Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT SECURE SCHEME FOR DATA AGGREGATION IN WIRELESS SENSOR NETWORKS USING THE ADDITIVE PROPERTY OF COMPLEX NUMBERS

[1]SAMIHA M. ELSHERIF , [2]MOHAMED ELSHRKAWEY, [3]M. ELSAYED WAHED

[1]Suez Canal University, Faculty of Computers & Informatics, Information System Department, Ismailia 41522, Egypt
[2]Suez Canal University, Faculty of Computers & Informatics, Information System Department, Ismailia 41522, Egypt
[3]Suez Canal University, Faculty of Computers & Informatics, Information System Department, Ismailia 41522, Egypt
E-mail: [1]samiha_ahmed@ci.suez.edu.eg, [1]samiha.ahmed910@gmail.com,[2] melshrkawey1964@yahoo.com, [3]mewahed@yahoo.com

ABSTRACT

Data aggregation is an essential technique that has been widely used in Wireless Sensor Networks (WSNs) to reduce the energy consumption of sensor nodes. It can preserve the significant amount of energy by aggregates data from sensor nodes which reducing the number of data packets. However, data aggregation applications need integrity protection and privacy preserving of the data while transmitting it from sensing nodes to the base station. The existing schemes such as IPDA, ICPDA, and PEPPDA suffer from high communication, computation cost and data delay even it support both privacy and integrity. Therefore, this paper proposes an efficient, secure data aggregation scheme for wireless sensor networks. The proposed scheme eliminates redundant sensor data without using decryption and maintains data privacy during transmission. We use the additive property of complex numbers to support privacy and integrity checking. The complex number has two parts; the real part will be used to hide sensitive data and the imaginary part will be used to check the integrity of the aggregated data. The proposed scheme is compared with IPDA, ICPDA, and PEPPDA in terms of communication overhead, accuracy, and energy consumption. Simulation results show that the proposed scheme achieves better performance than other schemes by reducing the communication overhead and checking the integrity of aggregated data without the delay of aggregated data. It also increases the network lifetime by eliminating the redundant data transmitted from each sensor node.

Keywords: *Data aggregation, Wireless Sensor Networks, Privacy, Complex Numbers, Integrity.*

1. INTRODUCTION

Wireless sensor networks (WSNs) are presented their abilities in many vital applications such as wildlife tracking, checking heart rates of human, military applications, traffic monitoring, etc,[1]. Wireless sensors have limited resources, including limited storage, limited processing facility, and communication capability. In addition, each sensor node is powered by a battery, which has a finite size and cannot be recharged or replaced due to environmental conditions [2-5]. Actually, Sensor nodes depend on their finite resources to survive. Due to these reasons, it is important to enhance the energy efficiency of nodes to improve the quality of the application service [6-8]. The first problem of WSNs is to minimize energy consumption in it. Because the amount of energy consumed for the communication is the greatest, thus it is essential to reduce communication overhead. The cost of communication can be reduced by sending the required and partially processed data is more significative than transmitting a large amount of raw data. Generally, sensor nodes consume energy due to sending raw data because duplicated messages are transmitted to the same sensor node,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

known as implosion, besides neighboring nodes receives the duplicated messages if two sensor nodes observing the same region, called overlapping. In recent years, data aggregation mechanisms have been proposed to combine data coming from many sensor nodes. A part of this technique is in-network aggregation, which aggregates data sequentially as data are passed through WSN [9-10]. It can also reduce the number of data transmissions and the number of sensor nodes engaged in collecting data from a WSN. Several data aggregation techniques are offered to reduce the amount of transmitting data through the WSN operations [11-14]. This problem can be also solved by employing the suitable techniques of the WSN topology. Generally, two network topologies are used in wireless sensor networks to avoid the long range of communication. The first topology is known as the *self-organized* network. This WSN topology is a temporary autonomous and multi-hop system. The design of the *self-organized* network is simple and dynamic, but each sensor node consumes huge amounts of power in data transmissions through the network [15] Figure 1 . The second topology is known as the *clustered network*. This clustered topology is presented to manage the distribution of the wireless sensors. The entire wireless sensor network is partitioned into non-overlapping clusters. Each cluster has an aggregator node (cluster head) to receive sensed data from other sensor nodes and forward these data to the remote base station. However, the energy utilization remains one of the major difficulties to the dissipation of this technology. So, an energy efficient mechanisms are required and must be designed for sensor nodes and then for clusters and to extend the network lifetime.So, LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is one of the leading protocols that is applied to reduce the consumed energy within the cluster topology. It performs its operations based on the routing method of the sensed data among the sensors nodes [16].

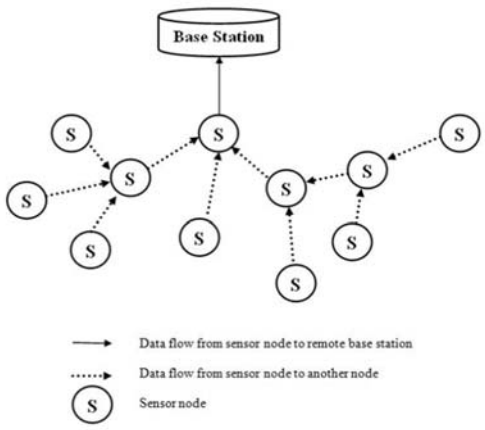

Figure 1. Self-organized network

The second problem of WSNs is how to preserve the privacy of the reading data from an adversary [17-18]. The confidentiality of data in many scenarios can be considered critical. For example, the sensors might track the movement of the enemy in military application and transmit immediate messages to the base station. Since data are transmitted wirelessly between sensor nodes, it is usually prone to eavesdropping and interception. It is important to maintain the privacy of data among sensor nodes even from trusted cooperating sensor nodes of the WSNs. It is necessary to prevent recovering the privacy of the data, even it is overheard or decrypted by the adversaries.

The last problem of WSNs is data integrity [19] . Data integrity is defined as the correctness of messages without injection a false data by an adversary. It is ensured that the received message is not modified or altered through its transmission by noise or by an adversary. If the data message is polluted by a noise it can be handled by using some mechanisms such as Cyclic Redundancy Checking (CRC). This unintentional process is out of our scope of this paper. The data aggregation result is essential for making a critical decision, thus it is required to verify data aggregation result before accepting it.

Generally, the success of wireless sensor network depends on a vital secure data aggregation technique that accomplishes the security goals [16]. However, the security models and protocols of sensor networks are different from those that are used in other types of networks due to their hardware resources and power constraints. Therefore, efficient, secure data aggregation techniques are required to deal with energy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

efficiency, data accuracy, latency and protecting data.

