Wireless Personal Communications (2021) 119:2675–2694
https://doi.org/10.1007/s11277-021-08351-0

VEDSDA: Voronoi Encryption and Decryption for Secure Data Aggregation in WSNs

S. Reshma[1] · K. Shaila[2] · K. R. Venugopal[3]

Accepted: 19 February 2021 / Published online: 27 May 2021

Abstract

The various application in Wireless Sensor Networks fascinated towards minimal and secure data transmission. In this paper, VEDSDA protocol is proposed to achieve reduction of data redundancy, data length and providing security for data transmission. The VEDSDA protocol used compression technique to reduce data length which helps to utilize less energy consumption. The data compression technique involves leveling, encoding and decoding phases. Levelling phase converts data to logical data where as encoding phase compress the data size at the source node and decoding phase decompress the data size at the destination. The voronoi diagram concept is used to encrypt and decrypt aggregated data. Thus, VEDSDA protocol is compared with existing protocol and proves better enhancement.

Keywords Decryption · Environmental monitoring · Encryption · Military surveillance · Voronoi diagram · Wireless sensor networks

1 Introduction

Sensor motes are limited resource reserved devices that are grouped together to form Sensor Networks. WSNs are applied in broad applications viz., military surveillance, environment monitoring, disaster recovery, etc. The VEDSDA protocol is focused on monitoring environment temperature and collectively transmits sensed data to BS In this scenario, WSNs are concerned about various challenges namely energy, limited bandwidth, node costs, deployment, security, time synchronization [1, 2].

The sensor node senses information and forward it to the destination via intermediate nodes. The intermediate node minimizes redundant data using max, min, avg and several aggregation functions before forwarding sensed data to the BS. In general, data aggregation strategies are classified into two categories i.e., structure based and

✉ S. Reshma
reshmam211@gmail.com

[1] Department of CSE, VTU-RRC, Belagavi, Karnataka, India

[2] Department of ECE, VKIT, Bengaluru, Karnataka, India

[3] Bengaluru University, Bengaluru, Karnataka, India

structure free protocol [3]. The structure-based protocol is flat, cluster, grid and tree-based protocols. In these protocols, data aggregation is done during the transmission phase whereas in structure-based protocols data aggregation is done in early phase irrespective of network size. Thus, there is no guaranteed packet delivery in structure free protocol [4].

In the cluster-based protocols [5–7], the redundant data is aggregated at the Cluster Head (CH) and in turn, CH is responsible for successful packet delivery to the BS using multiple hops via., other CH s. In [8, 9], protocols are designed to elect a cluster head using residual energy and thus this process minimizes energy consumption [10–12].

The nodes actively participating in the network are exposed to numerous attacks. For example, malicious nodes can enter into the network easily, rival nodes can misguide trust worthy node present in the network and may cause congestion; Attacks on secrecy and authentication, attacks on network availability, stealthy attack against service integrity [13–15]. The various cryptographic mechanism for WSNs guarantees data delivery to the Base Station. There are two cryptographic techniques namely public key cryptography and symmetric key cryptography. The proposed protocol focuses on public key cryptography, which obtains public key and private key using voronoi diagram.

1.1 Motivation

Since sensor nodes are limited energy constraint device, utilization of energy in an efficient methodology is a challenging task. In addition to energy, detection of legitimate node for successful data delivery is an added constraint in WSNs. Therefore, it is essential to propose a secure data aggregation protocol to improve successful packet delivery and energy efficiency.

1.2 Contribution

The proposed protocol provides security for aggregated data. VEDSDA Encryption phase involves three steps viz., Levelling, Encode and Encryption. Data aggregation phase aggregates data by eliminating redundant data using XOR function, the aggregated data is then compressed using VEDSDA compression function which utilizes less energy for data transmission. VEDSDA decryption phase involves three steps viz., Levelling, Decode of data and Decryption. Data Encryption and Decryption uses private key and public key computed using voronoi technique. Hence, time complexity for computation is decreased compared with other existing cryptography algorithm and consumes less energy.

1.3 Organization

Section 2 presents description of existing works and background work is explored in Sect. 3. The problem definition and objectives are discussed in Sect. 4 wherein Sect. 5 gives detail description on system and mathematical model of proposed protocol. Section 6 presents performance metrics and performance evaluation. Conclusions is then encapsulated in Sect. 7.

2 Related Work

This section discusses existing secure data aggregation protocols methodology, advantage and disadvantages.

Castelluccia et al. [16] proposed a homomorphic encryption strategy. This scheme aggregate a data which is encrypted based on the statistical values viz, mean, variance and standard deviation of the sensed data. This scheme encrypts data using homomorphic encryption strategy. The objective of encryption scheme is to replace the cipher text with xor (exclusive OR) operation. The encrypted data is aggregated based on statistical values viz, variance, mean and standard deviation of the sensed data utilizes less bandwidth.

Acharya et al. [17] have discussed order-preserving scheme, (OPES) for CDA (Concealed data aggregation) to improve energy and protection against ciphertext only attacks. The sensed values are sorted and splitted into buckets. The bucket size depends on different OPES stages like Model, flatten, transform. The data are mapped into flattened value and then flat values are mapped into cipher value. The flatten stage guarantees the deviation between all the values that are unknown. Thus, gives better energy distribution over the network and increases robustness and communication overhead.

Xu et al. [18] designed a new called PAVS for VSS. The vehicle senses the message and send to RSV s. RSV s verifies and classify data according to data classification algorithm. Finally, RSV s aggregates data using data aggregation algorithm. Thus, it resists sensing data link attack and increases scalability and data accuracy. It increases memory costs since it is necessary to hold long term secrets of data. Fu et al. [19] proposed Context-Aware Search Scheme in Cloud Computing. The information present in the cloud is represented as a Conceptual Graph (CG). Based on CG two schemes are presented viz., PRSCG and PRSCG-TF, these two schemes are used to search an information in a certificateless secured channel. Thus, it provides security for searching information in a cloud.

