SCDAP – Secured Cluster based Data Aggregation Protocol for Energy Efficient Communication in Wireless Sensor Networks

Lavanya Gunasekaran (lava@auist.net)
Anna University
B L Velammal
Anna University
Kulothungan K
Anna University

Research Article

Keywords: Wireless Sensor Networks, Data Aggregation, Energy Optimization, efficient Authentication, Key generation

Posted Date: September 28th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2067051/v1

SCDAP – Secured Cluster based Data Aggregation Protocol for Energy Efficient Communication in Wireless Sensor Networks

1) Lavanya G*

Research Scholar,
Department of Information Science and Technology,
College of Engineering Guindy,
Anna University, Chennai,
Tamil Nadu, India – 600 025.
E-mail: lava@auist.net
*Corresponding author

2) Velammal B L

Associate Professor,
Department of Computer Science and Engineering,
College of Engineering Guindy,
Anna University, Chennai,
Tamil Nadu, India - 600 025.
E-mail: velammalblceg@gmail.com

3) Kulothungan K

Associate Professor,
Department of Information Science and Technology,
College of Engineering Guindy,
Anna University, Chennai,
Tamil Nadu, India - 600 025.
E-mail: kulo.tn@gmail.com

Abstract:

A network of real time devices that can sense and transmit the information from the deployed environment by using multi hop communication is called as Wireless Sensor Network (WSNs). Despite the rapid advancement of WSN, where an increasing number of physical devices so called as sensors nodes are connected with each other, providing theimproved security withoptimized energy consumption during data transmission, communication and computation remains huge challenge. In wireless sensor networks, numerous sensor nodes are deployed in the physical environment to sense and collect the required information from the given environment. The sensed information are needed to be transmitted from the nodes to the control station in an energy efficient manner. Data aggregation is one kind of techniques which willoptimize the energy usage in wireless sensor networks during the data transmission. In data aggregation, the unnecessary data is removedwhich will significantly reduce energy of the nodes during data transmission. However, collected data during the data

aggregation should be completely protected and there are various threats that can be launched by the intruders to carry out unauthorised data access and can cause threat to the integrity of the network. Therefore, ensuring data security during the data aggregation process is very important and essential for the security of the network. In this paper, a Secure Cluster based Data Aggregation Protocol (SCDAP) have been proposed to provide better security through secure authentication and verification process, and to reduce overall energy consumption of the network by implementing secure clustering process to eliminate the redundant data in the network. Moreover, the proposed system is more efficient in generating public and private keys for effective and secure data transmission and verification process. The proposed system is experimentally tested in NS3 tool and proves that the proposed system reduces high energy consumption, computational and communicational cost, end-to-end delay and improves the packet delivery ratio. Moreover, the proposed system provides better security in the network when compared to other existing systems during the data aggregation.

Keywords: Wireless Sensor Networks, Data Aggregation, Energy Optimization, efficient Authentication, Key generation.

1. Introduction

Wireless sensor networks is a distributed collection of autonomous tiny sensor nodes which are deployed in given geographical location to sense andgather the physical information from the deployed environment and transmit the gathered information to the control station by using multi hop communication with radio signal as a communication medium[1]. Generally, the devices of WSN are called as smart objects which can able to sense the data from the deployed environment, process the sensed data and transmit data to other devices basedonby using multi hop communication with collaborative processing. Due to the resource constrained nature for the nodes in WSNs, providing energy optimization for the nodes of WSN, is a major challenge [2]. Since the nodes of WSNs, sense the information from the deployed environment and transmit the sensed information to nearest neighbour by using multi hop communication. By doing so, the same information has been sent by all the devices which results in redundant transmission [3]. Due to this concern, the energy consumption of the nodes in WSNs increases and results in the reduction of life time of devices in the network. Data aggregation is the fundamental mechanism for addressing these issues and provide better energy optimization in order to enhance the life time of the nodes in WSN. The major goals of data aggregation techniques in the WSN is to optimize the energy consumption of nodes and to achieve better QoS, which includes low data transmission latency, high reliability of data , low energy usage, and better consideration of data

priority[4]. In WSN, data aggregation is a smart process that collects and aggregates the data from numerous deployed sensors and then integrates it using an aggregation function to reduce the amount of data traffic injected into the system[5]. Indeed, the main idea behind data aggregation in WSN is to perform aggregation on devices in order to reduce the number of packets sent to the sink and, as a result, it causes reduction in network energy consumption[6]. In WSN, data aggregation provides three major benefits for diverse IoT systems: 1. Decreased injected traffic; 2. significantly reduced data transmission delay; and 3. Improved energy usage of WSN devices[7]. As a result, utilising data aggregation in the devices of WSN enhances the life of the nodes in the network[8].Due to the resource nature and communication medium of the WSN in an open channel, the devices of WSN is vulnerable to various types of attacks which are possible in the network during data aggregation[9]. The intruder can launch various active attacks and passive attacks which can cause harm to the network in terms data integrity and launch false data injection during data aggregation process[10]. By launching the false data injection attack, the data send during the data aggregation has been modified by the intruder and incorrect and malicious data will be transmitted to the base station[11]. By doing so, the intruder gains overall control of the network and compromise all the nodes during data aggregation process[12]. Considering all these scenarios, it is very much needed to provide efficient security with effective authentication during data aggregation process[13]. Motivated from these observations, in this paper an efficient Secured Cluster based Data Aggregation Protocol (SCDAP) protocol has been proposed which can able to provide efficient and secured data aggregation for the devices of the WSN. Moreover, the proposed SCDAP provides efficient clustering of nodes, provides efficient route discover for inter cluster and intra cluster communication, providing of efficient intermediate authentication by employing efficient key generation, encryption, decryption and providing efficient generation of signature and effective validation of generated signature to ensure the better authentication of the devices in WSN . Moreover, the proposed protocol provides efficient key revocation which prevents the intruders to launch side channel attack and reply attack during the data aggregation.

