieve data privacy is 1. 055*0. 000016 = 0. 0000168 joules. Total energyconsumption for 16 non-leaf nodes is 16* 0. 0000168= 0. 00027 joules. Hence, total energy consumption for both leaf and non-leaf nodes is 0. 00197 joules.

5. 2. 4 Calculation of energy consumption in SEEHPIP scheme for data privacy

For the proposed SEEHPIP 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*8/10^6 = 0. 000032 seconds. So, energy required for transmitting and receiving 4 bytes of data by each node is 1. 055*0. 000032 = 0. 000033 joules. The energy consumption for a network with 50 nodes is 50*0. 000033 = 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 III shows the comparison of energy consumption for data privacy in PEPPDA and SEEHPIP schemes with varying number of sensor nodes. Fig. 7 (d) depicts the graph for energy consumption by PEPPDA and SEEHPIP schemes for data privacy. It is evident from the graph that theenergy consumption of SEEHPIP scheme is less than PPAI scheme as it generates less number of messages in the network.

Table III: Comparison of energy consumption for data privacy in PEPPDA and SEEHPIP schemes

PEPPDA (m=3, k=3)				SEEHPIP
Number of nodes	Energy consumption for leaf nodes in joules	Energy consumption for non leaf nodes in joules	Total energy consumption in Joules	Total energy consumption in Joules
50	0. 0017	0. 00026	0. 0019	0. 0016
100	0. 0034	0. 00053	0. 0039	0. 0033
150	0. 0051	0. 00082	0. 0059	0. 0049
200	0. 0067	0. 0011	0. 0078	0. 0066

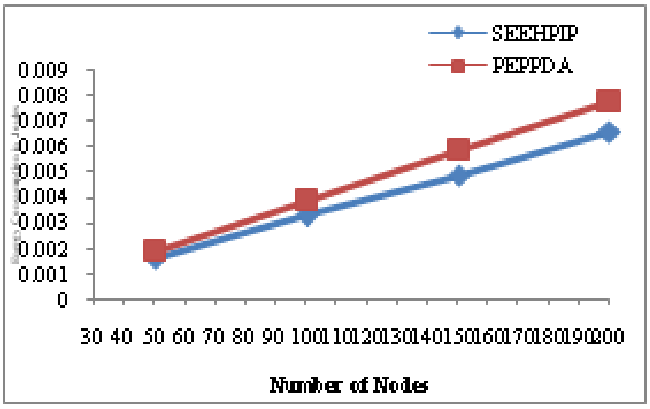


Fig. 7 (d) Energy consumption for privacy

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 withencryption key. So, each leaf node performs *m* encryption operations on *m* pieces. Aggregator node performs only one encryption operation. SEEHPIP 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 IV shows the communication cost of all the three schemes for key establishment and for achieving data privacy and integrity.

Table IV: Computational cost of PPAI, PEPPDA and SEEHPIP schemes

Schemes	Node Type	Number of operations to achieve data privacy and integrity			Number of operations required for secure key establishment for each node		
		Add	Sub	Encryptions and Decryptions	Encryptions and Decryptions		
					Best	Worst	Average
PPAI	Leaf	4	2	1, 0	4, 4	13, 11	8, 8
	Aggregator	8	2	1, Number of children of each aggregator			
PEPPDA	Leaf	1	m-1	m, 0	1, 1	1, 1	1, 1
	Aggregator	1	0	1, 0			
SEEHPIP	Leaf	4	2	1, 0	1, 1	1, 1	1, 1
	Aggregator	8	2	1, 0			

VI. Conclusion

In this paper, we have presented a new SEEHPIP 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 SEEHPIP 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 Cam, SuatOzdemir. Prashant Nair, DevasenapathyMuthuavinashiappan, H. OzgurSanil. “Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks”, Computer Communications, Vol. 29, Issue 4, 20 February 2006, pp. 446_455.

[2]. Joyce Jose, M Prince and Joana Jose. “PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks”, 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013.

[3]. RabindraBista, Myoung-Seon Song and JaeWoo Chang. "Preserving Privacy and Assuring Integrity in Data Aggregation for Wireless Sensor Networks", IEEE, 2010.

[4]. Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, Hung-Min Sun. "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", IEEE Transactions on parallel and distributed system, Vol. 23, No. 4. April 2012.

[5]. He W, Liu X, Nahrstedt K, Abdelzaher T. "PDA: Privacy preserving data aggregation in wireless sensor networks", Proceedings of 26th IEEE International Conference on Computer Communications (Infocom). Anchorage, laska. USA: 2045-2053, May 2007.

[6]. E-O, Blab, and M. Zitterbart. "An efficient key establishment scheme for secure aggregating sensor networks", in Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, pp. 303-310, March 2006.

[7]. Madden, Samuel R, Franklin, Michael J, Hellerstein, Joseph M, Hong W. "TAG: a tinyaggregation service for ad hoc sensor networks", OSDI, 2002.

[8]. C Itaagonwiwat, R Govindan, and D Estrin. "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks"MobiCom, 2002.

[9]. R Bista, Y K Kim, J W Chang. "A new Approach for Energy-Balanced Data Aggregation in Wireless Sensor Networks", CIT09, cit, vol. 2, pp. 9-15, 2009.

[10]. J Girao, D Westho_, M Schneider. "CDA: Concealed Data Aggregation for reverse multicast traffic in Wireless Sensor Networks". Inproc. 40thInternational Conference on Communications, IEEE ICC, May 2005.

[11]. Hongjuan Li, Kai Lin, Kequi Li. "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks", ComputerCommunication. 34 (2011); 591-597, 2011.

[12]. Y Yang, X Wang and S Zhu. _SDAP: a Secure Hop-by-Hop Data Aggregation Protocolfor Sensor Networks_. In Proc. 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing, May 2006.

[13]. Domingo-Ferrer J. "A provably secure additiveand multiplicative privacy homomorphism", In Proceedings of the 5th International Conference on Information Security, Sao Paulo, Brazil; pp.-483, September 30-October 2. 2002.

[14]. Castelluccia C, Mykletun E. Tsudik G. "Efficient Aggregation of encrypted data in wirelesssensor networks". In Proceeding of the 2nd Annual International Conference on Mobile andUbiquitous Systems: Computing, Networkingand Services, MobiQuitous, San Diego, CA. USA: PP. 109-117, July 17-21, 2005.

[15]. W He, X Liu, H Nguyen, K Nahrstedt, T Abdelzaher. "iPDA: An Integrity-Protecting Private Data Aggregation Scheme for wireless Sensor Networks". IEEE MILCOM, pp 1-7, November 2008.

H. S Annapurna is currently working as Associate Professor in the department of Computer Science &Engg., 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 Doctral degree in the area of cryptography and network security from Sri Siddhartha Academy of Higher Education, Tumkur, India.

M. Siddappa received B. E and M. Tech degree in Computer Science & 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 Srinivasan and Dr. V. Rajaraman from 1993 – 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 & Engineering from 1996 to 2003 in Sri Siddhartha Institute of Technology, Tumkur. Presently, he is working as Professor and Head, Department of Computer Science & Engineering from 1999 at Siddhartha Institute of Technology, Tumkur. He has visited Louisiana university Baton rouge and California university.