In this paper, we introduce a better framework schema to provide end to end confidentiality, data freshness, authentication and integrity aggregation in WSNs. The proposed technique depends on three modules. First module is using our modified version of LEACH protocol that achieves better performance in enhancing the energy consumption in WSN. The second module is the reduction method that used to avoid aggregating redundant data from sensor nodes. The third module uses the complex number properties to protect the sensitive data. It ensures that data are covered from other nodes and adversaries during transmissions to the base station. Sensitive data are transformed into a complex number and aggregated by aggregator nodes. After that base station receives the aggregated data and verifies the final aggregation result to ensure the integrity of the result. Also, a novel method is presented for eliminating redundant encrypted data during aggregation without decryption is presented. The rest of the paper is organized as follows. In section 2, includes the related work. In section3, the proposed data aggregation scheme is presented. In addition, the analysis and simulation results are represented in section 4. Finally, we conclude our work in section 5.

2. RELATED WORK

Based on nodes' types in the network, the privacy-preserving protocols are divided into two types, homogeneous protocols, and heterogeneous protocols. In homogenous protocols, all sensor nodes have the same resources, and the aggregator node performs sensing, aggregating and transmitting the aggregation result to the sink. All sensors can play the role of aggregator node. In heterogeneous, there is more than one type of sensor node and aggregator node is a special node that does aggregation and transmitting the aggregation result but not sensing the environment.

There are two main techniques, providing a secure data aggregation in WSN [2,20,21], Both of these techniques Hop-by-hop and end to end encryption techniques. In hop by hop, the protocols presented under this technique are exposed to attacks because the data are encrypted and decrypted at each forwarding node. Once a compromised sensor node decrypts the data, an adversary can easily reveal the sensory data received by this compromised sensor nodes. In addition, the adversary can inject false information into the data. Hence, expensive secure algorithms are needed to solve this problem causing a lot of overheads for both of the communication and the aggregation computation. In the end to end data aggregation techniques, aggregation is carried out on encrypted data rather than the plain text in hop by hop encrypted data aggregation techniques which achieve an end to end confidentiality.

The homogenous and heterogeneous techniques are divided into different types: Perturbation, Shuffling, Privacy homomorphism and hybrid. The perturbation is considered as a data customization. In this technique, every sensor node hides its sensed data before transferring it to its parent using an encryption key or seeds generated by randomization techniques [22]. A lot of woks are proposed for perturbation in homogenous and heterogeneous techniques [23-26].In shuffling technique, every sensor node slice its sensed data into a fixed number k and one piece is kept in the sensor node itself. The remaining k-1 slices are encrypted and transmitted to the k-1 number of neighboring sensor nodes. After that, every sensor node gathers the received data pieces contains its own piece of data and sends the aggregated data to a parent node, IPDA [27]. In privacy homomorphism technique, a special feature is used. It allows arithmetic operations to be done on the ciphertext without decryption, so it minimizes the energy consumption at the aggregator node [28-29], and our proposed schema belongs to this technique. The hybrid technique achieves privacy-preserving data aggregation by using more than one of the previous techniques [30].

In the previous section, we presented three important issues of WSNs, energy consumption, privacy and integrity of data. However, the following techniques provide both privacy preservation and data integrity, but they still support weak data integrity and privacy.

The first aggregation technique has been introduced without privacy and integrity [31]. These techniques offered based on the aggregation functions such as count, sum, and average. However, this technique is followed by several of secure aggregation techniques. The first technique was an integrity-protecting private data aggregation (iPDA) scheme [27]. In iPDA, data privacy is accomplished through data slicing and assembling

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

technique. On the other hand, data integrity is achieved using redundancy by creating disjoint aggregation paths/trees to assemble data of interests. For iPDA operation, every sensor node slices its sensed data randomly into m pieces and m-1 pieces. These pieces are encrypted and transmitted to the randomly selected sensor nodes of the aggregation tree storing one piece at the same sensor node. Each sensor node uses a different aggregation tree. When the encrypted data slices received by other nodes, they are decrypted, sum with a data slice of the receiving node. Next, the sum value is transmitted to the parent node according to the aggregation tree. Also, the summation of data from another group of sensor nodes has been sent to the base station through another aggregation tree. Finally, the aggregated data from two node disjoint aggregation trees have been compared at the base station. Base station accepts aggregated results only if the difference between the two trees does not contrast with the threshold value, otherwise, the aggregated result is rejected. This technique generates high traffic in the WSN to achieve data privacy which badly affects the communication cost. In addition, every sensor nodes have to decrypt all the slices received before aggregation causing more communication overhead.

Another technique known as iCPDA scheme was applied to a cluster network topology [32]. It has three rounds of interactions. First, every sensor node transmits a seed value to other cluster members, next, each node uses this seed value to hide its sensory data after that each sensor node transmits its hidden data to each cluster member. Then each sensor node adds its own hidden sensory data to the received hidden data and transmits the calculated aggregation results to its cluster head. Cluster head calculates the aggregation data of its member nodes via inverse and multiplication of matrices. This protocol suffers from some disadvantages. The communication overhead has increased periodically with the cluster size. The Use of large matrix effects on the computational overhead.

Also, PASKOS scheme is presented to achieve the privacy of the sensor nodes [33]. This scheme uses a hash function to compute a secret keyed value and added it to its sensed data value. It uses a modular arithmetic. Thus, the computations of the aggregation and randomized values (sensed data + secret keyed value mod m) have done using it. Next, all leaf nodes send their new value to their parent nodes. Parent nodes (non-leaf nodes) aggregates all received values. It is a hop by hop aggregation data type that does not achieve the end to end confidentiality and more communication overhead.

In [34] IPSDA they support privacy-preserving data aggregation and integrity checking by using an additive property of complex numbers. The real part has used to hide the sensed data of a sensor node from its neighboring nodes and attackers, whereas the imaginary part has used for integrity checking at both intermediate aggregators and the base station. Checking the integrity at each aggregator node effect on the energy consumption of aggregator that effects on network lifetime. This technique also doesn't preserve the end to end confidentiality.

In [35] authors proposed PEPPDA (Power Efficient Privacy-Preserving Data Aggregation) scheme to guarantee the privacy, authenticity of individual sensed data as well as the accuracy and confidentiality of the aggregated data without introducing a significant overhead on the battery limited sensor. This scheme is suitable for secure of military applications. The scheme has evaluated and simulated against privacy, authenticity, accuracy, the end to end confidentiality, and energy efficiency during data aggregation. Nonetheless, PEPPDA scheme doesn't consider data integrity, data freshness. In addition, it adds a computational overhead on each leaf node because they perform numbers of the encryption operation.

In [36] authors proposed an approach to preserve the integrity of the aggregation result. Their algorithm based on the elliptic curve discrete logarithm problem. However, of their work, it doesn't consider meeting security requirements such as confidentiality, source authentication, and availability. In [37] authors proposed a secure data aggregation scheme based on the homomorphic MAC, which is robust against eavesdropping and stealthy attacks. They evaluated and simulated their work against accurate aggregation results. Disadvantages of their work don't check source authentication, data freshness and only applied to the secure aggregation scheme for sum queries only. All the previous schemes have high communication overhead because they ignore the elimination of the redundant data.

