Data Transmission with Improving Lifetime of Cluster Network

Anitha S[a], Saravanan S[b], and Chandrasekar A[c]

[A]
Research Scholar, Department of Computer Science & Engineering., Annamalai University, Annamalai Nagar, TN, India
[b]Assistant Professor, Department of Computer Science & Engineering., Annamalai University, Annamalai Nagar, TN, India,
[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 followed 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 motivatedto provide cost effective and power efficient devices. Sensors are comprised of signal processing and sensing devices which offer numerous processingabilities 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 nodesthatcollects the packets from its neighborswhich further forwards them to its sink node independently [1]. Thus, WSN has the capacity to display the outside situations and altersthe detectedinformationwhich can be easily understood by the user.

WSN are used in several applications which involvehospitals, 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 enhancingthe 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 identifieddatavia multi-hop manner. In multi-hop each sensor nodeneeds 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, annominal routing trust centered routing approachfor 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 decreasethe 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 performanceof the system was distance [11].

Vinitha et al., (2019) provideda Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) which was an energy efficient multi-hop mannerfor WSN by applying Taylor series in C-SSA. This approach underwent two phases to obtain multi-hop routing namely Cluster Head assortmentanddata 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 nominatedfinesthop. Taylor C-SSA was employed for selecting the optimal hop. The approach extended the network lifetime while the but 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 authenticationwas 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 lifespanwas protractedand overall energy consumption was reduced. The onlylimitation 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 methodto deal with disturbancescreated by malicious nodes. The knowledge base scheme located at the base stationstores the events created by the network nodes. Moreover, events are classified and CHs are recognized to block the repetitive activities producedmaliciously. 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 systemwas 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. Thismethod 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 formationin WSN.A trust vale is utilized whereseveral 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)

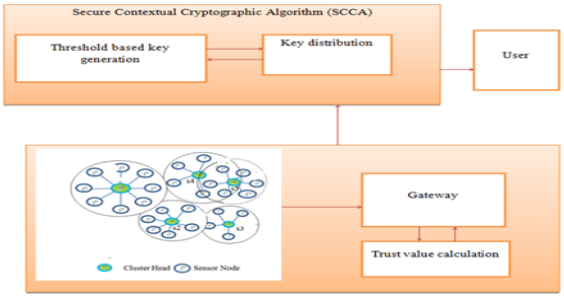

Figure 1: Schematic diagram of proposed Voronoi Clustered Secure Contextual Cryptographic Algorithm (VC-SCCA)

3.1Network 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 relatedcommunication and sensing areawhile 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 identifiedinformation from gatheredCH to gateway. Baggage technique is applied in each clusterto 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 CHselected 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'thurt from loop-backing and multiple broadcasts. In the control packet, the equations are formed as given below:

$x-x(mi) = pi(x-x(mi))$

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

pi=

n(i)=

where, ni is the slope of line having two CHs ch1(ai,bi) and ch2(aj,bj) as its end points.

pi=

xm=

y(m)=

Every sensor node receiving the broadcasted packet attunesitself 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.

$b(i)-b(mi)-pi(a(i)-a(mi) > 0$

$b(i)-b(mi)-pi(a(i)-a(mi) \geq 0$

$b(i)-b(mi)-pi(a(i)-a(mi) < 0$

$b(i)-b(mi)-pi(a(i)-a(mi) \leq 0$

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.

Notations used	Meaning
PK	Public key
MK	Master key
PFK	Public Functional key
MFK	Master Functional key
f(i)	Input function
SK [f(i)]	Function of secret key

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

Next, forfunctional 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 ithauthority where i ranges from 1 to n. Function f(i)is described as

fi(S) = ssi(KeyGen(MK,S))

where,ssi(s) yields the ith share when(n, k)-secret sharing is applied on secret sand KeyGen(M K, S) denotes the key generation algorithm of CP-ABE. Once the setup algorithm comes to an end, the data owner sends PKFto the users and SK[fi] to the ith 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, thegatewaygenerates 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 = ch(ai,bi) and ch (ai,bi).(am,bm)

pi=

n(i)=

A<=n(i)

Step-2: Cluster head formation

xm=

y(m)=

Step-2.1: Slope formation

pi=

Step-2.2: Finalization of two cluster heads ch1 and ch2

ch1(ai,bi) and ch2(aj,bj).