Damodar et al. [20] presented a clustering algorithm using Voronoi diagram. This algorithm computes the voronoi cells and forms cluster by grouping neighbour Voronoi cells. If similar cell points arise then similarity point is computed based on Euclidian distance. The various experiments are done using synthetic and biological datasets. The experimental results demonstrated capabilities of the projected method. Nithya et al. [21] proposed Voronoi Based Genetic Clustering (VBGC) for energy efficient data aggregation. It reduces number of bits for data transmission. Thus, improves energy efficiency. But in this algorithm CH changes for every period of time. This leads to overhead and more time complexity.

Vamsi et al. [22] presented a Secure Data Aggregation Framework for Wireless Sensor Networks. The BS detects and classifies malicious nodes from the data aggregation process. BS sends a malicious nodes information which are detected with the help of IDS and reports to all nodes in the network. Thus, this framework guarantees secure path with lesser packet loss. Annapurna et al. [23] proposed a Secure Data Aggregation with Fault Tolerance for Wireless Sensor Networks. In this approach, the sensed information from the source node is divided into multiple shares and then transmits via different paths and sensor nodes transmit redundant shares. This results in overcome packet loss. Once data received at Base Station, all the shares combine via different path to avoid malicious nodes. This approach mitigates malicious nodes but, utilizes more energy for transmitting redundant shares. Othman et al. [24] proposed novel approach for secure data aggregation using homomorphic encryption and Message Authentication Codes. Homomorphic encryption includes Elliptic Curve EIGamal algorithm to provide confidentiality for the sensed data and uses MAC computational result with pirvate key and send to cluster head. The cluster head aggregates MAC, then forwards aggregated and encrypted data to the Base Station. The Bases Station decrypts the data. Thus, minimizes communication and computation overhead.

Razaque et al. [25] proposed SDAACA protocol. The SDAACA involves two algorithms viz., Secure Data Fragmentation (SDF) and Node Joining Authorization (NJA). The SDF algorithm fragment data into small pieces where as NJA authenticates the newly entered node in the network to avoid sybil and sink hole attack. This protocol provides an increased end-to-end delay, reliability and minimum energy utilization in the presence of Sinkhole and Sybil attacks. But, the scalability of protocol is limited.

Mahimkar et al. [26] proposed a Secure Data Aggregation and Verification (Secure DAV) protocol. The sensor nodes stores and broadcasts its EC Public key/private key to all nodes among the clusters. Each cluster are assigned with the cluster key. The shared public keys/private keys and cluster keys are different and the shared cluster keys generates, partial signature. Next, cluster head accumulates all partial signature and then forwards to full signature to the Base Station. Finally, BS verifies the signature with the help of public key. SecureDAV protocol ensures that BS never accepts false data injected by malicious nodes.

Cam et al. [27] presented Energy-efficient and Secure Pattern-based Data Aggregation protocol for Wireless Sensor Networks. In this protocol, the sensor nodes forwards only non-redundant data to the CH based on the pattern code. Each sensed data has a corresponding pattern code and for the data transferred to the CH. The CH permits only unique pattern code. Therefore, CH receives only non-redundant data and it reduces minimum energy utilization. But there is a chance of missing useful information.

Sanli et al. [28] presented Secure-Reference-Based Data Aggregation (SRDA) protocol to improve energy efficiency. This protocol reduces the number of bits transmitted towards base station and secure connectivity between source and the destination. In this protocol, sensor nodes are grouped together and assigned to different deployment grids. Each sensor groups and neighbour groups are shared with local and global keys respectively, which are used to provide connectivity between local group and neighbour group of the sensor nodes. This key distribution scheme guarantees secured channel and less memory consumption.

Suat et al. [29] discussed Integrity Protecting Hierarchical Data Aggregation in Wireless Sensor Networks. This scheme distributed different encryption keys for sensor nodes to encrypt data. The sensor nodes are split into different region and keys are distributed based on region. Based on the encryption key, the base station differentiates its encrypted and aggregated data. This scheme provides data integrity and confidentiality by utilizing more amount of energy because of multiple key encryption procedure.

Ozdemir et al. [30] presented a DAR protocol for data aggregation and authentication of sensor data. This protocol detects false data injected by compromise nodes and avoids forwarding false data to the aggregator to aggregate the data. This protocol uses two subMAC to provide authentication. First subMAC used for encrypted data and the other for plain data. The aggregator aggregates both the subMAC and form two FMAC s likely to subMAC s and then transmit to Base Station through intermediate nodes. The intermediate nodes verify encrypted data integrity and provides better approach to improve security but, injects large false data leading to overhead and consumes more energy.

Shim et al. [31] proposed Secure Data Aggregation Scheme in Heterogeneous WSNs based on appropriate cryptographic primitives. The author has presented three schemes to provide security to the aggregated data viz., Sen-SDA, an identity-based signature scheme, and a batch verification technique. The Sen-SDA scheme is a combination of Homomorphic Encryption, EC-ElGamal+ and the pairing-free IBS scheme. An identity-based signature which are used to identify the nodes where as a batch verification technique finds invalid signatures in heterogeneous clustered WSNs. Thus, this protocol provides confidentiality for the sensed data.

3 Background

Zhang et al. [32] proposed MODA, CODA and RODA schemes. The raw data is sensed and received by MODA and the data compression is done by CODA to reduce energy utilization. After data compression, the redundant data is eliminated and is encoded into binary language. This encoding process formulate the encoding format with field and value. If the sensor node does not sense data then, the corresponding field value is placed with the value 0. Thus, encoding process consists of more zero elements which increases communication cost. Therefore, RODA randomly selects zero element's position and it is encrypted. So, RODA hides the position of non-zero element.

Hence, in our work, we focused on compressing data which reduces energy consumption and securing data using voronoi concept which helps to encrypt and decrypt the data. Thus, VEDSDA protocol achieves secure data aggregation.

4 Problem Definition

The network comprised of *n* number of nodes, each sensor node is having limited energy resource and nodes are grouped together and form *k* numbers of clusters in the network. Each sensor node in the network senses multiple information s, that are probably redundant ones. Therefore, redundant data transmission utilizes more energy and if the information size is large, it requires more energy for transmission. It is also necessary to secure the sensed information with limited resource parameter. The existing algorithms utilizes maximum time, energy and minimizes packet delivery ratio.