2. Literature Survey

Many researchers have proposed numerous methods for providing efficient and secured data aggregation for the devices in the WSN. Among them Onesimu JA et al.[14] have proposed a workable Privacy-Preserving Data Collection (PPDC) system. The suggested method conforms with healthcare security requirements and defends against sybil and other attacks

which aims for quick privacy-preserving data aggregation. This system secures the network privacy by using the client-server-to-user method. In their work, clustering-based k-anonymity model with -dissociation is used on the client side to anonymize the sensor nodes' data. By using this clustering technique, the privacy is therefore guaranteed. In contrast, the server employs the cluster-combination method to optimize communication costs and enhance privacy.Lightweight Secure Data Aggregation Scheme in Healthcare Using IoT (LSDA) was proposed by Othman SB et al.[15] Whereas this unique technique was described using a homomorphic encryption. The network can filter out erroneous packets and the nodes can conserve power during the transmission phase if each aggregator checks all the packets it receives from its member nodes. The LSDA scheme has four major steps namely encryption, authentication, aggregation, and decryption and verification. The integrity is checked using a homomorphic MAC algorithm. The proposed system makes it more difficult for the intruder to compromise the code, take control of the Aggregator, and disrupt or attack the entire network during the data aggregation. For Wireless Body Area Network (WBAN) systems, Sharmila AH et al. [16] have developed an Enhanced MAC-based secure delay-aware Healthcare Monitoring System (E-MHMS). The suggested approach guarantees efficient and safe data aggregation, with data divided into three categories namely crucial data, nearly critical data, and normal data. First, each authorised node receives keys from the base station (BS). The crucial data in E-MHMS is encrypted using the asymmetric RSA (Rivest-Shamir-Adleman) method before being sent to BS over exclusive channels. The proposed system is secured using the time-based elliptic curve technique. For every round, the key is distributed to all the legitimate nodes in the network. E-MHMS can withstand DoS attacks that affect communication in the network. The limitations are it uses numerous encryption algorithms, which consumes a lot of energy and causes computational and communication overhead in the network.In order to provide optimal data flow and secure patient data gained access control, Arul R et al. [17] have proposed "Multi-Modal Secure Data Dissemination Framework (MMSDDF)". The goal of the suggested framework is to lessen sybil attacks and other types of attacks. The blockchain uses timestamps and hash functions to prevent message tampering by attackers. In order to ensure that credentialed healthcare providers can get patient health information, the proposed system also includes a trustworthiness assessment approach for messages. This approach also allows for the detection of the attack and temporary removal of the malicious node, enabling the malicious node to be blacklisted upon agreement between the source and destination nodes. The limitations are the blacklisted list of malicious nodes are maintained on the block chain which causes overhead in terms

computation and communication.To ensure the privacy-preserving access control on the Internet-of-Medical-Things, Kumar M. et al. [18] have proposed "Escrow-Free Identity-based Aggregate Sign-encryption system to secure data transmission (EF-IDASC)" (IoMT). The proposed System's works on three stages are employed to secure data transmission between each component. Protecting the communications between all sensor nodes inside and outside the WBAN should come first, followed by securing the sensor nodes inside the WBAN. Data transmission is protected by the Identity-based Aggregate SignCryption (EF-IDASC) technique in the proposed system. Although the system has successfully demonstrated the key security aspects, communication costs are considerable.Tang Wet al [19] have proposed a multi-level aggregation strategy, in which devices provides health data sign the data and integrates with identity-based signature at the first level. To protect against differential attacks at a deeper level, healthcare facilities add noise to the data using differential privacy before sending the ciphertext to the cloud server. At the third layer, the cloud combines and decrypts the jumbled health data gathered from numerous healthcare facilities. Security research shows that the method can survive various attacks. However, the proposed technique provides significant cost computation advances.LDAC-KS, a lightweight distributed access control system with keyword search, has been proposed by Yang Yang et al. [20]. The recommended approach enables distributed access control of protected health data across numerous medical specialties. The method may offer a useful keyword search tool for cross-domain protected health information. The proposed system uses minimal data encryption, keyword trapdoor construction, and data recovery by using small amount of processing power from the user's terminal. The proposed technique considerbly reduces transmission costs while improving the efficiency of cost computation.J. Liu et.al [21] have proposed "Verifiable Data Aggregation Scheme (VDAS) for Internet of Things." In their system, KGC generate cryptographic keys which are employed for encryption and decryption. The data from the terminal nodes is combined by the aggregator nodes and append their own signature to the data being sent using the batch key mechanism. However, when aggregated data is concatenated by using the batch key approach and when the is signature is added, the size of the data grows, which increases the cost of computation and communication in the network.S. O. Ogundoy et al. [22] have proposed the system to protect user identification and conceal the physical location of devices. Additionally, the method lowers the cost of computation and transmission while defending against a number of security vulnerabilities. Data anonymity and node authentication are provided through an anonymous and secure aggregated system (ASAS), which also guarantees the integrity of the data. The query is sent to the PCS by the