Step-3: Arrangement of sensor nodes in cluster

b(i)-b(mi)-pi(a(i)-a(mi) > 0≤ 1 then intercluster communication

b(i)-b(mi)-pi(a(i)-a(mi) < 0 ≥ then intracluster communication

Step-4: Trust value calculation

threshold value =0.5

If 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

K1 =Y*Z* (A mod E)

K2=X*Z*(B mod F)

K3=Y*X*(C mod G)

At round-2

βK1 =α2 (Y*Z* (A mod E))

βK2= α2 (X*Z*(B mod F))

βK3= α2 (Y*X*(C mod G))

At round-3

β1K1 =α3 (Y*Z* (A mod E))

β1K2= α3(X*Z*(B mod F))

β1K3= α3 (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) withexisting 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 parametersused for entire network.

Table 2: Simulation Parameters

Parameters	Values
Area	500×500 m
Number of nodes	500
Transmission range	45m
Simulation time	25sec
Initial energy	0.6 J
Data rate	30Mbps

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

$$Energy = \frac{1}{p}\sum_{n}^{p} E_n$$

where, p and En represent the hops in multihop routing and energy of nth 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

Number of nodes	SeC-WSN	Taylor C-SSA	VC-SCCA
100	56	49	37
200	63	51	42
300	74	58	53
400	83	69	61
500	89	79	73

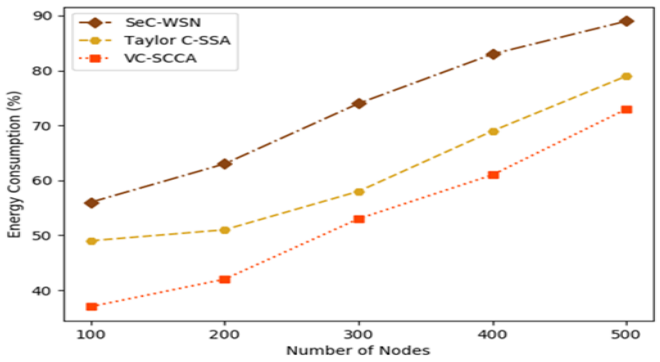

Figure 2: Comparison for energy consumption with the existing and proposed methods

Figure 2 depicts the energy consumption comparison of existing SeC-WSN, Taylor C-SSA and Proposed VC-SCCA. The X axis and Y axis represents 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 bemaximum to provide effective routing and is estimated by

$$Network\ Lifetime = \frac{1}{p} \times \sum_{n=1}^{p-1} \frac{M(N_n, N_{n+1})}{\beta}$$

Table 4displays 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

Number of nodes	**SeC-WSN (%)**	**Taylor C-SSA(%)**	**VC-SCCA (%)**
100	84	86	95.6
200	88	89	96.69
300	90	92	98
400	93	94	98.4
500	95	96	98.93

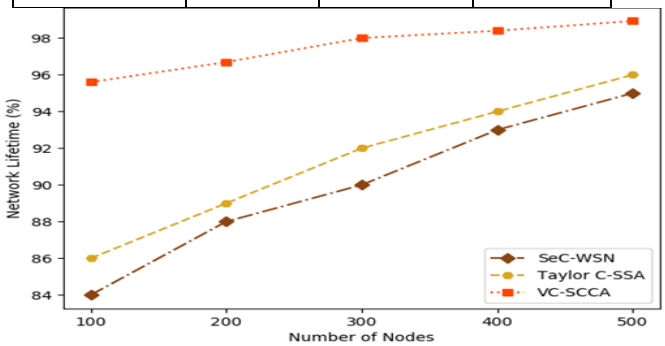

Figure 3: Comparison of network lifetime with the existing and proposed methods

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 lifetimeachieved 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.

$$PDR = \frac{number\ of\ packet\ received\ succesfully}{Total\ number\ of\ packets\ forwarded}$$

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)

Packet Deliver Ratio (PDR)

Number of nodes	**SeC-WSN (%)**	**Taylor C-SSA (%)**	**VC-SCCA (%)**
100	68.45	93.35	97.74
200	69.75	94.78	98.38
300	70.45	95.89	98.47
400	73.5	97.57	99.06
500	74.69	98.74	99.38