The main objective of the research work are:

(1) Effectively utilizes the energy of the network,
(2) Minimizes packet size and
(3) Maximizes packet delivery ratio.

Assumptions:

(1) Each nodes in the network senses moderate environment temperature between 30-35
(2) Initial energy level of all nodes remains same.

5 Implementation and Mathematical Model

To control the drawback of existing data aggregation, VEDSDA protocol focuses on reducing data size before data transmission and distributes encryption key to source and sink node respectively. The keys are obtained using voronoi concept which make use of minimum energy and time complexity. VEDSDA involves three phases which are depicted in Fig. 1. (1) VE phase (2) Data Aggregation Phase (3) VD phase. Algorithm 1 shows VEDSDA system flow algorithm.

Algorithm 1: VEDSDA algorithm

```
Procedure VEDSDA
    Input: $S$, a set of Sensor Nodes.
    Output: BS receives temperature data sensed by sensor nodes
    begin
        step 1: Event Generation (Senses Raw data)
            $X = d_1, d_2.d_3, d_4, , , , d_N$
        step 2: VE(S,X)
        step 3: Data_Aggregation( )
        step 4: Forwards data to BS
        step 5: VD( )
```

Lemma 1 $C \lhd S \rightarrow C \; where \; C = \sum_{i=1}^{p} S$

Proof Consider $C = \{C_1, C_2, C_3, \cdots C_M\}$ as a group of M clusters derived from a set of N sensor node, $S = \{S_1, S_2, S_3, \cdots S_N\}$. Each cluster C_i composed of p sensor nodes such that $C_i = \{S_1, S_2, S_3, \cdots S_p\}$. □

5.1 Voronoi Encryption Phase (VE Phase)

The Lemma 1 proves that p nodes are in each cluster senses environment temperature and ensures that temperature senses between 30 and 35 °C. This phase involves three steps shown in Algorithm 2 viz., (1) Levelling (2) Alpha Encoding and Compression Function (3) Voronoi Encryption.

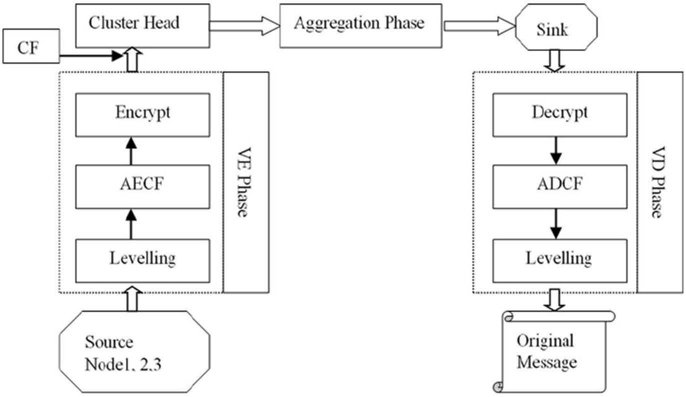

Fig. 1 VEDSDA system flow diagram

Algorithm 2: Voronoi Encryption

```
Procedure VE(S, X)
    Input: $S$ - a set of Sensor Nodes, $X$  raw data
    Output: Encrypted data
    begin
        step 1: Levelling

        for $X \leftarrow 0$ to $length(X)$ do
            if $d(i) > 30 \;\; d(i) < 35$ then
                $L = d(i) mod 0$
            else
                $L = 0$

        step 2: statistics = AEC( )
        step 3: Data_Aggregation( )
        step 4: VE(statistics, $V_PubKey$)
```

Algorithm 3: Voronoi Decryption

```
Procedure VD($R_d$, $V_SecKey$)
    Input: $R_d$  Data received form Sensor Nodes
    Output: Decrypted data
    begin
        step 1: $VD(R_d, V_SecKey)$
        step 2: ADC( )
        step 3: Levelling

        for $R_d \leftarrow 0$ to $R_d$ do
            $R_d = R_d + 30$

        step 4: VE(statistics, $V_PubKey$)
```

(1) Levelling

The sensed temperature statistics from sensor nodes are levelled using Eq. 1.

$$L(node(i)) = \begin{cases} D(i) mod\, 0 & if\, D(i) > 30\, and\, D(i) < 35 \\ 0 & otherwise \end{cases} \quad (1)$$

where $L(node(i))$ levelling value of *nodei*.

(2) Alpha Encoding and Compression Function

In the first step, the $L(node(i))$ is encoded into binary statistics. Figure 2 shows the encoding and decoding format. In Fig. 2, the fields indicate the position of levelled value. Based on levelled value, the respective fields are padded with 1 and other fields are padded with 0s.

Fig. 2 Encoding and decoding format

index	1	2	3	4	5
value					

In the second step, the binary statistics reduce energy utilization with light weight compression on Eq. 2, where α value is computed using Lemma 2. Thus, reduces number of 0 s transmitting over the network and saves transmission energy of each sensor nodes.

$$E_d(node(i)) = \alpha 0 \tag{2}$$

$$\alpha = 5\ pos \tag{3}$$

where α hides the *position* of 1 and provide security which in turn reduces the size of packet for data transmission. Thus, it helps to consume less energy during transmission phase. padded with 0s.

Lemma 2 *If* $F(i) = 1$ *then* $\alpha = index(Field(i))$.

Proof If the Field *value* is 1, then the respective field index is represented as $\alpha value$. For example, the value 1 in Fig. 3 is located under *index* 4. Therefore, consider 4 as α value. Then the statistics $\alpha 0$ are encoded as 40. □

(3) Voronoi Encryption Phase

The compressed value in phase ii is encrypted using V_{PubKey} which is computed by number of vertices in Voronoi diagram for N nodes. The V_{PubKey} is $2n - 5$ as shown in Fig. 3 source nodes header format is stored in all sensor nodes present in the network.

5.2 Data Aggregation Phase (DA Phase)

The encrypted sensed data captured from the function $V_{Enc}(E_d(node(i)), V_{PubKey})$ forwards to Cluster Head (CH). Then, the CH head aggregates data by using Exclusive-OR logic and eliminates redundant data. After aggregation, the data is forwarded to BS through intermediate CH.