Hence, in this research paper, we proposed an efficient, secure data aggregation scheme that supports both data privacy and integrity in terms of communication overhead, accuracy, and energy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consumption. The proposed scheme avoids also the transmitting of redundant data. It depends on algebraic properties of a complex number, which ensures the privacy of data and provides checking the data integrity of the aggregated value of the sensor nodes. Using complex numbers properties is more suitable than using asymmetric cryptography in WSNs, because it takes too many resources.

3. THE PROPOSED DATA AGGREGATION TECHNIQUE

The framework of the proposed scheme for the secure data aggregation is fulfilled based on a three modules. The first module is the type of the implemented WSN topology. The second module includes the reduction method used to minimize the transmitted data over the network. The last method includes the applied technique for the data aggregation method and securing the data during their Transmission. In the following subsections, each module will be explained and clarified.

3.1. Network Topology

We suppose a large number of sensor nodes to form a query-based WSN. Nodes will be organized as a cluster topology based on our modified version [38] of LEACH (Low Energy Adaptive Clustering Hierarchy) protocol [39] where base station locates in the center. The clusters are arranged such that, each cluster will cover the specific region from the all areas that should be observed by the designed topology. Each cluster includes two types of sensors. The first type is a set of the sensor nodes that are used to sense and to gather the data. Each sensor node is sensed within an area on the circle shape and the radius of the circle is R . The sensor is located at the center of the circle to detect up to the range R. The second type is defined as a cluster head (aggregator) which aggregates data from its member nodes. The base station has powerful resources with transmission ranges that can cover the whole network. It can broadcast messages to all sensor nodes directly.

The operations of the proposed cluster sensor network topology are performed in successive rounds. Each round has two phases, Set-up phase and steady-state phase. The operation of both phases can be explained as follows:

- In the setup phase, sensor nodes which have a higher energy will be selected to be a cluster head in the current round. Each cluster head broadcasts an announcement message to pronounce it as a CH node. Each sensor node receives this message will reply to an invitation to join to that cluster head. So, each cluster head recognizes the number of sensor nodes that will join to it.
- Steady-state phase, this phase is broken into frames, where each sensor node belongs to a cluster sends its data at most once per frame during its slot time.
- In each round, new cluster heads are selected to form a new cluster. Thus, the network lifetime can be calculated based on the number of rounds.
- However, the LEACH disadvantage is deduced from the clusters of a minor number of nodes in a steady state phase. These clusters will drain more energy than other clusters of larger nodes. Because the frequency of sending their data is more than others.

So, the improved TDMA schedule is proposed in four steps to solve this problem see Figure 2.

- Step 1. Each cluster head calculates the number of sensor nodes allocated to its cluster based on the number of receiving requests.
- Step 2. Each cluster head broadcasts a message contains the number of its attached nodes to the entire cluster heads in the WSN. At this end, each cluster head recognizes the largest capacity cluster.
- Step 3. The capacity of the largest cluster is designated to be the implemented duration of the TDMA schedule in all clusters through the steady-state phase.
- Step 4. According to modified TDMA in steady state phase, each sensor node within each cluster has a chance to send the same amount of data to their cluster heads. Thus, all sensor nodes will consume the same amount of energy. Clusters that hold a small number of sensor nodes after sending their data will go into the sleep mode during the remaining time of steady state phase.

The aggregation is performed based on this modified version of LEACH protocol. Each sensor node collects its sensory data and sends them to the aggregator (cluster head) through the steady-state phase. A sum aggregation is performed on the environmental readings.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

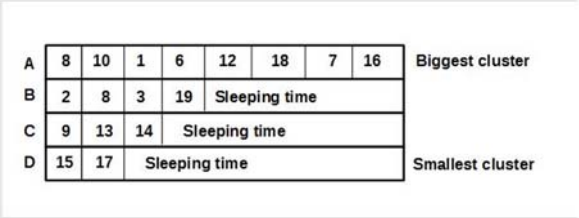

Figure 2. Modified TDMA Schedule

3.2 Reduction Method

Data aggregation has needed to reduce the energy consumption spend on transmission and computation operations. So, there are sensor nodes designed to act as a data aggregator to aggregate data packets from their neighboring nodes. In each round, another sensor node may act as a data aggregator depends on its residual energy to balance the energy utilization among sensor nodes. On the other hand, sensor nodes encrypt their environmental readings before sending it. In addition, the base station should not receive the data from a single sensor node, but from the whole network region. So, the objective of the proposed technique is to achieve an accurate and secure data aggregation. Hence, In order to minimize the number of the transmitted sensors within each cluster, the following method is proposed:

In each round, when the sensor nodes have data that will be sent to the aggregator, the following procedures are performed:

- Computes the Euclidean distance between the centers of each both of the neighboring sensor nodes.
- Compares between the computed distance and the sensing range of the both sensor nodes. If the computed distance is equal or less than the sensing range, this means that the detecting circle of both sensors is overlapped. So, only one of them is selected to send the data to the aggregator.
- The selection is performed based on:The maximum residual energy in each of the compared sensors nodes. The shortest distance between each of the compared sensors nodes and the aggregator. If the computed distance greater than the sensing range, this selection is excluded.

When there is a conflict between the two selection aspects, one of them should be preferred. So, the priority is gained to the sensor node that has the shortest range to the aggregator. The selection of set of sensor nodes only among all the sensor nodes to send the sensing data will aim to a two main benefits:

- Firstly, it saves the energy of the sensor nodes that will avoid sending data.
- Secondly, it minimizes the amount of transmitting data within the cluster.

So, the proposed method, not only save the energy, but, a considerable form of the aggregation will be accomplished in each cluster when gathering the data from the sensor nodes.

3.3 Secure Data Aggregation Technique

The key distribution that used in the proposed aggregation technique is similar to the ESPDA protocol [40] used for cluster topology. Each sensor node in the network is assigned with a secret key (K) that is a shared key. Another key is assigned to each sensor node named specific key (K_i) that is a built in key to avoid the dispersion of secret key of the whole sensor nodes in the network. Each sensor node has a unique ID_i which considered as a signature of sensor nodes. This information is stored in the sensor node before the deployment see Figure 3.

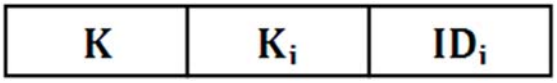

Figure 3. keys in sensor node.

The base station is also assigned with a secret key (K), a session key (k_s) and $(ID_i$ -$K_i)$ pairs of the whole sensor nodes in the sensor network are shown in Figure 4.