terminal nodes for authentication. Following authentication, FN collects all of the TDs' encrypted messages and aggregates them using the batch key approach. The combined data is then forwarded to PCS. At the PCS, the cost of communication is still significant.A time scheduling approach that uses movable sink nodes to effectively gather data was proposed by Wang et al. [23], where the transmission cost is minimised by using the minimal spanning tree with each mobile sink node travelling along its own route. The energy consumption of the system and the transmission latency both grow as the number of sensor nodes increases.An effective task offloading strategy based on that encourages mobility was proposed by Ning et al. [24]. A sustainable system that allows job offloading from the heavily used cloud to the less used one is built using the ball and bins principle. Additionally, it offers defence against DDoS attacks and only allows authenticated users to compute data.Sui et al. [25] have created a strong and effective secure aggregation method that employs hash-based message authentication and ElGamal encryption to safeguard the confidentiality, integrity, and authenticity of data. However, the discrete logarithm problem must be resolved during decryption for the ElGamal encryption system that supports homomorphic operations. Therefore, only small range data aggregation is supported by the technique. The two other techniques, multipurpose, also have issues with the constrained data range.The IDAP protocol is proposed by S. Kumar et al. [26] to provide a data aggregation mechanism for batch key-based verification. The collector node uses the batch key technique. All smart gadgets transfer data in batches, multiplying it by one after another, and so forth, before sending it to PCS. However, there is still room for improvement in the transmission cost of the proposed scheme. In both the aggregate and transmission phases of PPDA, authors protected the confidentiality of the data. Additionally, the data from the sensor nodes is aggregated using a batch key approach. The computing cost is increased by complex multiplication processes.Lin et.al[27] have proposed an innovative multidimensional privacy-preserving DA approach for wireless sensor networks which combines the super increasing sequence and perturbation techniques. The privacy of aggregated data is at risk due to the neighbour sensor node sharing its private key with the aggregator node. A superincreasing sequence of huge primes was established by Lu et al. [28] and paired with Paillier encryption to provide an effective and privacy-preserving aggregation strategy (EPPA) for the smart grid. Additionally, to speed up the multidimensional data encryption process, they utilised the multigeneration pattern.Jia et. al[29] have proposed a human-factor-aware privacy-preserving aggregation approach, in which multidimensional data are encrypted by a randomised and a few secret keys, makes use of safe multiparty computation techniques. This system is

unsecure, nevertheless, as multiple nodes can share the same multidimensional data and leak secret keys. Based on bilinear pairing cryptography. Liu et al. [30] proposed an anonymous multidimensional DA system in which reported data are aggregated in plaintext form to allow addition and non-addition operations. A two-subset DA technique was proposed by Lu et al. [31] that used the fractional-order group to encrypt various dimensions data.To achieve adaptive contextual privacy and security in WBAN, context-aware access control and authentication based on attribute-based sign encryption and identity-based sign encryption have been proposed by A. Arfaoui [32]. They developed certificateless sign encryption, which ensures that only partial private keys generated by key generation centres, to address the key escrow issue and prevent impersonation attacks (KGC).The importance of access control in WBAN has been highlighted by Hong et al. [33], who combined threshold access policy with attribute-based encryption (ABE), ciphertext policy attribute-based signature (CP-ABS), and attribute-based encryption (ABE). A plan for data aggregation from various data sources in e-healthcare IoT devices has been put forth in another work by Tang et al. [34]. In order to achieve their goals of protecting patient privacy and provide just rewards for medical data, they used the BGN cryptosystem with Shamir's secret sharing scheme.MuhamedTurkanoviü et.al [35] have proposed a key agreement system for the Internet of Things, in which hash functions and XOR operations lessen the amount of processing that takes place in a limited node. Here, the gate way node produces a shared password during the pre-deployment stage and sends it via an insecure channel. As a result, impersonation attacks is caused by the attacker in the network. The overall observation from the literature survey is that most of the existing data aggregation protocols fails to provide efficient privacy and enhanced authentication during data aggregation. More most of the existing data aggregation protocols subjected to false data injection attacks and suffers from considerable computation and communication overhead. Motivated from these observations, in this paper an efficient Secured Cluster based Data Aggregation Protocol (SCDAP) protocol has been proposed which can able to provide efficient and secured data aggregation for the nodes in WSN

3. Secured Cluster based Data Aggregation Protocol (SCDAP)

The main goal of the proposed SCDAP protocol is to provide energy efficient and secured data aggregation to the devices in WSN. The SCDAP protocol works on five phase’s namely key generation phase, network cluster formation phase, secured data aggregation phase, data transmission phase and data reception phase. In key generation phase, the public and private

key are generated by employing Diophantine power equation which is uses all unknown integers to solve unknown problems. The advantages of using this equation in generation of keys is to ensure the randomness during key generation and in multiparty key exchange. The second phase is network cluster formation phase. In this phase, the nodes of the network are grouped into various clusters and each cluster have the corresponding clusters along with their cluster members. The third phase is secured data aggregation phase. During this phase, the data's are aggregated by the CH and it is transmitted to the BS in a secured manner with help of mutual authentication among member nodes to CH and CH to member nodes and finally CH to Base station. The next phase is data transmission phase. In this phase data is transmitted in a secured manner by encrypting it with the sender private key and signing them by employing digital signature algorithm. In data reception phase, the receiver nodes validates the incoming data by decrypting with their public key and verifies the signature by using message verification algorithm. If signature is found correct, the received devices forwards the packets to the next Neighbour nodes else the received packets are discarded by the receiver nodes in the network.

3.1 Key generation phase

The initial phase of the proposed system is key generation phase. The main goal of this phase to generate public key and private key for secured data aggregation to the devices in the WSN. For efficient generation of the Diophantine equation is using all unknown integers to solve unknown problems in the equation. Equation (1) gives Diophantine power equation. Algorithm 1 generates public and private key.

Algorithm1: Key Generation

Diophantine power equation will be $P^3 - XQ^3 = 1$----- (I)

1. Let consider X be the prime number
2. Let consider integer pair as (P,Q)
3. Choose value for s, t, u, Φ(v), y and z
4. Calculate γ using

   $\gamma = [\Phi(v) + P]^3 - X[y + Q]^3$ --- (II)

$$\gamma = \Phi(v)^3 + P^3 + 3\Phi(v)P^2 + 3\Phi(v)^2P - Xy^3 - XQ^3 - 3XyQ^2 - 3X^2Q \text{ ----- (1)}$$

5. Calculate public key β using γ from (1)

$\beta = [\gamma + Xy^3 + 3XQ^2 + 3Xy^2Q] * b^3 mod\ \Phi(v)$ -------- (2)

b^3 is used to multiply in the equation (2) since the power of equation is (I) is cubic.

