Data Transmission with Improving Lifetime of Cluster Network

Anitha S\textsuperscript{a}, Saravanan S\textsuperscript{b}, and Chandrasekar A\textsuperscript{c}

\textsuperscript{a} Research Scholar, Department of Computer Science & Engineering, Annamalai University, Annamalai Nagar, TN, India
\textsuperscript{b}Assistant Professor, Department of Computer Science & Engineering, Annamalai University, Annamalai Nagar, TN, India
\textsuperscript{c}Professor, Department of Computer Science and Engineering, St. Joseph’s College of Engineering, TN, India.

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: The efficiency of selecting the cluster head plays a major role in resolving the complexities faced in network management aiming to improve the longevity of sensors in the network. The clustering process is improved by selecting proper cluster heads with the consideration of energy conservation among participant nodes. While coming to security concept on WSN, the trust based cluster head selection is significant with the assumption of cooperation of all sensor nodes. In view of this assumption, the traditional methods could not help in defining the ideal cluster head of the network. This work proposes Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA) by combining Voronoi method for clustering process and cryptographic algorithm for secure data transmission. This is considered as two-tier architecture whereas, clustering takes place in first tier and encryption along with decryption takes place in the second tier. The proposed algorithm is compared with two state-of-art methods such as, Secured WSN (SeC-WSN) and Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) in terms of energy consumption, Packet Delivery Ratio (PDR), network lifetime, encryption time and decryption time. As a result, the proposed VC-SCCA achieves 53.2% of energy consumption, 98.6% of packet delivery ratio, 97.5% of network lifetime, 62.8sec of encryption time and 71.2sec decryption time.

Keywords: Wireless Sensor Networks (WSN), Security, Clustering, Lifetime, Cryptography.

1. Introduction

The rapid development in WSN has motivated to provide cost effective and power efficient devices. Sensors are comprised of signal processing and sensing devices which offer numerous processing abilities for nodes in WSN to provide wireless communication. The sensor networks are used in several sectors such as in disaster places, chemical plant and even as a nuclear reactor. Wireless Sensor Network consists of various nodes that collects the packets from its neighbors which further forwards them to its sink node independently [1]. Thus, WSN has the capacity to display the outside situations and altersthe detected information which can be easily understood by the user.

WSN are used in several applications which involve hospitals, military, and home [2]. The recent large scale WSN applications are of various fields like environmental monitoring, surveillance and so on. Generally, sensors are inexpensive and provide less battery power; thereby causing energy issues. The issues considered to be a major one is to maximize network lifetime. In applications where the data has to be gathered, every node is responsible to sense data packets [3]. The process data aggregation reduces data traffic thereby storing energy as various incoming data packets were integrated as a single one [4]. Hence, several applications are developed for enhancing the overall lifespan of the system.

Moreover, the wireless infrastructure is most challenging one in terms of the self-organizing and variable communication [5]. Under wireless sensor application the Sensor Nodes (SNs) forwards the identified data to a multi-hop manner. In multi-hop each sensor node needs the assistance of its neighbours for forwarding the information to base station / sink node [6] and hence it generates numerous vulnerabilities in WSN. When an attacker compromises any of the cooperating node, information loss occurs thereby degrading the quality of data at the receiving end [7,8]. Hence, anominal routing trust centered routing approach for WSN has to be designed for proving secure data transmission.

The organization of this paper is prescribed here: Section 2 presents the literature survey and limitations. Section 3 describes the proposed methodology for securing data transmission. Section 4 describes the complete details about the performance of the proposed approach and conclusion with future directions in section 5.

2. References

Hassan et al., (2020) practically proved that CH-load reduction had the largest effect on enhancing the energy efficiency of the clustering algorithms compared to some other energy efficiency-enhancing factors. So, a model divides the whole load of CH role and is allocated to whole new nodes. By using the Wireless Power Transfer (WPT) strategy, each node in the cluster transfers a specific amount of energy (equal to a part of the CH load that is assigned to the node) to the CH node. All the nodes energy transferred to CH node instead of an individual node. So, the lifetime of the WSN was is greatly enhanced. The simulation results showed that this
model achieved higher lifetime improvement compared to Leach and K-means clustering algorithms respectively [9].