5.3 Voronoi Decryption Phase (VD Phase)

In this phase, the received data from source node is decrypted in step(i) and decoded in step (ii). Finally, in step(iii) the statistical value is levelled to obtain original environment temperature.

(1) Voronoi Decryption

The base station involves in decrypting data by using V_{SecKey} stored in BS routing table (shown in Fig. 4) using Theorem 1.

Node_ID	Cluster_ID	Cluster_Head	Residual_Energy	V_{Pubkey} (2n−5)

Fig. 3 Source node routing table

Fig. 4 Base station routing table

BS_node_id	Residual_Energy	V_{SecKey} (3v+1)

Theorem 1 *The Voronoi Secret Key derives Voronoi Public Key*

$$V_{SecKey} \vdash V_{PubKey} \tag{4}$$

$$2V_{Edges} = 3V_{SecKey} \tag{5}$$

$$V_{Edge} = V_{PubKey} + N - 2 \tag{6}$$

Proof Equation 4 derives the public key using Eq. 5 and it is proved in the following steps. Equation 5 is written with assigning V_{Edge} value from Eq. 6. Equation 6 is a standard formula to obtain the number of edges in the voronoi diagram.

$$\begin{aligned}
&2(V_{PubKey} + N - 2) = 3V_{SecKey}\\
&2(V_{PubKey} + N - 2) = 3V_{PubKey} + 1\\
&\quad \because V_{SecKey} = 3v + 1 \ \mathit{and} \ v = V_{PubKey}\\
&2V_{PubKey} + 2N - 4 = 3V_{PubKey} + 1\\
&2N - 4 - 1 = 3V_{PubKey} - 2V_{PubKey}\\
&2N - 5 = V_{PubKey}\\
&\quad \therefore V_{PubKey} = 2N - 5
\end{aligned}$$

□

Theorem 1 proves V_{PubKey} derivation using V_{SecKey} to decrypt the statistics received from sensor nodes.

From Theorem 1, it is clear that the obtained V_{PubKey} is same as V_{PubKey} stored in Sensor Nodes. With this key, the encrypted statistics is decrypted.

(2) Alpha Decoding and Decompression Function

In this phase, the decrypted data is decompressed by separating integer and zero value. The obtained integer is represented as α in Eq. 7.

$$D_d = \alpha 0 \tag{7}$$

Once the decompression is completed, the data is decoded with the use of α value computed during decompression which is used to locates the exact position of $1s$

$$pos = 5\,\alpha \tag{8}$$

Based on pos value place 1 in the respective field in the encoding format and remaining fields are padded with $0\,s$. Thus, in this step, data is decoded into binary statistics. Finally, in the next step binary statistical data is levelled to original information.

(3) Levelling

The statistics computed in preceeding step is summed with integer value 30 °C to originate the original temperature sensed by the sensor nodes. The detail course of action is illustrated in a step by step procedure.

Illustration 1 In Fig. 5, given $N = 18$, $M = 3$, $P = 5$, $S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}\}$.

Step 1 According to Lemma 1, the number of sensor nodes (N) present in the network group (S) and set (S) is derived into subgroup (C). Consider cluster $C_1 = \{s_1, s_2, s_3, s_4, s_5, s_6\}$, $C_2 = \{s_7, s_8, s_9, s_{10}, s_{11}, s_{12}\}$ and $C_3 = \{s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}\}$ whereas, S_4, S_9 and S_16 are the CH for C_1 ,C_2 ,C_3 respectively.

Step 2 S_1 senses raw data 32, S_2 senses raw data 35, S_3 senses 33, S_5 senses 33, S_6 senses 28.

Step 3 Levelling (using Eq. 1)

$$\begin{aligned} S_1 &\leftarrow 32\%30 = 2 \\ S_2 &\leftarrow 35\%30 = 5 \\ S_3 &\leftarrow 33\%30 = 3 \\ S_5 &\leftarrow 33\%30 = 3 \\ S_6 &\leftarrow 28\%30 = 0(\textit{discarded}) \end{aligned}$$

Step 4 AEC Phase

(i) Encoding

$$\begin{aligned} S_1 &\leftarrow 01000 \\ S_2 &\leftarrow 00001 \\ S_3 &\leftarrow 00100 \\ S_5 &\leftarrow 00100 \end{aligned}$$

(ii) Compression

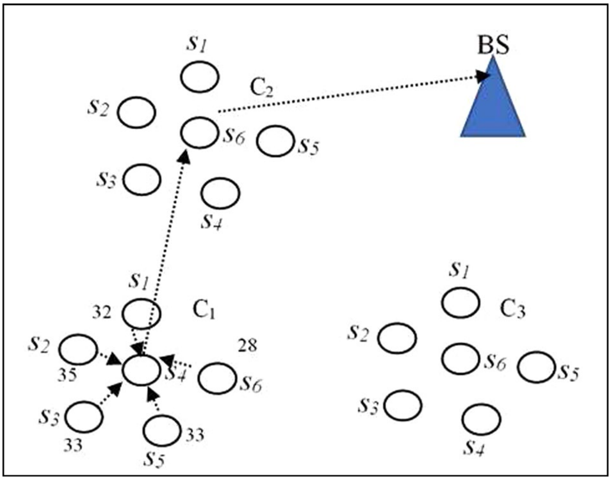

Fig. 5 Encoding and decoding format

$$\begin{aligned} S_1 &\leftarrow 20\\ S_2 &\leftarrow 50\\ S_3 &\leftarrow 30\\ S_5 &\leftarrow 30 \end{aligned}$$

Step 5 The compressed value in Step 4 is encrypted using V_{PubKey} which is computed by number of nodes in Voronoi diagram. The V_{PubKey} is $2n - 5$, standard formula to obtain the edge count in voronoi diagram.

$$\begin{aligned} S_1 &\leftarrow 20 + 2(18)\,5 = 20 + 36 - 5\\ &= 20 + 31\\ &= 51\\ S_2 &\leftarrow 50 + 2(18) - 5 = 50 + 36 - 5\\ &= 81\\ S_3 &\leftarrow 30 + 2(18) - 5 = 30 + 36 - 5\\ &= 30 + 31\\ &= 61\\ S_5 &\leftarrow 30 + 2(18) - 5 = 30 + 36 - 5\\ &= 30 + 31\\ &= 61 \end{aligned}$$

Step 6 The encrypted data from each sensor nodes are forwarded to Cluster Head. Whereas CH oversees data aggregation.

$$\begin{aligned} S_1 &= 51\\ S_2 &= 81\\ S_3 &= 61\\ S_5 &= 61 \end{aligned}$$

The CH applies Ex-XOR logic to eliminate data and hence, obtains aggregated data as 51, 81 and 61.