For each round,

- When the base station wants data from sensor nodes, a session key is established by it.
- Then, it broadcasts the session key and additional information used to verify the integrity of the aggregated data to all sensor nodes in the network using a shared key K.
- Once a sensor node receives a message containing session key k_s. It decrypts the message to get the session key and additional information.
- Sensor node establishes its own encryption key by XOR ing the session

Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

key k_s with sensor node specific key K_i.

$$K_{ei} = K_i \oplus k_s \quad (1)$$

K	K_s	$ID_i - K_i$

Figure 4.Keys in Base station

The base station is then received the aggregated sensed data from aggregators nodes. It first configures the K_i of the sender sensor node by using ID_i of the sender and the aggregator nodes. Then it generates the decryption key by XOR-ing the K_i with the session key. The confidentiality, authentication, and data freshness are achieved by the use of encryption and decryption key for each session.

Generally, the aggregation process uses functions, such as addition, subtraction, mean and exclusive or to eliminate redundant data and reduce the cost of the data transmission. However, In [25], an additive property of complex numbers is used to aggregate the sensed data in WSNs. It is used to achieve the integrity protection of the sensed data. The data is transmitted in the form of a complex number $\boldsymbol{C_i = (a_i + b_i i)}$:

Where:

$\boldsymbol{a_i}$: is the real part and used to mask the sensed data of sensor node **i** from other neighboring nodes in the cluster and adversaries.

$\boldsymbol{b_i}$: is a real number having i for sensor node **i**.

$\boldsymbol{b_i i}$: is the imaginary part and used for checking the integrity at the aggregator and the base station.

The proposed technique modified the previous formula. The modifications occurs on both a and b. They computed on different ways than [25]. These modifications ensure more security on the transmitted data. It also avoids the decryption operation on the aggregator node. Decryption operation will be performed only at the base station.

The proposed technique consists of four phases: ***Setup***, ***Encryption-Sign***, ***Aggregation***, and ***Verification***. The ***Setup*** phase is to prepare each sensor node and the base station in the network for storing all necessary secrets information besides keys. After that, Sensors will be organized as a cluster topology. Wherever a sensor node is ready to send its sensed data to its aggregator, it performs ***Encryption-Sign*** phase. Subsequently, an aggregator received all the sensed data from its sensor nodes. It performs ***Aggregation*** phase. It aggregates all the received data and sends the results (aggregated cipher-text and aggregated signature) to the base station. The final phase is the ***Decrypt-verify.*** The base station checks the authentication and the integrity of the received aggregation results. It extracts the individual reading data and decrypting the aggregated results. The four phases are explained as follows:

Setup

- All necessary keys are stored in sensor nodes. We mentioned the types of keys installed in each sensor node before. These keys used for encryption and decryption of sensed data.
- Sensor nodes start to form a cluster topology, see Figure 5 .
- The base station wherever it wants data from the sensor nodes. It establishes an elliptic curve **EC** over a finite field $\mathbf{F_p}$ where **p** is a prime number. An elliptic curve is described by cubic equations. It is appropriate for cryptographic applications. Finite field is a set of integers of order **p** with the arithmetic operations modulo **p**.Thus the more prime number is larger the more privacy-preserving is achieved. It generates a generator point on the elliptic curve defined as **G**.

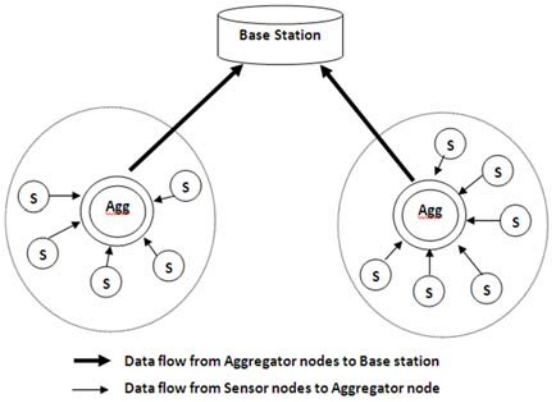

Figure 5.Cluster Topology

Encryption-Sign phase

- This phase begins when the base station sends a query for the SUM aggregation function to whole sensor nodes in the network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- It sends a message to all sensor nodes contains a prime number value defined as V_i, G, a session key k_s used for each session, and a unique private number (**UV**) as a seed for each sensor node in the network. **UV** value can be selected from an integer range between lower and upper bound. This number is private in the network. The privacy of sensed data can be increased by increasing the size of the range.
- Then, a sensor node has the ability to establish its own encryption key K_{ei}. This key is used only to encrypt the multiplication of sensed data with V_i.
- A sensor node has a reading data defined as (RD_i). It first concealed its sensed reading data in a by integrating it with a unique private value (UV_i). Then an integer value b_i is computed as follows:

$$b_i = (G \circ RD_i + V_i) * UV_i \quad (2)$$

Where:
i: recognize each sensor node.
G: is the generator point on the elliptic curve.
RD_i: is the reading data for sensor node i.
V_i: is a prime number defined by the base station for sensor node i.
$\circ$: stands for the inner product of vectors **G** and RD_i
UV_i : is a unique private value for each sensor node in the network.

- RD_i Value is decomposed into two parts RD_{i1} and RD_{i2}. Complex numbers have properties, thus it can be added, subtracted, multiplied, and divided by formally applying associative, commutative, and distributed laws of algebra. For example, the reading data **13** of sensor node **3** is encrypted into **25+84*i***. The reading data **13** is first added to **12**, where **12** is a UV_3 value. The mask value **25** is calculated. Then let a generator point **G** is equal **(5,7)**. RD_i is split into two parts **(6,7)**, $V_3 = 5$ and $b_3 i$ is calculated as follows:

$$b_3 = (G \circ RD_3 + V_3) * UV_3$$
$$b_3 = (5,7) \circ (6,7) + 5$$
$$= 84 * 12 \ mod \ 29$$
$$b_3 i = 22i$$

  - The complex number will be in the following form:

$$C_3 = 25 + 22i$$

- After that sensor nodes multiply reading data RD_i with UV_i to generate value Z_i . This value is used in the verification phase.

$$Z_i = RD_i * UV_i \quad (3)$$

  - Applying it for sensor node 3:

$$Z_3 = (6,7) * 12 = (72,84)$$

- Sensor node encrypt Z_i value using ecryption key K_{ei} and append its ID_i to it.
- The sensor node generates cipher-text (CT_i) of the reading data. It transmits the data to its aggregator node in the cluster as:

$$CT_i = (C_i, K_{ei}(Z_i) \parallel ID_i) \quad (4)$$

Where,
CT_i: is the cipher-text of sensor node i.

- The sensor node transforms the reading data into another point on the elliptic curve. Thus, it's difficult for an adversary to find the plain text RD_i even if it knows only the complex number C_i due to the factoring integer composite of large primes is difficult.