Ghosal et al., (2020) introduced an (OPTIC On-demand, oPTImal Clustering) algorithm for WSNs. Here, the process of selecting cluster head was not periodic, instead was adaptive based on the dynamic occurrence of events. The objective of this OPTIC algorithm was to decrease the computation as well as message overheads. From the results obtained, it was proved that this OPTIC algorithm improved the energy balance at about 18% and network lifetime by nearly 19% than the non-clustering and two clustering state-of-the-art approaches [10].

Vishnu et al., (2020) presented a three-tier architecture to provide secure cluster-based WSN (SeC-WSN) to ensure security and QoS. On the whole network, controllers provide global view and flow rules are deployed on switches related to the network status and level of security. Simulation results of ns-3 proved that this approach improved 5% of throughput, 7.8% of PDR and 16% of energy consumption. The major factor which degraded the performance of the system was distance [11].

Vinitha et al., (2019) provided a Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) which was an energy efficient multi-hop manner for WSN by applying Taylor series in C-SSA. This approach underwent two phases to obtain multi-hop routing namely Cluster Head assortment and data broadcast. At first, particular nodes with highest energy were nominated as cluster head and then Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was utilized transmitting information efficiently. Sensor nodes forward the information over cluster head which in turn sends to base station via nominated finest hop. Taylor C-SSA was employed for selecting the optimal hop. The approach extended the network lifetime while the throughput obtained was not satisfactory [12].

Alghamd et al., (2018) discussed a simple energy efficient approach where security at every hop with end-to-end node authentication was provided. This approach transferred information to the nodes having more energy thereby secured communication was provided. In WSN, the parameter that is considered as most important is the energy of node. This model is appropriate for distributing packets in accordance with the energies of nodes thereby break down in the network is avoided. From the simulation results, it was observed that packet loss as well as delay was reduced and network lifespan was improved which is critically important in the communication of WSN. The drawback is that the average distance is high from source to destination [13].

Amuthan et al., (2018) developed called Hyper-Exponential Reliability Factor-based Cluster Head Election (HRFCHE) scheme which involved Semi-Markov method with the objective to increase the lifespan of the network. HRFCHE approach resulted in high performance where the network lifespan was protracted and overall energy consumption was reduced. The only limitation is that egocentricity of the sensor nodes was considered to measure the transition behavior when numerous other activities were available [14].

Mehmood et al., (2017) designed a knowledge-based context-aware method to deal with disturbances created by malicious nodes. The knowledge base scheme located at the base station stores the events created by the network nodes. Moreover, events are classified and CHs are recognized to block the repetitive activities produced maliciously. With the inference engines, CHs gathers the information about the maliciousness of intruder. The major drawback is that every node present in the cluster is not benefited by the selected and moreover every operation is monitored [15].

Cengiz et al., (2016) coined an energy-efficient multi-hop routing procedure for wireless sensor network which reduced overhead. Moreover, lifetime of the system was significantly enhanced. This procedure utilized relay nodes to transmit the data accumulated by cluster. Thus, in WSN, as relay nodes were used, positive impact was provided while energy dissipation. This method is not the right choice for larger networks [16].

3. Proposed Work

This section presents the proposed security aware clustering and data transmission algorithm named as Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA) which is based on graphical cluster formation in WSN. A trust value is utilized wherever factors like threshold based key generation and key distribution among both inter cluster and intra cluster communication is considered. This model is employed to provide high secure network. In the first step, cluster head (CH) and clustering is done using the voronoi method to find the optimal CH having maximum energy. Next, secure data transmission is carried out via Secure Contextual Cryptographic Algorithm (SCCA). Figure 1 illustrates the schematic diagram of the proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)
3.1 Network model

The lifetime of the network has to be prolonged for which clustering approach is involved where energy is conserved in the large network. This network is categorized as homogeneous and heterogeneous cluster WSN where the former is utilized for related communication and sensing area while the latter for diverse communication and sensing area. The types of cluster communication that occurs while transmitting are Intra-cluster and Inter-cluster communication.