6. Private key = y^3 since the power of equation is 3
7. Public key is dependent on γ from equation (II), P,Q,X of equation (I) and s,t component.

By employing generated public key and private key the encryption and decryption of the aggregated data takes place for establishing the secured data transmission in the devices in WSN.

4.2 Network clustering phase

In the network clustering phase, the sink node chooses the Cluster Head (CTH) node based on sensor nodes Residual energy (Res_Eng), Distance (D) and Throughput (TP) among the neighbours' nodes in the network. The Sink node starts the selection process of Cluster Head (CTH) and makes decision from n number nodes to generate the efficient clusters in the network. Algorithm 2 gives cluster head selection.

Algorithm2: Cluster Head Selection

Input: Set of sensor nodes $SNn = \{SN1, SN2, \ldots\ldots SNn\}$

Output: Cluster Head (CTH)

Step 1: For all clusters formed in the network, store them into a vector CLT as follows

$$C = \{CLT1, CLT2, \ldots\ldots\ldots\ldots CLTn\}$$

Step 2: For every sensor node in every cluster C, find Distance (D)

D = Maximum Distance between two sensor nodes in each cluster.

D = $\sqrt{(x2 - x1)^2} - \sqrt{(y2 - y1)^2}$

The sensor node which is having high hop distance is selected for cluster head selection process.

Step 3: Store Residual energy (Res_Eng) for each sensor nodes in vector as

$Res\_Eng_{\ n} = \{Res\_Eng1, Res\_Eng2, \ldots\ldots\ldots\ldots Res\_Eng\ n\}$

Step 4: Find $HIGH\_Res_{Eng}$ among the sensor nodes Res_Eng

$$HIGH\_Res\_Eng = max\{Res\_Eng1, Res\_Eng2, \ldots\ldots\ldots Res\_Eng\ n\}$$

Step 5: Find $Throughput\ (TP)$ for every sensor node $SNn = \{SN1, SN2, \ldots\ldots SNn\}$

$$TP = Total\ number\ of\ transmission\ by\ each\ sensor\ nodes\ /\ time$$

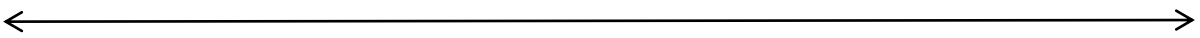
Step 6: Find an efficient Cluster Head (CLH)

$If\ (TP == High\ \&\&\ Res\_Eng == High\ \&\&\ D == medium)$

$Then$

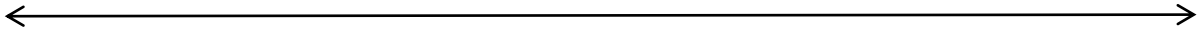
"$Select\ the\ corresponding\ node\ as\ CTH$"

$$else\ repeat\ steps\ 2\ to\ 5$$



In this phase, the sensor node which is having high throughput with minimum residual energy and distance is selected as Cluster Head (CTH). Various number of clusters are formed based on the two parameters namely Residual energy and Mean hop count.

Algorithm3: Cluster formation



N-means Clustering

Input: Sensor nodes (SN1, SN2, ..., SNn)

M- Maximum number of clusters

Output: Best Cluster

Begin

(K=2)-means (CL) => Cluster

TopScore => α

```
While | Cluster | < M do
    New Cluster = { };
  For every Cn € Cluster do
        CL (Cn) =C2n;
    If SIC (Cn) > SIC (C2n) then
        New Cluster U Cn = New Cluster;
        Else
           New Cluster U C2n = New Cluster;
        End
    End
  End
New Cluster = Cluster
If SIC (Cluster) >TopScore then
   SIC (Cluster) = TopScore;
   Cluster = BestCluster
End
End
return BestCluster
End
```

N-means algorithm takes sensor nodes and maximum number of clusters as an input. The maximum number of clusters are estimated by the equation (1) which takes the square root value with half the sensor node size as maximum and two commonly used as minimum.

$K = \frac{\sqrt{|N|}}{2}$ ----- (1)

The (k=2) - means algorithm gives two clusters from the given sensor nodes. In this newly applied algorithm, cluster are formed based on Schwarz Information Criterion (SIC) Score given in the equation (2).

$SIC\ (Mi)\ = Li\ (N) - Pi/2 * log\ |N|$ ------- (2)

Where Li (N) is log likelihood of sensor nodes and Pi is the number of parameters in Mi

If SIC Score is less than (k=2) – means cluster, then replace the original cluster with their cluster. Or else, retain the original cluster as it is. Finally, the cluster with best SCI is selected as Best Cluster.

4.3 Secure Data aggregation phase

The next phase of the proposed protocol is secured data aggregation phase. In data aggregation phase initially CTH collects the sensor nodes information and data which is needed to be transmitted. Then the Cluster head (CTH) sends all sensed data to the Aggregated Cluster Head (ACH) and finally ACH sends the data to BS in a secured manner. Algorithm 4 gives steps to be followed for Cluster head (CTH) collects Sensor nodes information (SNn) and Algorithm 5 gives the steps to be followed by Cluster head (CTH) sends all sensed data to the Aggregated Cluster Head (ACH). Algorithm 6 gives the steps to be followed for encrypting and decrypting the data for providing efficient secured data transmission from ACH to BS.