Aggregation phase

- An aggregator node receives all cipher-texts from its sensor nodes in the cluster.
- It aggregates all cipher texts.
- It adds its own sensed data to the aggregated cipher texts.
- It adds all real parts together and imaginary part together.

$$y = \sum_{i=1}^{j} C_i \quad (5)$$

$$y = \sum_{i=1}^{j} a_i + (\sum_{i=1}^{j} b_i) \ mod \ p \ \ i \quad (6)$$

Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Decrypt-verify phase

- It is the final phase, the base station receives all intermediate results sets y_{si} .
- It computes all results by aggregated them and computes the final aggregation y_i.
- Since the final aggregation result is a complex number form and the reading data is concealed with in V_i. Thus to deduce the actual final SUM value, it's required from base station to identifying the information of the contributed sensor nodes.
- The base station decided based on final results if it can accept it or refuse the results:
    - First, it computes V' that used to ensure the integrity of aggregated data. It multiply V_i with (UV_i) for each sensor node in the network.
    - Second, it decrypts all Z_i using decryption key for each sensor node and summation all Z_i.
    - Third, it computes b', if $b'=b_i$ then it accepts the result.

$$V' = \sum_{i=1}^{j} UV_i * V_i \quad mod\ p \quad (7)$$

$$Z' = \sum_{i=1}^{j} Z_i \quad mod\ p \quad (8)$$

$$b' = G \circ Z' + V' \ mod\ p \ (9)$$

The sequence flow diagram for our secure data aggregation is shown in Figure 6.

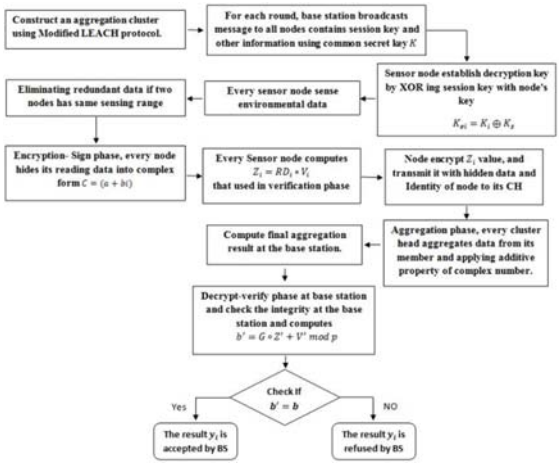

Figure 6.Sequence Flow diagram of secure data aggregation.

3.4 Security analysis

The security requirements of our scheme such as data integrity, freshness, confidentiality and source authentication are achieved for the aggregated data.

Data aggregation can be used by an attacker to violate the confidentiality of the aggregated data for example, by compromising a few sensor nodes located close to the base station. Here, we deal with this threat via using the encryption and decryption key for each session. The approach for keeping sensed data secret is to hide it into another form (complex number form) besides using the encryption secret key to encrypt the multiplier value of sensed data with private unique value, hence achieving an end to end confidentiality. However, data aggregation protocols usually cannot do aggregation process on encrypted data. Thus, such data aggregation protocols perform two steps, first it must decrypt the sensor's sensed data to perform data aggregation, and second, it encrypts the aggregated data before sending it to other upper-level sensor nodes. The encryption and decryption done on the sensor data at intermediate aggregator prevent an end to end data confidentiality besides the delay and energy consumption of these processes. As the attacker is powerful or the application is strong, the data confidentiality could be achieved by encrypting the hidden sensed data (Z_i).

Also, our proposed scheme ensures that all the received data is the original data. This is because each message of sensed data is transmitted only once from the original source, and the ID_s is attached to each message. Authentication is also achieved by encrypting the hidden sensed data (Z_i)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

with encryption key (K_{ei}). Thus a base station can easily determine the K_i of the sensor node by using ID_s of aggregator and sensor node.

4. PERFORMANCE EVALUATION

4.1 Simulation setup

In this section, we evaluate the performance of the proposed scheme in terms of security properties, communication overhead, aggregation accuracy, and energy consumption. The simulation is conducted in MATLAB 2015a to measure the performance of the scheme in terms of communication overhead and energy consumption. We considered 100 sensor nodes for simulation and one base station, which have more computational and power capabilities than sensor nodes and located at (50,175). The initial energy for each sensor node is 100 J, and other parameters are considered in **Error! Reference source not found.**. The simulation of the proposed approach is running at an average of 20 times. The proposed scheme is evaluated according to two fields: theoretical and practical.

Table 1. Simulation parameters

Parameters	Values
Area size	100m X 100m
Transmit power	660 mw
Receiving power	395 mw
Idle power	335 mw
Data packet	1024 bytes

It is important to define the security requirements of the application and to realize the risks and the consequences that can affect on the network security. In this paper, we category attack models into three sections according to their attacking methodology, and study how these attacks may be applied to affect in our proposed scheme.

Passive attacks over the wireless channel: passive attackers are concerned about eavesdropping messages transmitted over wireless channels. In the proposed scheme, the sensed data are hidden in complex number form also it's encrypted using a specific encryption key, which deals with eavesdropping. Thus, the passive attackers cannot decrypt the eavesdropped message data without knowing the decryption key. The properties of our proposed secure data aggregation for WSNs resolve the countermeasures to passive attacks.

Active attack over the wireless channel: various types of active attacks can be generated to manipulate the wireless channels and triggered with the aggregator nodes based on their limited functions. In the proposed scheme, when an attacker compromises an aggregator it cannot decrypt the aggregated cipher text or each individual ciphertext because decryption key is not stored in an aggregator. Attackers also do not have a valid signature (ID_s) to append it with broadcast messages and cannot pretend to be aggregators or the base station to trigger attacks. Thus, this proposed scheme is robust to the sinkhole and selective forwarding attacks because the attacked aggregators have the ability to ignore all the communication packets with forged node ID_s.

4.2 PERFORMANCE ANALYSIS

We evaluate our proposed scheme against iPDA, iCPDA and PEPPDA in terms of communication overhead and accuracy.

Communication overhead: is measured by the number of messages transmitted by a sensor node in a session. It is related to data aggregation, key distribution, and integrity. It is essential at an intermediate aggregator node due to expensive operations are done on it. In Figure 7 the communication overhead is shown with respect to varying number of the sensor nodes. Since the simulation is performed using a large number of sensor nodes, the number of data messages in all schemes is increased. This is because every node in the network capable of sensing data and when the number of nodes is increased, the number of messages also increases in the schemes. The proposed scheme outperforms other schemes because they generate additional unnecessary messages in the network. The reason of this that each node can customize its data by itself without needing an extra messages for data privacy and integrity checking in the network. On the other hand, In iPDA, They generate extra messages in the network for data privacy and integrity checking which generates six messages and iCPDA generates four messages this cause a high data collision due to exchange messages among sensor nodes. They also consume more energy than the proposed scheme for successful data transmission.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