Step 7 The data aggregated are then forwards to the Base Station. The BS decrypts received data based on V_{Seckey}. The V_{Seckey} is derived from number of edges in Voronoi diagram. The $V_{Seckey} = 3v + 1$. From theorem 1, the proposed algorithm obtains VPubKey which is encrypted at source node with the help of V_{Seckey}. Therefore,

$$
\begin{aligned}
S_1 &\leftarrow 51 - 2(18)\,5 = 51 - 36 - 5 \\
&= 51 - 31 \\
&= 20 \\
S_2 &\leftarrow 81 - 2(18) - 5 = 81 - 36 - 5 \\
&= 81 - 31 \\
&= 50 \\
S_3 &\leftarrow 61 - 2(18) - 5 = 61 + 36 - 5 \\
&= 61 - 31 \\
&= 30
\end{aligned}
$$

Step 8 After the decryption is done, obtain α value using Eq. 7.

$$
\begin{aligned}
S_1 &= 20 \\
S_2 &= 50 \\
S_3 &= 30
\end{aligned}
$$

Hence,

$$
\begin{aligned}
\alpha_1 &= 2 \\
\alpha_2 &= 5 \\
\alpha_3 &= 3
\end{aligned}
$$

Step 9 Decode the data received from step 8 by placing 1 in the respective index and remaining padded with 0 as proved in Lemma 2.

$$
\begin{aligned}
S_1 &\leftarrow 01000 \\
S_1 &\leftarrow 00001 \\
S_1 &\leftarrow 00100
\end{aligned}
$$

Step 10 Finally, this step, level the value to numerical value and multiply with value 30 which is used to obtain mod in the first step to obtain original sensed data.

(i) Levelling

$$
\begin{aligned}
S_1 &\leftarrow 2 \\
S_1 &\leftarrow 5 \\
S_1 &\leftarrow 3
\end{aligned}
$$

(iii) Addition

$$
\begin{aligned}
S_1 &\leftarrow 32 \\
S_1 &\leftarrow 35 \\
S_1 &\leftarrow 33
\end{aligned}
$$

The obtain data from step 10 is similar to data sensed by the sensor nodes. Thus, our proposed protocol provides the security for temperature readings sensed by sensor nodes with minimum energy utilization and promising data reception at the base station without packet loss.

6 Simulation and Performance Evaluation

The VEDSDA protocol is simulated using *NS*2 and compared with MODA [38]. The simulation environment network size varies from 50 to 300 nodes respectively. The area is configured to 1000 square meters. The sink node is situated at 500*sqm* and the simulation variables are shown in Table 1.

6.1 Performance Evaluation Parameter

Communication cost It is defined as quantity of time required for transmitting data.

Packet delivery ratio (PDR) It is the fraction of number of data received at the base station per time.

Encryption time The time taken to encrypt data sensed by sensor nodes.

Decryption time The time taken to decrypt data received at the BS.

Energy consumption The total energy consumed for transmitting data from source to base station

Throughput rate The rate of data packet transmitted per unit time.

6.2 Performance Evaluation

The communication costs of MODA [32] and proposed protocol VEDSDA is depicted in Fig. 6. In MODA [32], the number of bits is reduced to 3 so that it helps to reduce the communication costs and increases overhead due to random selection of zero element for hiding. Where as, in VEDSDA protocol AECF algorithm compress the sensed data to 2 bits which reduces communication costs compared with MODA. Thus, AECF algorithm achieves 37% improvement over MODA algorithm.

Figure 7 shows VEDSDA protocol that exhibits increased constant PDR compared with MODA. The reduction of redundant data and data length ensures lesser energy utilization and better network connectivity. VEDSDA protocol shows 5% improvement over MODA protocol. The results satisfies the improvement even with the introduction of various malicious nodes in each execution.

Table 1 Simulation variables

Parameter	Values
Sensor nodes	50, 100, 200
Network topology	500 m * 500 m
Traffic	CBR
Transmission range	40 m
Maximum clusters	16
Startup energy	1 J
packet length	64
Transmission energy	0.016 J
Reception energy	0.018 J
Idle energy	0.0005 J
Simulation time	20000 s