Algorithm 4: Cluster head (CTH) collects Sensor nodes information (SN_n)

1. *For all clusters in the network,*
2. *Sink node sends* (ID_{SN}, Res_Eng_{SN}, TP_{SN}, RP_{SN})*where*
   ID_{SN} *is a Identification of sensor nodes,*
   Res_Eng_{SN}= *Total energy – Consumed energy,*
   TP_{SN} *is a Total number of packets sent and*
   RP_{SN} *is a Total number of packets received.*
3. *Cluster head forms matrix for Cluster head Aggregation* (A_{CTH})

$$A_{\text{CTH}} = \begin{pmatrix} ID & Res\_Eng & TP & RP \\ SN1 & SN1 & SN1 & SN1 \\ . & . & . & . \\ . & . & . & . \\ SNn & SNn & SNn & SNn \end{pmatrix} - - - - - - - - - (1)$$

Algorithm 5:Cluster head (CTH) sends all sensed data to the Aggregated Cluster Head (ACH)

1. *For all cluster heads* (CTH) *in the network,*
2. *Sink node sends* (ID_{CTH}, A_{CTH})*were*
3. ID_{CTH}*is a Identification of cluster heads*

A_{CTH}

is a Aggregated sensor information collected from each cluster by the cluster head

4. *Sink node forms a matrix ACH*

5. $A\text{CH} = \begin{pmatrix} ID & ACTH \\ CTH1 & CTH1 \\ . & . \\ . & . \\ . & . \\ CTHn & CTHn \end{pmatrix}$ ----------(2)

4. *Sink node collects and communicates with ACH.*
5. *Hence the sink node contains a Overall Aggregation in the form of matrix* $(Overall\_Agg)$

$$Overall\_Agg = Equation\ (1) + Equation\ (2)$$

$$Overall\_Agg = \begin{pmatrix} ID & Res\_Eng & TP & RP \\ SN1 & SN1 & SN1 & SN1 \\ . & . & . & . \\ . & . & . & . \\ SNn & SNn & SNn & SNn \end{pmatrix} + \begin{pmatrix} ID & ACTH \\ CTH1 & CTH1 \\ . & . \\ . & . \\ . & . \\ CTHn & CTHn \end{pmatrix} - - - (3)$$

Algorithm 6. ACH sends the data to BS

// Encryption procedure //

1. Generated public key (β, v) is received.
2. The source node wants to send the message (MGS) which is represented in terms of positive ASCIII value integer.
3. Encrypt the message (MGS)

   $C(MGS) = MGS^{\beta} mod\ v$ ------ (3)
4. The cipher text of the message (MGS) will be C (MGS) which is sent to receiver sensor node.

Equation (3) is used for encrypting the data with public key. The equation (3) gives the encrypted data which has to be transmitted from the source node to the destination node until it researches to the BS.

// decryption process//

1. Private Key (y^3, v) is used to decrypt the cipher text of the original message C (MGS) received from the source node.

   MGS(C) = C^{y^3} mod v ------ (4)
2. Hence, original message MGS is received in the equation (4).

The equation (4) provides the original data to the required destination node after successful decryption of the message which is needed to be transmitted to the BS.

5. Performance Evaluation and Results

The proposed protocol SCDAP is tested and evaluated with various existing protocols namely EPPA, EPPADA and SLC-DAA by using NS3 network simulator. The performance metrics employed by the proposed protocol namely energy consumption, communication overhead, computational cost, End-to-End delay and packet delivery ratio. Table 1 gives the simulation parameter for the proposed protocol.

Name of the Simulator	NS3
Network Area	500*500 M^2
Deployed sensor nodes	800
Original energy	3J

Transmission Energy	0.75J
Receiving Energy	0.38J
Data size	3090 bits
Total Rounds	55
Network Coverage	100 – 150 M
Generation model	Two ray model

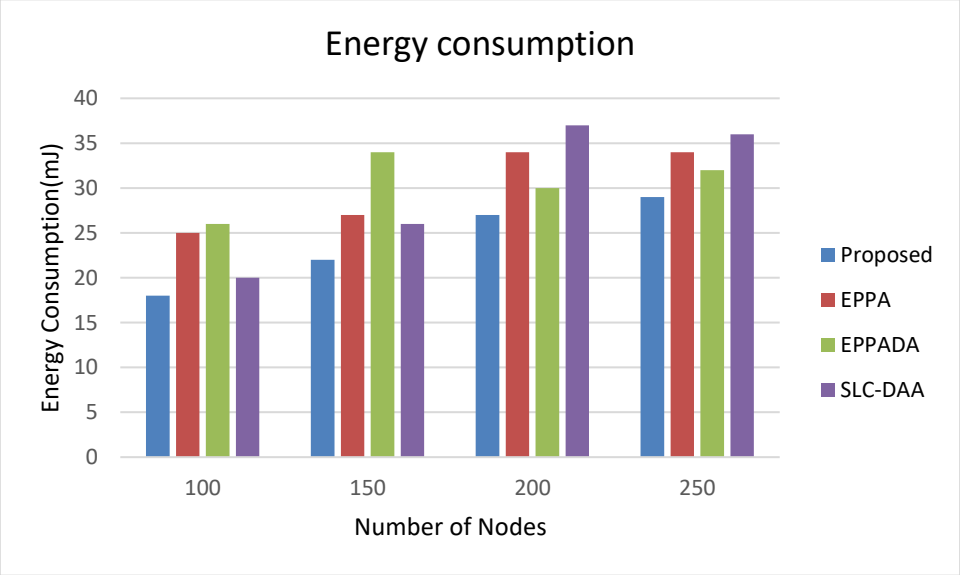


Figure 1: Energy Consumption

Figure 1 gives the comparative analysis of overall energy consumption of the sensor nodes from various existing algorithms. From the figure it is understood that the proposed protocol provides better communication overhead in the network when compared to other existing protocols. The proposed employs efficient data aggregation and clustering of sensor nodes for reducing the overall energy consumption in the network. Thereby the proposed protocol has significant reduction in both control messages and data messages in the network and reduces redundant data in the network. By doing so, the proposed protocol reduces the processing of both control messages and data messages. Hence the proposed system consumes better energy when compared to other existing protocols.