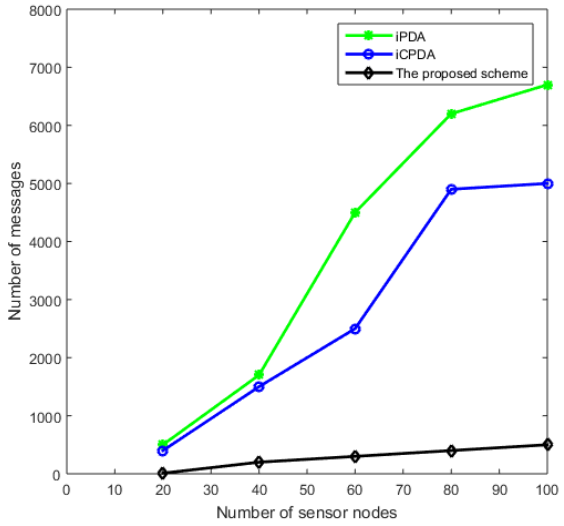

Figure 7. Communication overhead in terms of number of messages

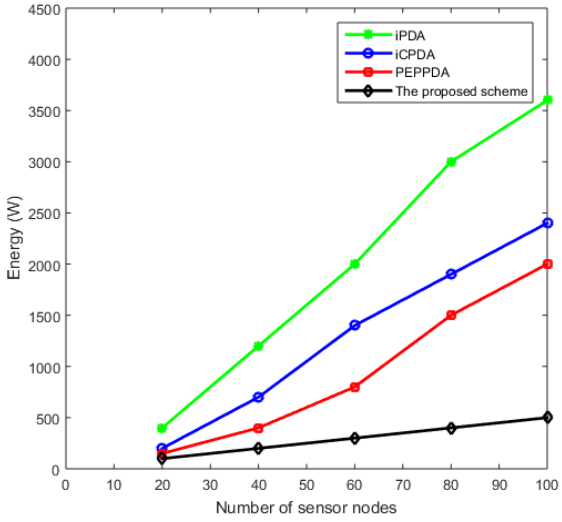

Figure 8. Communication Overhead in terms of energy consumption

The messages produced in the network are finally consumed by the base station. Therefore, the transmission and the reception of message processes are included. These processes require a considerable amount of energy. Figure 8 shows communication overhead in terms of energy consumption iPDA, iCPDA, PEPPDA, and the proposed scheme with respect to the number of sensor nodes in the network. As shown, when the number of sensor nodes is increased, the energy consumption is increased in the schemes. This is due to the generation of every message in the network needs some amount of energy to reach the base station. It is obvious that the proposed scheme is lower than other schemes due to unnecessary messages in the network while achieving privacy and integrity in data aggregation. And also every node stays active for a long period to transmit all messages. This improvement happens also by avoiding the identical readings data transmissions from sensor nodes. By eliminating identical readings, only unique data are transmitted and aggregator node will aggregate small number of data messages. Reducing the amount of transmissions saving more energy. In addition, the data transmission cost is reduced. Furthermore, the usage of the additive property of a complex number for data transmission is another factor for reducing the energy consumption.

Accuracy and data propagation delay: is defined as the ratio between the aggregated data received at the base station through the network and the actual aggregated data of all sensor data. The number of the transmitted data message of aggregation result is less than iPDA, iCPDA, and PEPPDA so the chance of causing a collision is also decreased. Another reason is the reduced number of operations of decryption and encryption at the intermediate aggregator node which causes a delay in the transmission process. It reduces the possibility of node compromising attack, so it decreases the chance of occurring alteration of the sensed data. Thus, accuracy is increased. The delay of data in iPDA, iCPDA, and PEPPDA is increased due to the number of messages that needed to communicate (e.g. transmit and receive) Figure 9. Sensor nodes in schemes needed to be active to perform all communications than the proposed scheme. The delay of data is calculated as the average time required by customizing data of nodes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to reach the base station.

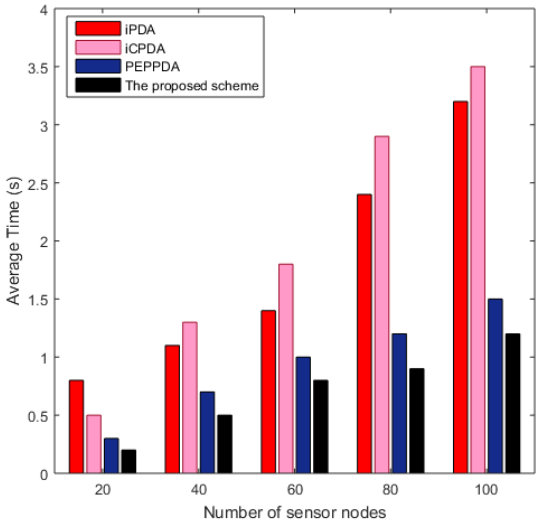

Figure 9.Data Propagation delay

5. CONCLUSION AND FUTURE WORK

In this paper, we proposed an efficient, secure data aggregation scheme which ensures the integrity of the aggregated data and can be applied on different WSNs applications. First, the proposed data aggregation scheme is based on three modules. The first one is the network topology that is used. We used our modified version of LEACH protocol. This version of LEACH protocol achieves an enhancement of energy consumption in WSN. Second module, is the reduction method that used to avoid the aggregation the redundant data from sensor node. Third module is used by applying the additive property of complex number to protect sensitive data and maintaining data privacy and integrity of aggregated data. The additive property of complex numbers is applied to perform two tasks. Firstly, it hides the sensitive data with a unique private value (real part). Secondly, it adds the real part to the imaginary part. The Imaginary part is generated by using a prime number value that used in the verification process. Thus sensed data are transformed into a complex number form before transmitting towards the sink. We protect sensed data of sensor node from being known by its neighboring sensor nodes in WSNs. It is difficult for an attacker to obtain information even its eavesdropping and decrypt data. Data integrity is achieved by using the imaginary part of the complex number those effects on the protection and ensures the integrity of data from any threats. Simulation results in terms of communication overhead and accuracy show more efficient than IPDA, ICPDA and PEPPDA.

For future work, we will improve the proposed scheme to support other aggregation functions such as MAX and MIN aggregations. We will also investigate in intrusion detection mechanisms to overcome node compromising attack.

REFERENCES

[1] Amara, S. O., Beghdad, R., & Oussalah, M. (2013). Securing Wireless Sensor Networks: A Survey. EDPACS , 47 (2), 6-29. DOI: 10.1109/COMST.2008.4625802

[2] Ozdemir, S., & Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks , 53 (12), 2022-2037. https://doi.org/10.1016/j.comnet.2009.02.023.