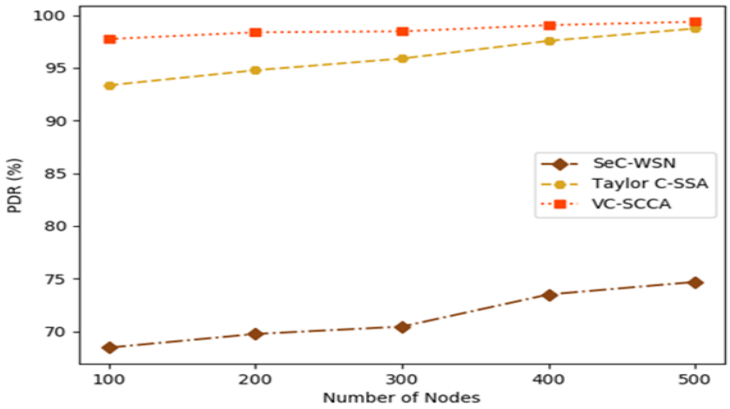

Figure 4: Comparison of PDR with the existing and proposed methods

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 ratioachieved 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

Data in bytes	SeC-WSN (sec)	Taylor C-SSA(sec)	VC-SCCA(sec)
30	65	56	45
40	72	67	56
50	84	72	63
60	89	78	71
70	93	86	79

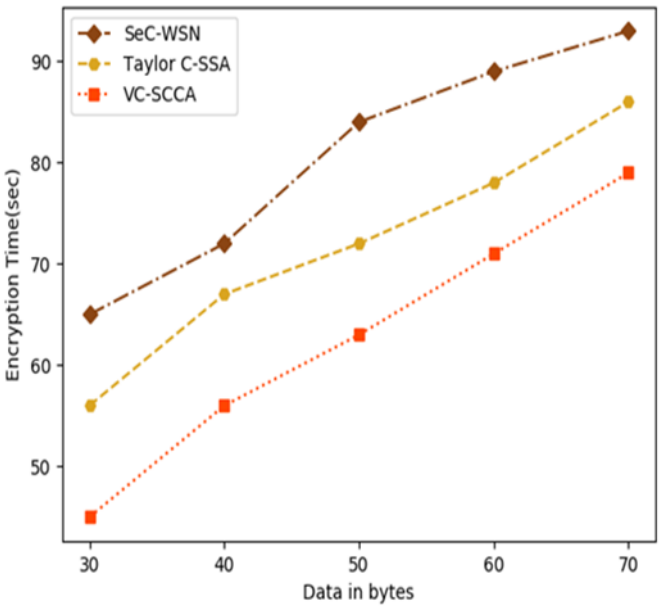

Figure 5: Comparison of encryption time with the existing and proposed methods

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 62.8sec 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 takenby every data for decryption when the key is known which is summarized in table 7.

Table 7: Analysis of decryption time

Data in bytes	SeC-WSN (sec)	Taylor C-SSA(sec)	VC-SCCA(sec)

30	78.65	77.87	67.78
40	79.85	78.88	68.98
50	83.67	81.93	72.67
60	85.67	82.74	73
70	89.45	83.76	73.57

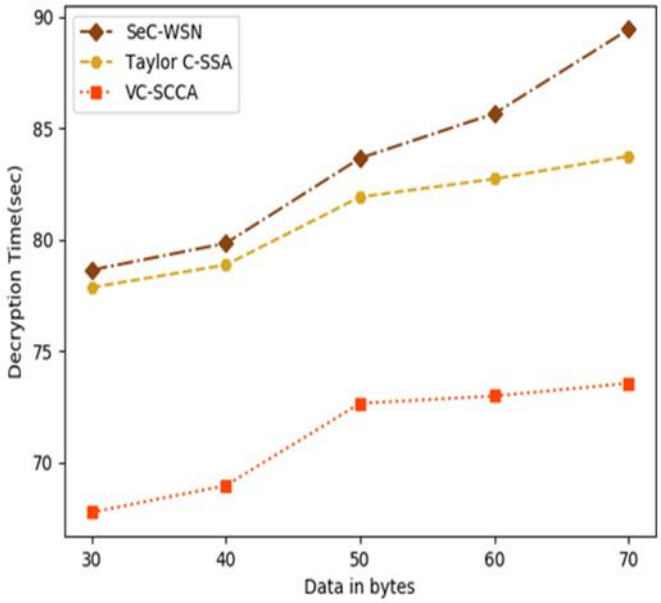

Figure 6: Comparison of decryption time with the existing and proposed methods

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 decryptiontime in seconds respectively. The proposed method takes 71.2sec 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