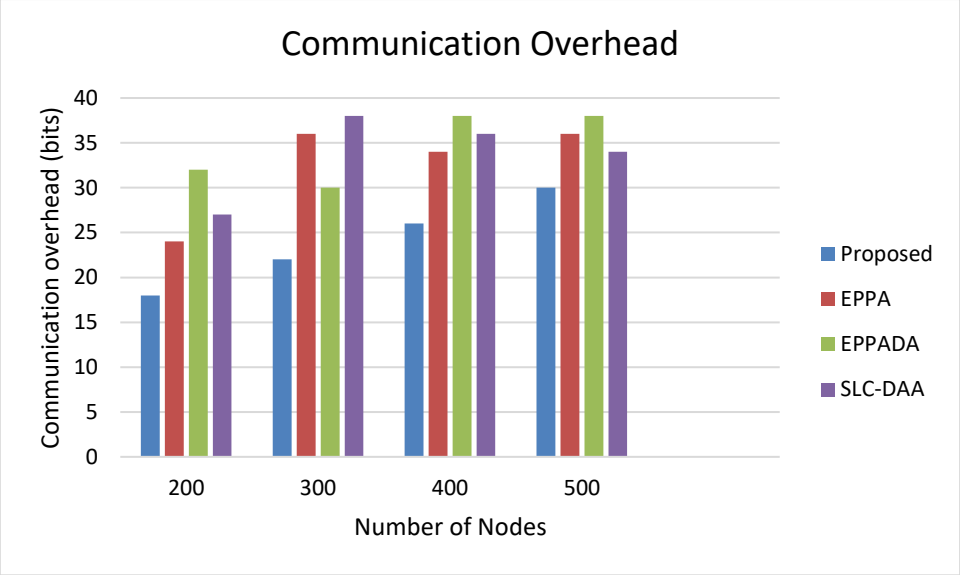


Figure 2: Communication Overhead

Figure 2 gives the comparative analysis of overall communication overhead of the sensor nodes from various existing algorithms. From the figure, it is understood that the proposed protocol provides better communication overhead in the network when compared to other existing protocols. The proposed employs efficient data aggregation and clustering of sensor nodes for reducing the overall energy consumption in the network. Thereby the proposed protocol has significant reduction in both control messages and data messages in the network and reduces redundant data in the network. By doing so, the proposed protocol reduces the processing of both control messages and data messages. Hence, the proposed protocol has better communication overhead when it is compared with other existing protocols.

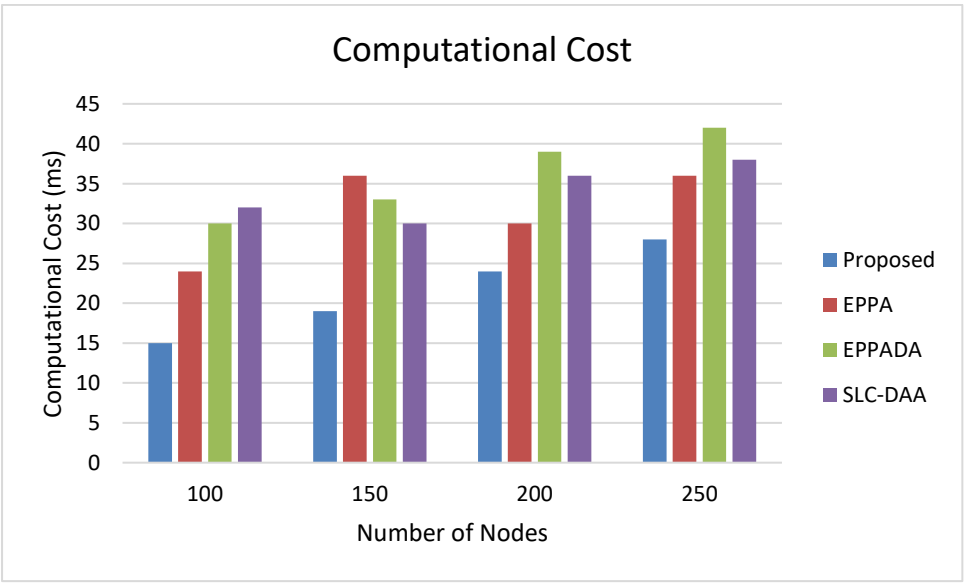


Figure 3: Computational cost

Figure 3 provides better computational cost when compared to other existing protocols. The proposed protocol uses secure key generation and authentication techniques for secure data transmission and reception by avoiding malicious activities in the network.By doing so, the proposed protocol limits the impact of malicious nodes in the network by reducing the packet drop ratio and increase in the packet delivery ratio. Moreover, the proposed protocol has significant reduction in both control messages and data messages in the network and reduces redundant data in the network. By doing so, the proposed protocol reduces the processing of both control messages and data messages. Hence, the computational cost of the overall network is reduced by the SCDAP protocol.