[3] Roy, S., Conti, M., Setia, S., & Jajodia, S. (2012). Secure Data Aggregation in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security , 7 (3), 1040-1052. DOI: 10.1109/TIFS.2012.2189568

[4] Joyce, J., Princy, M., & Jose, J. (2013). Integrity protecting and privacy preserving data aggregation protocols in wireless sensor networks: a survey. International Journal of Computer Network and Information Security , 5 (7), 66. DOI: 10.5815/ijcnis.2013.07.08

[5] Lin, Y. H., Chang, S. Y., & Sun, H. M. (2013). CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks. IEEE Transactions on Knowledge and Data Engineering , 25 (7), 1471-1483. DOI: 10.1109/TKDE.2012.94

[6] Carvalho, G., Anpalagan, A., Woungang, I., & Dhurandher, S. K. (2012). Energy-efficient radio resource management scheme for heterogeneous wireless networks: a queueing theory perspective. Energy, 3(4).

[7] Yoon, M., Kim, Y.-K., & Chang, J.-W. (2013). An energy-efficient routing protocol using message success rate in wireless sensor networks. JoC, 4(1), 15-22.

[8] Sumathi, R., & Srinivas, M. (2012). A survey of QoS based routing protocols for wireless sensor networks. Journal of Information Processing Systems, 8(4), 589-602.

[9] Madden, S. R., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2005). TinyDB: an acquisitional query processing system for sensor networks. ACM Transactions on database systems (TODS), 30(1), 122-173.

[10] Bista, R., Kim, Y.-K., & Chang, J.-W. (2009). A new approach for energy-balanced data aggregation in wireless sensor networks. Computer and Information Technology, 2009. CIT'09. Ninth IEEE International Conference on, 2, pp. 9-15.

[11] Akkaya, K., Demirbas, M., & Aygun, R. S. (2008). The impact of data aggregation on the performance of wireless sensor networks. Wireless Communications and Mobile Computing , 8 (2), 171-193. DOI: 10.1002/wcm.454.

[12] Boubiche, S., Boubiche, D. E., Bilami, A., & Toral-Cruz, H. (2016). An Outline of Data Aggregation Security in Heterogeneous Wireless Sensor Networks. Sensors , 16 (4), 525. DOI: 10.3390/s16040525.

[13] Patel, R., & Kanawade, S. (2017). Deployment of Data Aggregation Technique in Wireless Sensor Network. Proceedings of the International Conference on Data Engineering and Communication Technology, (pp. 675-680). DOI: 10.1007/978-981-10-1675-2_66.

[14] Moh'd Alia, O. (2017). Dynamic relocation of mobile base station in wireless sensor networks using a cluster-based harmony search algorithm. Information Sciences , 385, 76-95. https://doi.org/10.1016/j.ins.2016.12.046

[15] Kafetzoglou, S., & Papavassiliou, S. (2011). Energy-efficient framework for data gathering in wireless sensor networks via the combination of sleeping MAC and data aggregation strategies. International Journal of Sensor Networks , 10 (1-2), 3-13. DOI: http://dx.doi.org/10.1504/IJSNet.2011.040899

[16] Othman, S. B., Bahattab, A. A., Trad, A., & Youssef, H. (2015). Confidentiality and integrity for data aggregation in WSN using homomorphic encryption. Wireless Personal Communications , 80 (2), 867-889. DOI:10.1007/s11277-014-2061-z.

[17] Feng, T., Wang, C., Zhang, W., & Ruan, L. (2008). Confidentiality protection for distributed sensor data aggregation. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, (pp. 56-60).

[18] Taban, G., & Gligor, V. D. (2009). Privacy-preserving integrity-assured data aggregation in sensor networks. Computational Science and Engineering, 2009. CSE'09. International Conference on, 3, pp. 168-175.

[19] Jose, J., Kumar, S. M., & Jose, J. (2013). Energy efficient recoverable concealed data aggregation in wireless sensor networks. Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on, (pp. 322-329). DOI: 10.1109/ICE-CCN.2013.6528517

[20] Alzaid, H., Foo, E., & Nieto, J. G. (2008). Secure data aggregation in wireless sensor network: a survey. Proceedings of the sixth Australasian conference on Information security-Volume 81, (pp. 93-105).

[21] Jha, M. K., & Sharma, T. (2011). Secure data aggregation in wireless sensor network: a survey. International Journal of Engineering Science and Technology, 1(3), 2013-2019.

[22] Kargupta, H., Datta, S., Wang, Q., & Sivakumar, K. (2003). On the privacy preserving properties of random data perturbation techniques. Data Mining, 2003. ICDM 2003. Third IEEE International Conference on, (pp. 99-106).

[23] Sheng, B., & Li, Q. (2008). Verifiable privacy-preserving range query in two-tiered sensor networks. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, (pp. 46-50).

[24] He, W., Liu, X., Nguyen, H., & Nahrstedt, K. (2009). A cluster-based protocol to enforce integrity and preserve privacy in data aggregation. Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on, (pp. 14-19).

[25] Yoon, M., Kim, Y.-K., & Chang, J.-W. (2013). A new data aggregation scheme to support energy efficiency and privacy preservation for wireless sensor networks. International Journal of Security and Its Applications, 7(1), 129-142.

[26] Kim, Y.-K., Lee, H., Yoon, M., & Chang, J.-W. (2013). Hilbert-curve based data aggregation scheme to enforce data privacy and data integrity for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(6), 217876.

[27] He, W., Nguyen, H., Liuy, X., Nahrstedt, K., & Abdelzaher, T. (2008). iPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks. Military Communications Conference, 2008. MILCOM 2008. IEEE, (pp. 1-7).

[28] Castelluccia, C., Mykletun, E., & Tsudik, G. (2005). Efficient aggregation of encrypted data in wireless sensor networks. Mobile and Ubiquitous Systems: Networking and Services,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2005. MobiQuitous 2005. The Second Annual International Conference on, (pp. 109-117).

[29] Kumar, M., Verma, S., & Lata, K. (2015). Secure data aggregation in wireless sensor networks using homomorphic encryption. International Journal of Electronics, 102(4), 690-702.

[30] Conti, M., Zhang, L., Roy, S., Di Pietro, R., Jajodia, S., & Mancini, L. V. (2009). Privacy-preserving robust data aggregation in wireless sensor networks. Security and Communication Networks, 2(2), 195-213.

[31] Fung, W. F., Sun, D., & Gehrke, J. (2002). Cougar: the network is the database. Proceedings of the 2002 ACM SIGMOD international conference on Management of data, (pp. 621-621).

[32] He, W., Liu, X., Nguyen, H., & Nahrstedt, K. (2009, June). A cluster-based protocol to enforce integrity and preserve privacy in data aggregation. In Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on (pp. 14-19). IEEE.

[33] Zhang, L., Zhang, H., Conti, M., Di Pietro, R., Jajodia, S., & Mancini, L. V. (2013). Preserving privacy against external and internal threats in WSN data aggregation. Telecommunication Systems, 52(4), 2163-2176.

[34] Yoon, M., Jang, M., Kim, H.-I., & Chang, J.-W. (2014). A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks. International Journal of Distributed Sensor Networks.

[35] Jose, J., Princy, M., & Jose, J. (2013). PEPPDA: Power efficient privacy preserving data aggregation for wireless sensor networks. Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on, (pp. 330-336).