Parameters	**Existing SeC-WSN [11]**	**Existing Taylor C-SSA [12]**	**Proposed VC-SCCA**
Energy consumption (%)	73	61.2	53.2
Network Lifetime (%)	90	91.4	97.5
Packet Delivery Ratio (%)	71.3	96	98.6
Encryption time (sec)	80.6	71.8	62.8
Decryption time (sec)	83.4	81	71.2

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 achieves53.2% of energy consumption, 97.5% of network lifetime, 98.6% packet delivery ratio, 62.8sec of encryption time and 71.2sec decryption time.

References

1. Y. Swathi, S. Chitnis, “Game theory trust model with authentication and AES encryption (GTAAES) model for secure data aggregation in WSN”, International Journal of Advanced Sciences and Technology, vol.29, pp.2193–2207, 2020.

2. L. Zhou, Y. Shan, “Privacy-preserving, energy-saving data aggregation scheme in wireless sensor networks”, Journal of Inf. Process. Syst., vol.16, no.1, pp.83–95, 2020.
3. G.MN Veerabadrappa, P.M. Booma, “ESDAM - efficient and secure data aggregation against malicious nodes in Iot environment”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.9, no.2, pp.2278–3075, 2019.
4. Masdari M, Bazarchi S.M, Bidaki M, “Analysis of secure LEACH-based clustering protocols in wireless sensor networks”, Journal of Networks and Computing Applications, vol.36, no.4, pp.1243-1260, 2013.
5. T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis and P. Karkazis, “A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks”, Wireless Personal Communications, vol.69, no.2, pp.805-826, 2012.
6. J. Duan, D. Yang, H. Zhu, S. Zhang and J. Zhao, “TSRF: A TrustAware Secure Routing Framework in Wireless Sensor Networks”, International Journal of Distribution Sensor Networks, vol.2014, pp.1-14, 2014.
7. T. Eissa, S. Abdul Razak, R. H. Khokhar and N. Samian, “Trust-Based Routing Mechanism in MANET: Design and Implementation”, Mobile Networks Applications, vol.18, no.5, pp.666-677, 2013.
8. G. Zhan, W. Shi and J. Deng, “Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs”, IEEE Transactions on Dependable Security Computing, vol.9, no.2, pp.184-197, 2012
9. Hassan A, Anter A and Kayed M, “A Robust Clustering Approach for Extending the Lifetime of Wireless Sensor Networks in an Optimized Manner with a Novel Fitness Function”, Sustainable Computing: Informatics and Systems, 2020
10. Ghosal A, Halder S and Das S. K, “Distributed on-demand clustering algorithm for lifetime optimization in wireless sensor networks”, Journal of Parallel and Distributed Computing, 2020.
11. Vishnu V. M and Manjunath P, “SeC-SDWSN: Secure cluster-based SDWSN environment for QoS guaranteed routing in three-tier architecture”, International Journal of Communication Systems, vol.32, no.14, 2020.
12. Vinitha A and Rukmini M. S. S, “Secure and energy aware multi-hop routing protocol in WSN using taylor-based hybrid optimization algorithm”, Journal of King Saud University-Computer and Information Sciences, 2019.
13. Alghamdi, Turki A, “Secure and energy efficient path optimization technique in wireless sensor networks using DH method”, IEEE Access, vol.6, pp.53576-53582, 2018.
14. Amuthan A and Arulmurugan A, “Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in WSNs”, Journal of King Saud University-Computer and Information Sciences, 2019.
15. Mehmood A, Khanan A, Umar M. M, Abdullah S, Ariffin K. A. Z and Song H, “Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks”, IEEE Access, vol.6, pp.5688-5694, 2017.
16. Cengiz, Korhan and Tamer Dag, “Energy aware multi-hop routing protocol for WSNs”, IEEE Access, vol.6, pp.2622-2633, 2016.
17. Sampathkumar, A., Murugan, S., Rastogi, R., Mishra, M.K., Malathy, S. and Manikandan, R., 2020. Energy Efficient ACPI and JEHDO Mechanism for IoT Device Energy Management in Healthcare. In Internet of Things in Smart Technologies for Sustainable Urban Development (pp. 131-140). Springer, Cham.