3.2 Clustering process

In WSNs, the cluster setup has to be appropriate for Intra-cluster and Inter-cluster infrastructures. There are totally five clusters namely A, B, C, D, and E are considered. Heterogeneous cluster network comprises of sensor nodes as well as cluster head. The source node forwards the identified information from gathered CH to gateway. Baggage technique is applied in each cluster to choose the connected cluster head dominator as cover set degree. After certain duration, CH enters sleep mode when the residual energy is too low. In the next cycle, the CH selected previously is not considered; as an alternate, the coverage number is computed for every sensor node.

Based on the control packet of Voronoi, every sensor node identifies the CH for communication[17]. The CH forwards the control packet of Voronoi by means of the address of destination as broadcast address. All sensor nodes receiving the packets will in turn forward them such that it won’t hurt from loop-backing and multiple broadcasts. In the control packet, the equations are formed as given below:

\[ \text{x} - \text{x}(\text{mi}) = \text{pi}(\text{x}(\text{mi})) \]

where, \( \text{pi} \) stands for the slope of perpendicular bisector between two adjacent CH whereas, \( \text{ch}(\text{ai,bi}) \) and \( \text{ch}(\text{ai,bi}).(\text{am,bm}) \) are the mid-points of the above mentioned CH. \( \text{pi} \) can be estimated by

\[ \text{pi} = \frac{n(i)}{n(i)=} \]

where, \( n(i) \) is the slope of line having two CHs \( \text{ch1}(\text{ai,bi}) \) and \( \text{ch2}(\text{aj,bj}) \) as its end points.

\[ \text{pi} = \]

\[ \text{xm}= \]

\[ \text{ym}= \]

Every sensor node receiving the broadcasted packet attunes itself with respective CH by solving the equations present in the control packet of Voronoi. According to the equations of lines contained in the packet, every sensor node identifies the respective CH as shown below.

\[ \text{b(i)} - \text{b(mi)} - \text{pi}(\text{a(i)} - \text{a(mi)}) > 0 \]

\[ \text{b(i)} - \text{b(mi)} - \text{pi}(\text{a(i)} - \text{a(mi)}) \geq 0 \]

\[ \text{b(i)} - \text{b(mi)} - \text{pi}(\text{a(i)} - \text{a(mi)}) < 0 \]

\[ \text{b(i)} - \text{b(mi)} - \text{pi}(\text{a(i)} - \text{a(mi)}) \leq 0 \]

3.3 Trust value calculation

Initially, the threshold value is assumed as 0.5. The nodes are given a rating based on the nodes behavior. If the rating is above 0.5, then it is assumed as a trusted node, otherwise untrusted. Once the node is classified, the message is encrypted and decrypted by using the key and it is sent to the user.

3.3.1 Threshold based key generation

Table 1 presents the notations used in this paper.

<table>
<thead>
<tr>
<th>Notations used</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PK</td>
<td>Public key</td>
</tr>
<tr>
<td>MK</td>
<td>Master key</td>
</tr>
<tr>
<td>PFK</td>
<td>Public Functional key</td>
</tr>
<tr>
<td>MFK</td>
<td>Master Functional key</td>
</tr>
<tr>
<td>f(i)</td>
<td>Input function</td>
</tr>
<tr>
<td>SK [f(i)]</td>
<td>Function of secret key</td>
</tr>
</tbody>
</table>

Initially, the setup algorithm of SCCA is applied where few security parameters are considered by way of input and generates a public key PK as well as a master key MK.

Next, for functional encryption, the algorithm by considering few security parameters as input, generates a functional public key PFK and a functional master key MFK.