[36] Zhu, L., Yang, Z., Li, M., & Liu, D. (2013). An Efficient data aggregation protocol concentrated on data integrity in wireless sensor networks. International Journal of Distributed Sensor Networks.

[37] Zhou, Q., Yang, G., & He, L. (2014). An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks. International Journal of Distributed Sensor Networks, 10(1), 962925.

[38] Elshrkawey, M., Elsherif, S. M., & Wahed, M. E. (2017). An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Networks. Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2017.04.002.

[39] Heinzelman, W. B. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications , 1 (4), 660-670. DOI: 10.1109/TWC.2002.804190

[40] {\c{C}}am, H., {\"O}zdemir, S., Nair, P., Muthuavinashiappan, D., & Sanli, H. O. (2006). Energy-efficient secure pattern based data aggregation for wireless sensor networks. Computer Communications, 29(4), 446-455.

Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPENDIX A

An Example

Let generator point on the elliptic curve $G = (5,7)$ defined over finite field $F_{29}$and $p = 29$. Suppose we have 7 sensor nodes, two of them are aggregators' nodes, node 1 and node 2. First cluster contains 4 sensor nodes (1, 3, 5, 7) and second cluster contains 3 sensor nodes (2, 4, 6). According to **Error! Reference source not found.** we have the reading data for each sensor node and complex number form for each sensor node. To generate imaginary part data for each sensor node, we first split each reading value into two parts and then using equation 2 to deduce bi.

Encryption-Sign:

- For cluster 1, data for each sensor node that will be transferred is:
  $C_1 = (19+13i, K_{e1}(Z_1) \parallel ID_1)$
  $C_3 = (14 + 18i, K_{e3}(Z_3) \parallel ID_3)$
  $C_5 = (24 + 2i, K_{e5}(Z_5) \parallel ID_5)$
  $C_7 = (25 + 2i, K_{e7}(Z_7) \parallel ID_7)$
- For cluster 2:
  $C_2 = (22+18i, K_{e2}(Z_2) \parallel ID_2)$
  $C_4 = (20+1i, K_{e4}(Z_4) \parallel ID_4)$
  $C_6 = (30+24i, K_{e6}(Z_6) \parallel ID_6)$

Aggregation phase

Each aggregator aggregates received data from its cluster members:

- For cluster 1, cluster head node 1 will aggregates its data with the received data from its members:

$$y_{1,3,5,7} = C_1 + C_3 + C_5 + C_7$$

$$y_{1,3,5,7} = (82 + 62\ mod\ 29\ i, K_{e1}(Z_1) \parallel ID_1 + K_{e3}(Z_3) \parallel ID_3 + K_{e5}(Z_5) \parallel ID_5 + K_{e7}(Z_7) \parallel ID_7)$$

$$y_{1,3,5,7} = (82 + 4i, K_{e1}(Z_1) \parallel ID_1 + K_{e3} \parallel ID_3 + K_{e5}(Z_5) \parallel ID_5 + K_{e7}(Z_7) \parallel ID_7)$$

- For cluster 2, node 2 is responsible for the aggregation process:

$$y_{2,4,6} = C_2 + C_4 + C_6$$

$$y_{2,4,6} = 72 + 43\ mod\ 29\ i, K_{e2}(Z_2) \parallel ID_2 + K_{e4}(Z_4) \parallel ID_4 + K_{e6}(Z_6) \parallel ID_6$$

$$y_{2,4,6} = 72 + 14i, K_{e2}(Z_2) \parallel ID_2 + K_{e4}(Z_4) \parallel ID_4 + K_{e6}(Z_6) \parallel ID_6$$

After that, each cluster head sends the aggregated data to the base station to decrypt and verify the aggregated data. The base station receives $y_{1,3,5,7}$ and $y_{2,4,6}$. First base station determines the K_i for each sensor node by using $ID_i s$ of the aggregator and the sender node. Then it generates the decryption key by XOR ing node specific key with the session key transmitted by it to the network. Thus a base station can configure the Z_i value for each sensor node. It computes Z' by summation all Z_i value.

$$y = y_{1,3,5,7} + y_{2,4,6}$$

$$y = (154 + 18i, K_{e1}(Z_1) \parallel ID_1 + K_{e3}(Z_3) \parallel ID_3 + K_{e5}(Z_5) \parallel ID_5 + K_{e7}(Z_7) \parallel ID_7 + K_{e2}(Z_2) \parallel ID_2 + K_{e4}(Z_4) \parallel ID_4 + K_{e6}(Z_6) \parallel ID_6$$

Thus $b = 18$

$$Z' = Z_1 + Z_2 + Z_3 + Z_4 + Z_5 + Z_6 + Z_7$$
$$Z' = (11,2)$$

A Base station at the beginning of each session, it sends a prime number value and a unique private value to every sensor node in the network. Thus, it can deduce V' by multiplying each prime number belongs to the sensor node with unique private value for each sensor.

$$V' = \sum_{i=1}^{j} UV_i * V_i\ mod\ 29$$

$$V' = (2 * 5) + (3 * 7) + (1 * 3) + (5 * 2) + (8 * 13) + (9 * 11) + (7 * 3)$$
$$V' = 268\ mod\ 29 = 7$$

$$b' = G \circ Z' + V'\ mod\ p$$
$$b' = (5,7) \circ (11,2) + 7 = 76\ mod\ 29 = 18$$

$$b' = b\ without\ i$$

Hence, the result y (real part data) is accepted. Here base station can easily deduce the actual aggregated data from every sensor by subtracting real part data with the summation of all unique private values of every sensor node.

$$actual\ aggregation = 154 - \sum_{i=1}^{j} UV_i$$
$$actual\ aggregation = 154 - 35 = 119.$$

The final aggregation result is always accurate and reliable because of two reasons. First, by using a complex number form which is an algebraic expression and thus the underlying algebra gives an accurate result of the aggregated data from sensor

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes. Second, since the unique private value is fixed integer values, not random numbers after the base station collects data it can easily subtract exactly the same data values that have been added to the sensor reading value during data hiding process by every sensor node.

ID_i	RD	(RD_1, RD_2)	UV	$a = RD + UV$	V	bi	Complex form	$Z_i = RD_i * UV_i$
1	17	(8,9)	2	19	5	$13i$	$19+13i$	(16,18)
2	19	(9,10)	3	22	7	$18i$	$22+18i$	(27,1)
3	13	(6,7)	1	14	3	$24i$	$14+24i$	(6,7)
4	15	(7,8)	5	20	2	$1i$	$20+i$	(6,11)
5	16	(8,8)	8	24	13	$2i$	$24+2i$	(6,6)
6	21	(10,11)	9	30	11	$24i$	$30+24i$	(3,12)
7	18	(9,9)	7	25	3	$23i$	$25+23i$	(5,5)

Table 2. Example