Fig. 6 Communication costs compared with existing protocol MODA

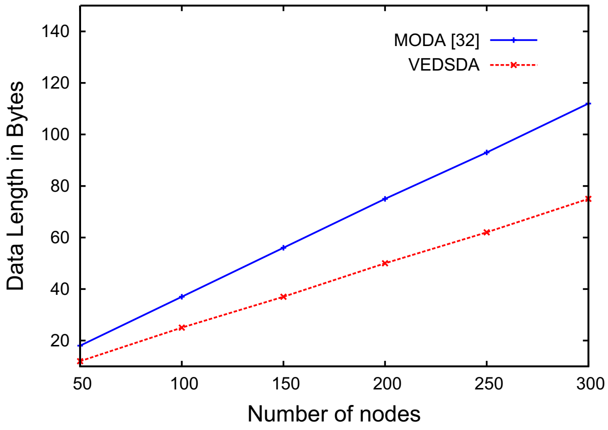

Fig. 7 PDR of VEDSDA and MODA

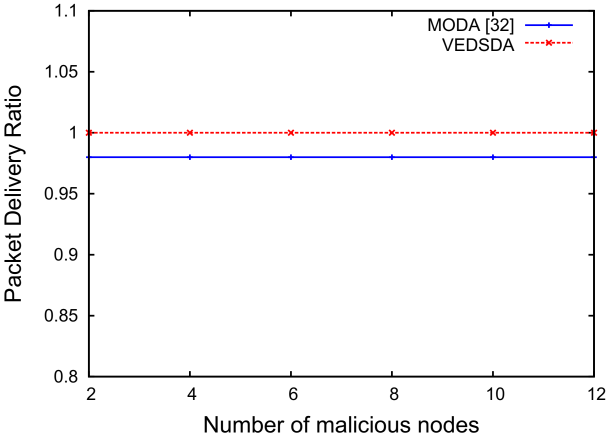

Table 2 Communication cost, energy consumption and throughput rate

Number of nodes	Data length in bytes		Average energy in mJ		Throughput rate	
	MODA	VEDSDA	MODA	VEDSDA	MODA	VEDSDA
50	31	12	0.41	0.23	83.34	91.4234
100	62	25	0.56	0.37	109.356	168.654
150	93	37	0.67	0.56	120.42	170.234
200	125	50	0.94	0.71	133.356	170.654
250	156	62	1.23	0.89	133.43	175.432
300	187	75	1.57	1.18	133.785	175.56

Figure 8 and Table 2 depicts the comparison of encryption time simulation results is analysed with MODA algorithm. VE encryption algorithm involves one-point addition and one scalar multiplication where as MODA algorithm consists of two scalar multiplication and one-point addition. The complete VE process executes *n* times and MODA algorithm

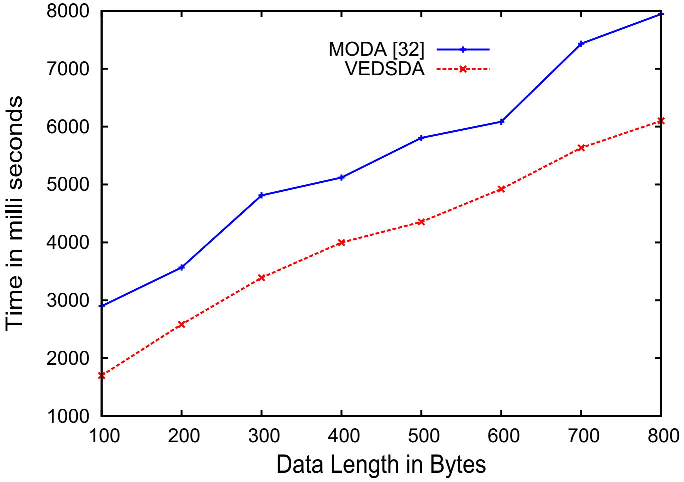

Fig. 8 Encryption time

executes $c_t * n_b * m$ times. This shows that VE algorithm performance is 18.4% more compared with MODA algorithm.

Figure 9 shows the Decryption time taken by VD algorithm and MODA algorithm. Table 3 provides the comparison of simulation result. The basic mathematical operations viz., one-point addition and one scalar multiplication inclusion in VD algorithm increases operation speed whereas MODA algorithm also uses one-point addition and one scalar multiplication. But the complete process in MODA algorithm executes $n_b n$ times and VD algorithm executes n times. Thus, VD algorithm exhibits 12.9% improvement in decryption time compared with MODA algorithm.

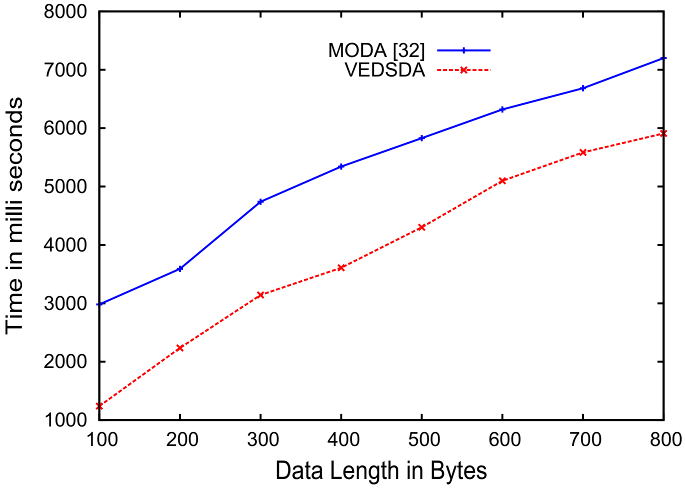

Fig. 9 Decryption time

The energy consumption of both MODA [32] and VEDSDA algorithm is shown in Fig. 10. In a network, energy utilized for data transmission depends on various bits transmitted in a network. The MODA algorithm compressed data length which are collected by nodes to three bits (Table 4). In VEDSDA algorithm, AECF function reduces data

Fig. 10 Energy consumption

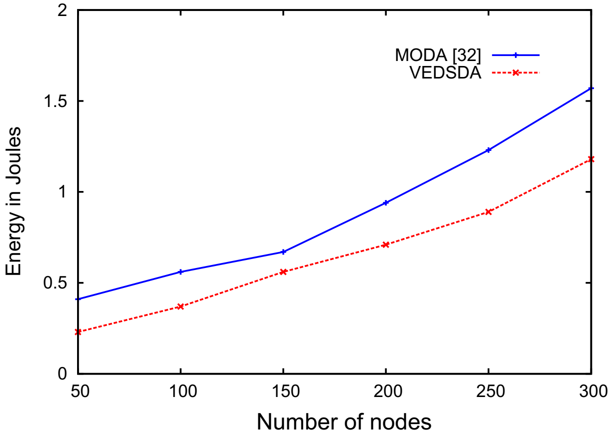

Fig. 11 Throughput

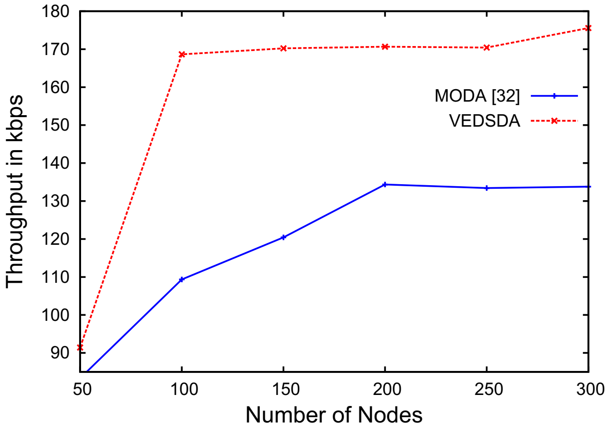

Table 3 Encryption and decryption time

Data length in bytes	Time in ms (encryption)		Time in ms (decryption)	
	MODA	VEDSDA	MODA	VEDSDA
100	2898	1700	2981	1239
200	3567	2584	3590	2235
300	4813	3390	4739	3143
400	5121	3998	5343	3609
500	5806	4354	5829	4303
600	6098	4921	6321	5098
700	7432	5634	6684	5584
800	6099	6099	7201	5910