Finally, function \( f(i) \) is taken as input and functional secret key \( SK [f(i)] \) is produced as output by means of MKF for ith authority where \( i \) ranges from 1 to \( n \). Function \( f(i) \) is described as
Data Transmission with Improving Lifetime of Cluster Network

\[ f_i(S) = s_{si}(\text{KeyGen}(M K, S)) \]

where, \( s_{si}(s) \) yields the \( i \)th share when \((n, k)\)-secret sharing is applied on secret \( s \) and \( \text{KeyGen}(M K, S) \) denotes the key generation algorithm of CP-ABE. Once the setup algorithm comes to an end, the data owner sends PKF to the users and SK[\( f_i \)] to the \( i \)th authority over the secure channel.

### 3.4 Key distribution

The quantum key is used by the user as well as gateway for data transmission. In this process, the gateway generates a string of secret bits termed as qu-bits. Here, based on the obtained qu-bits, quantum key is generated and is used in encryption as well as decryption process. When a request is received from the users, the gateway transmits qu-bits to the user. According to this process, a set of strings is generated by the user which is then forwarded to the admin who matches the qu-bits based on its index for ensuring if the user is trusted or not. If trusted user, the key encryption as well as decryption process is generated at both ends namely gateway and user followed by data transmission.

### 3.5 Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)

**Step-1:** Cluster formation by voronoi control packet

\[ x-x(mi) = pi(x-x(mi)) \]

midpoints = \( \text{ch}(ai, bi) \) and \( \text{ch}(ai, bi). (am, bm) \)

\[ pi= \]

\[ n(i)= \]

\[ A<=n(i) \]

**Step-2:** Cluster head formation

\[ x(m)= \]

\[ y(m)= \]

**Step-2.1:** Slope formation

\[ pi= \]

**Step-2.2:** Finalization of two cluster heads \( ch_1 \) and \( ch_2 \)

\( ch_1(ai, bi) \) and \( ch_2(aj, bj) \).

**Step-3:** Arrangement of sensor nodes in cluster

\[ b(i)-b(mi)-pi(a(i)-a(mi)) > 0 \leq 1 \text{ then intercluster communication} \]

\[ b(i)-b(mi)-pi(a(i)-a(mi)) < 0 \geq \text{ then intracluster communication} \]

**Step-4:** Trust value calculation

\[ \text{threshold value} = 0.5 \]

If \( \text{threshold} > 0.5 \) then trusted node else untrusted node

**Step-5:** Data transmission

- **Destination Address =** \( DA \) \{source_id, data_size, length\}
- **Broadcast Address =** \( BA \) \{destination_id, data_size, length\}

**Step-5.1:** Key generation and expansion

At round \( 1 \)

\[ K_1 = Y*Z*(A \mod E) \]

\[ K_2 = X*Z*(B \mod F) \]

\[ K_3 = Y*X*(C \mod G) \]

At round \( 2 \)

\[ \beta K_1 = \alpha_2 (Y*Z*(A \mod E)) \]

\[ \beta K_2 = \alpha_2 (X*Z*(B \mod F)) \]

\[ \beta K_3 = \alpha_2 (Y*X*(C \mod G)) \]

At round \( 3 \)
\[ \beta_1 K_1 = \alpha_3 (Y^*Z^* (A \mod E)) \]
\[ \beta_1 K_2 = \alpha_3 (X^*Z^* (B \mod F)) \]
\[ \beta_1 K_3 = \alpha_3 (Y^*X^* (C \mod G)) \]

Step-6: Data transferred to user

4. Performance analysis

Extensive experiments were carried with the proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA) with existing methods such as Secured WSN (SeC-WSN) and Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA). The performance is analyzed with parameters like energy consumption, Packet Delivery Ratio (PDR), network lifetime, encryption time and decryption time. Table 2 presents the simulation parameters used for entire network.

Table 2: Simulation Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>500x500 m</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>500</td>
</tr>
<tr>
<td>Transmission range</td>
<td>45m</td>
</tr>
<tr>
<td>Simulation time</td>
<td>25 sec</td>
</tr>
<tr>
<td>Initial energy</td>
<td>0.6 J</td>
</tr>
<tr>
<td>Data rate</td>
<td>30Mbps</td>
</tr>
</tbody>
</table>

Energy consumption: This is the total energy of all hops computed as given below

\[
Energy = \frac{1}{p} \sum_{n} E_n
\]

where, \(p\) and \(E_n\) represent the hops in multihop routing and energy of \(n\)th hop respectively.