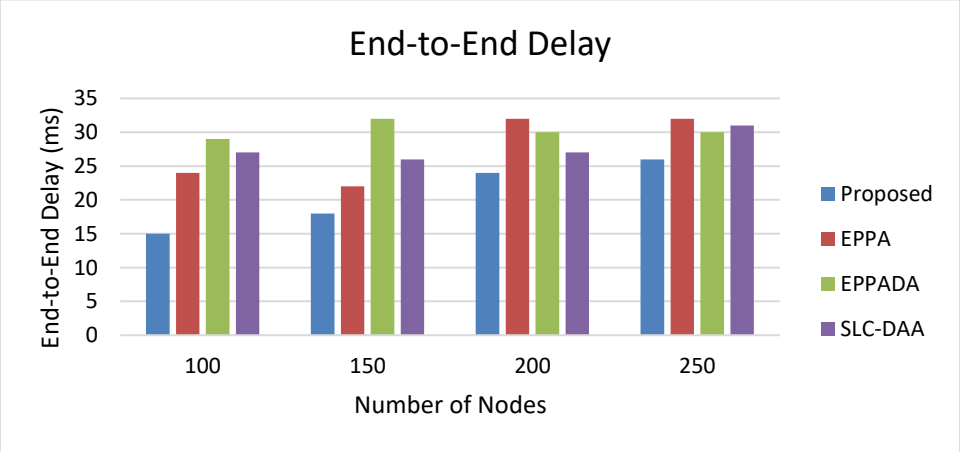


Figure 4: End-to-End Delay

Figure 4 provides better end-to-end delay of the proposed protocol when compared it is compared with other existing protocols. The proposed system uses efficient clustering and data aggregation of sensor nodes thereby it reduces the propagation delay and queuing delay in the network in a significant manner. Moreover, the proposed protocol has significant reduction in both control messages and data messages in the network and reduces redundant data in the network. By doing so, the proposed protocol reduces the processing of both control messages and data messages. Hence, the proposed protocol have better end to end delay when it is compared with other existing protocols.

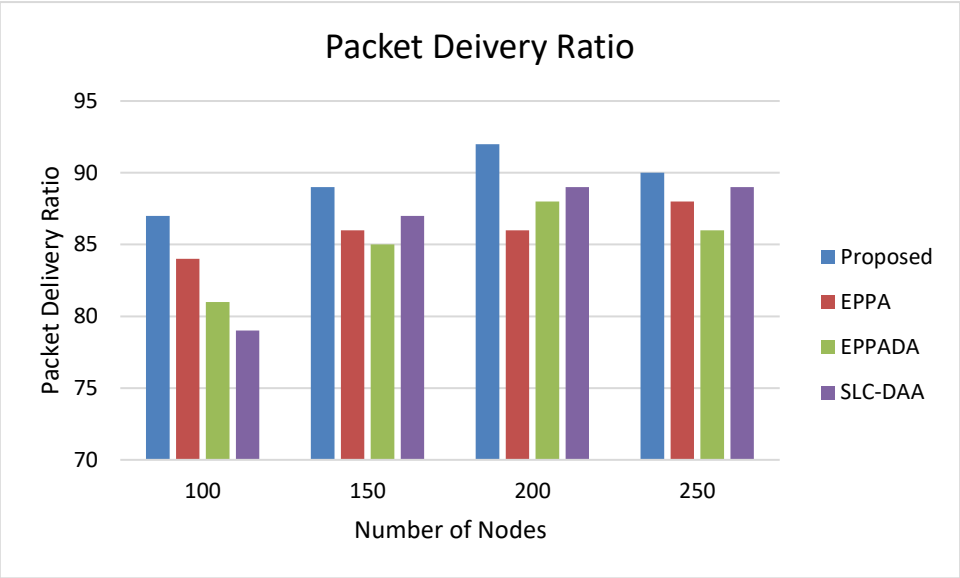


Figure 5: Packet Delivery Ratio

Figure 5 provides better packet delivery ratio for the proposed protocol when it is compared with other existing protocols. The reason for the improvement is that the proposed system employs efficient and secured data transmission of data which providesbetter packet drop ratio. Moreover, the proposed protocol provides better security defense against various malicious nodes in the network. Hence, the proposed system better packet delivery ratio in comparison with other existing protocols.

6. Conclusionand future work

In this work, SCDAP protocol has been proposed to provide efficient and secure data aggregation in wireless sensor network. The main aim of the proposed protocol is to reduce the control messages and data messages sent across the network. The proposed protocol works in three phase's namely key generation phase, network clustering phase and secure data aggregation phase. The proposed protocol is implemented in NS3 network simulator with realistic simulation parameters. The results of the simulation is compared with other existing protocols with the performance metrics namely energy consumption, communication overhead, computational cost, end-to-end delay and packet delivery ratio. From the simulation results it is understood that the proposed protocols provides better packet delivery ratio, end-to-end delay and better computational and communicational overhead when it is compared with other existing protocols. Moreover, the proposed system provides better defense against various malicious activity in the network. The future work of the proposed

protocol is to provide secure and efficient data aggregation for the nodes which has mobility in the network and to improve the QoS parameters in the network.

References

1. G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," Future Gener. Comput. Syst., vol. 82, pp. 375–387, May 2018.
2. F. Rezaeibagha, Y. Mu, S. Zhang, and X. Wang, "Provably secure homomorphic signcryption," in Proc. 11th Int. Conf. Provable Security (ProvSec), Xi'an, China, Oct. 2017, pp. 349–360.
3. F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, and K. Huang, "Fully secure lightweight certificateless signature scheme for IIoT," IEEE Access, vol. 7, pp. 144433–144443, 2019.
4. J. Hong, B. Liu, Q. Sun, and F. Li, "A combined public-key scheme in the case of attribute-based for wireless body area networks," Wireless Netw., vol. 25, no. 2, pp. 845–859, 2019.
5. W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight e-Healthcare IoT devices with fair incentives," IEEE Internet Things J., vol. 6, no. 5, pp. 8714–8726, Oct. 2019.
6. Z. Wang, "Blind batch encryption-based protocol for secure and privacy preserving medical services in smart connected health," IEEE Internet Things J., vol. 6, no. 6, pp. 9555–9562, Dec. 2019.
7. D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in Proc. 2nd Conf. Theory Cryptography (TCC), Cambridge, MA, USA, Feb. 2005, pp. 325–341.
8. C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput. (STOC), Bethesda, MD, USA, May/Jun. 2009, pp. 169–178.
9. J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud assisted wireless wearable communications: Challenges, solutions, and future directions," IEEE Wireless Commun., vol. 22, no. 2, pp. 136–144, Apr. 2016.