Table 4 Packet delivery ratio

Number of malicious nodes	Data length in bytes	
	MODA	VEDSDA
2	1	0.98
4	1	0.98
6	1	0.98
8	1	0.98
10	1	0.98
12	1	0.98

length to two bits. So, AECF function transmits lesser number of bits when compared with MODA algorithm. Therefore, VEDSDA algorithm consume lesser energy for transmitting data. Hence, VEDSDA achieves 39% improvement over MODA algorithm.

Figure 11 conveys throughput rate of VEDSDA and MODA. It depicts that VEDSDA protocol provides early data delivery to the BS compared with MODA algorithm. This is due to lesser data transmission using AEDC and strong VED algorithm. The AEDC algorithm reduces data size to 2 bits. Thus, helps to deliver data to the destination with lesser time. Figure presents 42% high throughput rate compared with MODA algorithm.

The result in Table 5 shows time complexity of VEDSDA and MODA algorithm. Figure 12 shows execution process time of VEDSDA protocol is less compared with MODA algorithm.

7 Conclusions

The communication costs used for data transmission is minimized using AECF and AEDF function to reduce data size. This shows improvement in energy utilizatio and data compression, VEDSDA protocol consists of VED technique which exhibits larger PDR with lesser energy consumption and guarantees security for data sensed. The VED technique involves lesser energy over existing protocols due to minimum calculation in encryption and decryption. Therfore, this protocol provides 37% Communication Costs, 5% Throughput Rate, 18.4% Encryption Time, 12.9% Decryption Time, 5% Packet Delivery Ratio and 39% Energy Consumption improvement over existing protocol.

Table 5 Time complexity

Number of clusters	Time complexity	
	MODA	VEDSDA
	$\mathcal{O}(c_t n_b m)$	$\mathcal{O}(n)$
10	400	50
20	800	100
30	1200	150
40	1600	200
50	2000	250

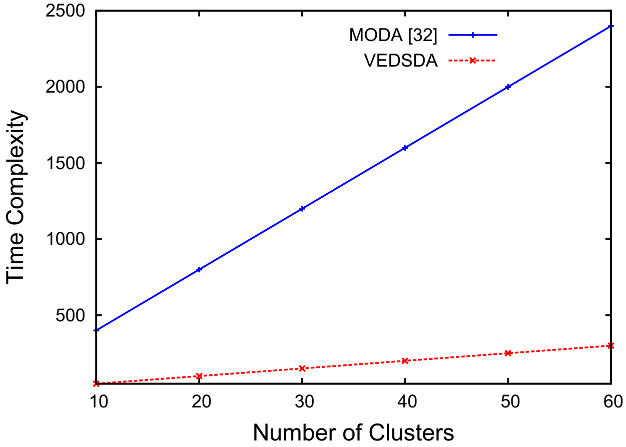

Fig. 12 Time complexity

Funding Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Karthik, S., & Ashok Kumar, Dr. A. (2015). Challenges of wireless sensor networks and issues associated with time synchronization. In *Proceedings of advanced networking and applications* (pp. 2402–2406).
2. Alotaibi, M. (2014). Security to wireless sensor networks against malicious attacks using hamming residue method. *EURASIP Journal on Wireless Communications and Networking, 25*(3), 750–761.
3. Gupta, M., Gao, J., Yan, X., Cam, H., & Han, J. (2014). Top-K interesting subgraph discovery in information networks. In *TInternational council for open and distance education (ICDE) conference* (pp. 820–831).
4. Lu, H., Li, J., & Guizani, M. (2014). Secure and efficient data transmission for cluster-based wireless sensor networks. *IEEE Transactions on Parallel Distribution System, 25*(3), 750–761.
5. Krishnan, A. M., & Kumar, P. G. (2015). An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous WSN. *IEEE Transactions on Parallel Distribution system, 20*(2), 423–424.
6. Nguyen, M. T., Teague, K. A., & Rahnavard, N. (2016). CCS: Energy-efficient data collection in clustered wireless sensor networks utilizing blockwise compressive sensing. *Computer Networks, 106,* 171–185.
7. Abirami, T., & Anandamurugan, S. (2015). Data aggregation in wireless sensor network using shuffled frog algorithm. *Wireless Personal Communications, 90*(2), 1–13.
8. Bojan, S., & Nikola, Z. (2013). Genetic algorithm as energy optimization method in WSN, on Telecommunications Forum (TELFOR) (pp. 97–100).
9. Kandukuri, S., Lebreton, J., Murad, N., Lorion, R., & Genon-Catalot, D. (2016). Data window aggregation techniques for energy saving in wireless sensor networks. In *IEE symposium on computers and communication (ISCC)* (pp. 226–231).
10. He, D., Kumar, N., & Lee, J. H. (2016). Privacy-preserving data aggregation scheme against internal attackers in smart grids. *Wireless Networks, 22*(2), 491–501.