Table 3 shows the comparison of energy between existing Secured WSN (SeC-WSN) and Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) with proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)

Table 3: Analysis of energy consumption

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>SeC-WSN</th>
<th>Taylor C-SSA</th>
<th>VC-SCCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>56</td>
<td>49</td>
<td>37</td>
</tr>
<tr>
<td>200</td>
<td>63</td>
<td>51</td>
<td>42</td>
</tr>
<tr>
<td>300</td>
<td>74</td>
<td>58</td>
<td>53</td>
</tr>
<tr>
<td>400</td>
<td>83</td>
<td>69</td>
<td>61</td>
</tr>
<tr>
<td>500</td>
<td>89</td>
<td>79</td>
<td>73</td>
</tr>
</tbody>
</table>

Figure 2: Comparison for energy consumption with the existing and proposed methods

Figure 2 depicts the energy consumption comparison of existing SeC-WSN, Taylor C-SSA and Proposed VC-SCCA. The X axis and Y axis represent the number of nodes and energy consumed in percentage respectively. Energy consumption of the proposed method is 53.2% which is less than the existing methods.

Network Lifetime: This is the lifetime of node which has to be maximum to provide effective routing and is estimated by
Data Transmission with Improving Lifetime of Cluster Network

\[
\text{Network Lifetime} = \frac{1}{p} \sum_{n=1}^{p-1} \frac{M(n, n+1)}{\beta}
\]

Table 4 displays the comparison of network lifetime between existing Secured WSN (SeC-WSN) and Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) with proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)

Table 4: Analysis of network lifetime

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>SeC-WSN (%)</th>
<th>Taylor C-SSA (%)</th>
<th>VC-SCCA (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>84</td>
<td>86</td>
<td>95.6</td>
</tr>
<tr>
<td>200</td>
<td>88</td>
<td>89</td>
<td>96.69</td>
</tr>
<tr>
<td>300</td>
<td>90</td>
<td>92</td>
<td>98</td>
</tr>
<tr>
<td>400</td>
<td>93</td>
<td>94</td>
<td>98.4</td>
</tr>
<tr>
<td>500</td>
<td>95</td>
<td>96</td>
<td>98.93</td>
</tr>
</tbody>
</table>

Figure 3: Comparison of network lifetime with the existing and proposed methods

Figure 3 depicts the network lifetime comparison of existing SeC-WSN, Taylor C-SSA and Proposed VC-SCCA. The X axis and Y axis represents the number of nodes and network lifetime in percentage respectively. Network lifetime achieved by the proposed method is 97.5% which is greater than the existing methods.

Packet Delivery Ratio (PDR): This is the rate packet transferred successfully from the source to destination node in the network.

\[
PDR = \frac{\text{number of packet received successfully}}{\text{Total number of packets forwarded}}
\]

Packet Deliver Ratio (PDR)

Table 5 shows the comparison of Packet Delivery Ratio (PDR) between existing Secured WSN (SeC-WSN) and Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) with proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)

Table 5: Analysis of Packet Deliver Ratio (PDR)

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>SeC-WSN (%)</th>
<th>Taylor C-SSA (%)</th>
<th>VC-SCCA (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>68.45</td>
<td>93.35</td>
<td>97.74</td>
</tr>
<tr>
<td>200</td>
<td>69.75</td>
<td>94.78</td>
<td>98.38</td>
</tr>
<tr>
<td>300</td>
<td>70.45</td>
<td>95.89</td>
<td>98.47</td>
</tr>
<tr>
<td>400</td>
<td>73.5</td>
<td>97.57</td>
<td>99.06</td>
</tr>
<tr>
<td>500</td>
<td>74.69</td>
<td>98.74</td>
<td>99.38</td>
</tr>
</tbody>
</table>
Figure 4: Comparison of PDR with the existing and proposed methods

Figure 4 depicts the PDR comparison of existing SeC-WSN, Taylor C-SSA and Proposed VC-SCCA. The X axis and Y axis represents the number of nodes and PDR in percentage respectively. Packet delivery ratio achieved by proposed method is 98.6% which is greater than the existing methods.