10. X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, “Privacy protection for wireless medical sensor data,” IEEE Trans. Depend. Security Comput., vol. 13, no. 3, pp. 369–380, May/Jun. 2016.
11. M. Barbosa and P. Farshim, “Certificatelesssigncryption,” in Proc. IACR Cryptol. ePrint Archive, 2008, p. 143.
12. A. Arfaoui, O. R. M. Boudia, A. Kribeche, S. Senouci, and M. Hamdi, “Context-aware access control and anonymous authentication in WBAN,” Comput. Security, vol. 88, Jan. 2020, Art. no. 101496.
13. X. Liu, R. H. Deng, W. Ding, R. Lu, and B. Qin, “Privacy-preserving outsourced calculation on floating point numbers,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2513–2527, Nov. 2016
14. Onesimu JA, Karthikeyan J, Sei Y. An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services. Peer-to-Peer Netw. Appl2021; 14:1629–49.
15. Othman SB, Bahattab AA, Trad A, Youssef H. LSDA : lightweight secure data aggregation scheme in healthcare using IoT. In: 10th International Conference on Information Systems and Technologies, Lecce, Italy, Dec 28, 2019 - Dec 30; 2019. https://doi.org/10.1145/3447568.3448530. Tunisia.
16. Sharmila AH, Jaisankar N. E-MHMS: enhanced MAC-based secure delay-aware healthcare monitoring system in WBAN. Cluster Comput 2020;23:1725–40. https://doi.org/10.1007/s10586-020-03121-2.
17. Arul R, Al-Otaibi YD, Alnumay WS, et al. Multi-modal secure healthcare data dissemination framework using blockchain in iomt. PersUbiquitComput 2021. https:// doi.org/10.1007/s00779-021-01527-2.
18. Kumar M, Chand S. A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. IEEE Internet Things J. Oct. 2020;7(10):10650–9. https://doi.org/10.1109/JIOT.2020.3006523.
19. Tang W, Ren J, Deng K, Zhang Y. Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. IEEE Internet Things J. 2019;6(5): 8714–26. https://doi.org/10.1109/JIOT.2019.2923261.
20. Yang Yang, Zheng Xianghan, Tang Chunming. Lightweight distributed secure data management system for health internet of things. J. Netw. Comput. Appl. 2017;89:26–37. https://doi.org/10.1016/j.jnca.2016.11.017.

21. J. Liu, J. Han, L. Wu, R. Sun, and X. Du, ‘‘VDAS: Verifiable data aggregation scheme for Internet of Things,’’ in Proc. IEEE Int. Conf. Commun. (ICC), May 2017, pp. 1–6.
22. S. O. Ogundoyin and S. O. Awoyemi, ‘‘EDAS: Efficient data aggregation scheme for Internet of Things,’’ J. Appl. Secur. Res., vol. 13, no. 3, pp. 347–375, Jul. 2018
23. T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, ‘‘Sustainable and efficient data collection from WSNs to cloud,’’ IEEE Trans. Sustain. Comput., vol. 4, no. 2, pp. 252–262, Apr. 2019.
24. N. Yang, X. Fan, D. Puthal, X. He, P. Nanda, and S. Guo, ‘‘A novel collaborative task offloading scheme for secure and sustainable mobile cloudlet networks,’’ IEEE Access, vol. 6, pp. 44175–44189, 2018
25. Z. Sui, M. Niedermeier, and H. de Meer, “RESA: A robust and efficient secure aggregation scheme in smart grids,” in Proc. Int. Conf. Crit. Inf. Infrastruct. Security, 2015, pp. 171–182.
26. X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, ‘‘Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 4755–4763, Jun. 2019
27. X. Lin, R. Lu, and X. Shen, “MDPA: Multidimensional privacy preserving aggregation scheme for wireless sensor networks,” Wireless Commun. Mobile Comput., vol. 10, no. 6, pp. 843–856, 2010.
28. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
29. W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, “Human-factor-aware privacy-preserving aggregation in smart grid,” IEEE Syst. J., vol. 8, no. 2, pp. 598–607, Jun. 2014.
30. X. Liu, Y. Zhang, B. Wang, and H. Wang, “An anonymous data aggregation scheme for smart grid systems,” Security Commun. Netw., vol. 7, no. 3, pp. 602–610, 2014.
31. R. Lu, K. Alharbi, X. Lin, and C. Huang, “A novel privacy-preserving set aggregation scheme for smart grid communications,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), San Diego, CA, USA, 2015, pp. 1–6
32. A. Arfaoui, O. R. M. Boudia, A. Kribeche, S. Senouci, and M. Hamdi, “Context-aware access control and anonymous authentication in WBAN,” Comput. Security, vol. 88, Jan. 2020, Art. no. 101496

33. J. Hong, B. Liu, Q. Sun, and F. Li, “A combined public-key scheme in the case of attribute-based for wireless body area networks,” Wireless Netw., vol. 25, no. 2, pp. 845–859, 2019.

34. W. Tang, J. Ren, K. Deng, and Y. Zhang, “Secure data aggregation of lightweight e-Healthcare IoT devices with fair incentives,” IEEE Internet Things J., vol. 6, no. 5, pp. 8714–8726, Oct. 2019

35. Mohammad SabzinejadFarash,,MuhamedTurkanoviü, SaruKumari, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment." Ad Hoc Networks 36 2016,pp. 152-176.

Ethical Approval

Not Applicable.

Competing interests

No, I declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Authors' contributions

Author 1 conceived of the presented idea. Author 1 developed the theory and performed the computations. Author 2 &3 verified the analytical methods, encouraged Author 1 to investigate [Energy optimisation techniques) and supervised the findings of this work. All authors discussed the results and contributed to the final manuscript.

Funding

No fund or grant received for this paper.

Availability of data and materials

No, all of the material is owned by the authors and/or no permissions are required.