11. Hiker, A., Cerqueira, E., Curado, M., & Monteiro, E. (2016). A two-tier adaptive data aggregation approach for M2M group communication. *IEEE Sensors Journal, 16*(3), 823–835.
12. Jiang, M., Fu, A., & Wong, R. (2015). Exact Top-k nearest keyword search in large networks, In *Proceedings of the 2015 ACM SIGMOD international conference on management of data—SIGMOD '15* (pp. 393–404).
13. Castelluccia, C., Chan, A., Mykletun, E., & Tsudik, G. (2009). Efficient and provably secure aggregation of encrypted data in wireless sensor networks. *ACM Transactions on Sensor Networks, 5*(3), 1–36.
14. Costa, D. G., Figueredo, S., & Oliveira, G. (2017). Cryptography in wireless multimedia sensor networks: A survey and research directions. *International Journal of Cryptography, 1*(4), 1–18.
15. Castellucia, C., Mykletun, E., & Tsudik, G. (2009). Efficient and provably secure data aggregation of encrypted data in wireless sensor networks. *ACM Transactions on Sensor Networks, 5*(3), 1–35.
16. Castelluccia, C., Mykletun, E., & Tsudik, G. (2005). Efficient aggregation of encrypted data in wireless sensor networks, In *The second annual international conference on mobile and ubiquitous systems: Networking and services* (pp. 109–117).
17. Acharya, M., Girao, J., & Westhoff, D. (2005). Secure comparison of encrypted data in wireless sensor networks. *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'05), 1*(22), 47–53.
18. Xu, C., Lu, R., Wang, H., Zhu, L., & Huang, C. (2017). PAVS: A new privacy-preserving data aggregation scheme for vehicle sensing systems. *Sensors, 17*(3), 1–18.
19. Fu, Z., Sun, X., & Ji, S. (2016). A lightweight multi-layer authentication protocol for wireless body area networks. In *IEEE INFOCOM 2016—The 35th annual ieee international conference on computer communications* (pp. 20–29).
20. Damodar Reddy, E., & Prasantha, K Jana. (2012). Clustering biological data using voronoi diagram. In *Proceedings of ADOCNS 2011* (pp. 188–197).
21. Kalyani, S. N., & Kumar, S. S. (2015). Energy efficient data aggregation using voronoi diagram. In *Proceedings of internal conference on signal processing and communication* (pp. 10–13).
22. Vamsi, P. R., & Kant, K. (2015). Secure data aggregation and intrusion detection in wireless sensor networks. In *Proceedings of internal conference on signal processing and communication* (pp. 10–13).
23. Annapurna, H. S., & Siddappa, M. (2015). Secure data aggregation with fault tolerance for wireless sensor networks. In *International conference on emerging research in electronics, computer science and technology* (pp. 252–258).
24. Razaque, A., & Rizvib, S. S. (2017). Secure data aggregation using access control and authentication for wireless sensor networks. *Computers and Society, 70,* 532–545.
25. Mahimkar, A., & Rappapart, T. S. (2004). 'ecureDAV: A secure data aggregation and verification protocol for sensor networks. In *Proceedings of IEEE global telecommunications conference* (pp. 2175–2179).
26. Roy, S., Conti, M., Setia, S., & Jajodia, S. (2012). Secure data aggregation in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 9*(3), 681–694.
27. Cam, H., Ozdemir, S., Nair, P., & Muthuavinashiappan, D. (2003). ESPDA: Energy-efficient and secure pattern-based data aggregation for wireless sensor networks. In *Proceedings of IEEE sensors* (pp. 732–736).
28. Sonli, H. O., Ozdemir, S., & Cam, H. (2004). SRDA: Secure reference-based data aggregation protocol for wireless sensor networks. In *Proceedings of IEEE*60_t*hvehicular technology conference* (pp. 4650–4654).
29. Ozdemir, S., & Xiao, Y. (2011). Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. *Computer Networks, 55*(8), 1735–1746.
30. Ozdemir, S., & Cam, H. (2010). Integrity of false data detection with data aggregation and confidentiality transmission in wireless sensor networks. *IEEE/ACM Transactions on Networking, 18*(3), 736–749.
31. Shim, K. A., & Park, C. M. (2015). A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(8), 2128–2139.
32. Zhang, P., Wang, J., Guo, K., Wu, F., & Min, G. (2018). Multi-functional secure data aggregation schemes for WSNs. *Ad Hoc Networks, 69,* 86–99.

S. Reshma Research Scholar, Visvesvaraya Technological University—Research Resource Center. She is presently working as a Test Engineer in Evry India Pvt Ltd., Bangaluru. She received her bachelor's degree in computer science and Engineering from Visvesvaraya Technological University and Master of Technology from Visvesvaraya Technological University, Regional Center, Bangalore. Her research interest is in the area of Wireless Sensor Networks.

Dr. K. Shaila Professor in Department of Electronics and Communication and was the Head of the Department, Vivekananda Institute of Technology. She obtained her Ph.D. in Computer Science and Engineering from Bangalore University, M.E. in Electronics and Communication from University Visvesvaraiah College of Engineering, Bangalore University and B.E. from PES Institute of Technology, Bangalore University, Bangalore. She has over twenty years of teaching experience. She has authored Digital Circuits and Systems published by Tata McGraw Hill, New Delhi and Secure Data Communication Techniques by LAP LAMBERT publishers, Germany. She has published papers in refereed International Journals and International Conferences. She has received Best Teacher and Best Researcher Award. Her name appears in Marquis Who's Who in the World Science and Engineering. She is the Life member of ISTE, iMAPs, Member of ACM, IEANG and reviewer for conference and journals. Her research areas include Wireless Sensor Networks, Adhoc Networks and Image Processing.

Dr. K. R. Venugopal Vice Chancellor, Bangalore University. He has Eleven Degrees with Ph.D. in Computer Science Engineering from IIT-Madras, Chennai and another Ph.D. in Economics from Bangalore University. He has degrees in Law, Mass Communication, Electronics, Economics, Business Finance, Computer Science, Public Relations and Industrial Relations. He has authored and edited 64 books and published more than 700 papers in refereed International Journals and International Conferences. He has supervised 630 M.E. dissertations, 25 Ph.Ds and filed 101 Patents. He was a Post Doctoral Research Scholar and a visiting Professor at University of Southern California, USA. He has been conferred Fellow of IEEE, USA and ACM Distinguished Educator for contributions to Computer Science Engineering and Electrical Engineering Education.