Encryption time: It is the time taken to encrypt the data. The proposed VC-SCCA method is evaluated with various data lengths of data and the time taken to encrypt data is estimated which is summarized in table 6.

Table 6: Analysis of encryption time

<table>
<thead>
<tr>
<th>Data in bytes</th>
<th>SeC-WSN (sec)</th>
<th>Taylor C-SSA (sec)</th>
<th>VC-SCCA (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>65</td>
<td>56</td>
<td>45</td>
</tr>
<tr>
<td>40</td>
<td>72</td>
<td>67</td>
<td>56</td>
</tr>
<tr>
<td>50</td>
<td>84</td>
<td>72</td>
<td>63</td>
</tr>
<tr>
<td>60</td>
<td>89</td>
<td>78</td>
<td>71</td>
</tr>
<tr>
<td>70</td>
<td>93</td>
<td>86</td>
<td>79</td>
</tr>
</tbody>
</table>

Figure 5: Comparison of encryption time with the existing and proposed methods

Figure 5 depicts the encryption time comparison of existing SeC-WSN, Taylor C-SSA and proposed VC-SCCA. The X axis and Y axis represents the data in bytes and encryption time in seconds respectively. The proposed method takes 62.8 sec for encryption which is lesser than the existing methods.

Decryption time: It is the time taken for generating plain text from the cipher text obtained. The proposed VC-SCCA is evaluated with various data lengths of data and estimated the time taken by every data for decryption when the key is known which is summarized in table 7.

Table 7: Analysis of decryption time

<table>
<thead>
<tr>
<th>Data in bytes</th>
<th>SeC-WSN (sec)</th>
<th>Taylor C-SSA (sec)</th>
<th>VC-SCCA (sec)</th>
</tr>
</thead>
</table>

426
Figure 6: Comparison of decryption time with the existing and proposed methods

Figure 6 depicts the decryption time comparison of existing SeC-WSN, Taylor C-SSA and proposed VC-SCCA. The X axis and Y axis represents the data in bytes and decryption time in seconds respectively. The proposed method takes 71.2 sec for decryption which is lesser than the existing methods. Table 8 presents the overall performance of the proposed system against the existing methods with various parameters considered for comparison.

Table 8: Overall Performance Analysis

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy consumption (%)</td>
<td>73</td>
<td>61.2</td>
<td>53.2</td>
</tr>
<tr>
<td>Network Lifetime (%)</td>
<td>90</td>
<td>91.4</td>
<td>97.5</td>
</tr>
<tr>
<td>Packet Delivery Ratio (%)</td>
<td>71.3</td>
<td>96</td>
<td>98.6</td>
</tr>
<tr>
<td>Encryption time (sec)</td>
<td>80.6</td>
<td>71.8</td>
<td>62.8</td>
</tr>
<tr>
<td>Decryption time (sec)</td>
<td>83.4</td>
<td>81</td>
<td>71.2</td>
</tr>
</tbody>
</table>

5. Conclusion

This paper mainly concentrates on security aware clustering and data transmission algorithm named as Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA) by considering security as a significant paradigm for providing efficient data transmission. Rather than the traditional approaches, this approach considers security based on trust model and cryptography method. Moreover, this mechanism also clusters the sensor nodes where the lifetime of the entire network lifetimes is considerably increased. Cluster heads alone are responsible to calculate the trust of nodes in the network. The data is then transmitted to the user, with proper verification during key distribution. This procedure is reiterated by every sensor for the sensed outcomes. As a result, the proposed algorithm achieves 53.2% of energy consumption, 97.5% of network lifetime, 98.6% packet delivery ratio, 62.8 sec of encryption time and 71.2 sec decryption time.

References