ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/342694477

Enhancing performance of WSN by utilising secure QoS-based explicit routing

Article *in* International Journal of Computer Aided Engineering and Technology · January 2020

DOI: 10.1504/IJCAET.2020.108107

CITATIONS
2

READS
54

2 authors:

Kantharaju H C
Vemana Institute of Technology, Koramangala, Bengaluru
11 PUBLICATIONS **15** CITATIONS
SEE PROFILE

Narasimha Murthy K N
Christ University, Bangalore
26 PUBLICATIONS **45** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Energy Minimization in Cellular Networks View project

Project Surface Water Change Detection Modelling View project

All content following this page was uploaded by Narasimha Murthy K N on 21 September 2020.

The user has requested enhancement of the downloaded file.

Enhancing performance of WSN by utilising secure QoS-based explicit routing

H.C. Kantharaju*

Department of Computer Science and Engineering,
Vemana Institute of Technology,
Koramangala, Bengaluru, 560034, KA, India
Email: hc.kantharajuvit@gmail.com
*Corresponding author

K.N. Narasimha Murthy

Faculty of Engineering,
Christ University,
Bengaluru, 560074, KA, India
Email: murthy_knn@yahoo.co.in

Abstract: Wireless sensor networks (WSN) are infrastructure less and self-configured a wireless network that allows monitoring the physical conditions of an environment. Many researchers focus on enhancing the performance of WSN in order to provide effective delivery of data on the network, but still results in lower quality of services like energy consumption, delay and routing. We tackle this problem by introducing a new routing algorithm, *QoS-based explicit routing algorithm* which helps in transmitting the data from source node to destination node on WSN. We also involve clustering process in WSN based on *genetic algorithm and particle swarm optimisation (GA and PSO) algorithm*. We proposed identity-based digital signature (IBDS) and enhanced identity-based digital signature (EIBDS) that involves reduction of computation overhead and also increasing resilience on the WSN. We also use advanced encryption standard (AES), for ensuring the security between nodes and avoid hacking of data by other intruders.

Keywords: wireless sensor network; WSN; cryptography; digital signature; quality of service; QoS.

Reference to this paper should be made as follows: Kantharaju, H.C. and Murthy, K.N.N. (2020) 'Enhancing performance of WSN by utilising secure QoS-based explicit routing', *Int. J. Computer Aided Engineering and Technology*, Vol. 13, Nos. 1/2, pp.101–124.

Biographical notes: H.C. Kantharaju is a Research Scholar and Assistant Professor at the Department of Computer Science and Engineering, Vemana Institute of Technology, Koramangala, Bengaluru-560034, KA, India. Currently, he focuses on sensor networks related to clustering, routing and security in a real-time application manner.

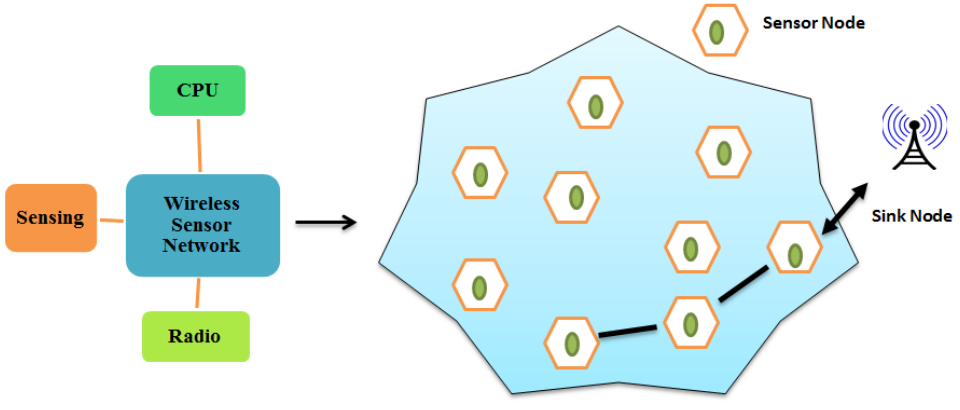
K.N. Narasimha Murthy is a Professor at the Faculty of Engineering, Christ University, Bengaluru-560074, KA, India. He currently focuses on the type of adhoc and sensor networks. He is participated many national and international conferences in the area of networking especially in wireless sensor networks and ad hoc networks.

Copyright © 2020 Inderscience Enterprises Ltd.

1 Introduction

Generally, wireless networks required to maintain a topology with minimum degree and self-organisation. Self-organisation is used to avoid link failures and node failure for huge traffic conditions (Smys and Bala, 2012; Smys et al., 2010). Wireless sensor networks (WSNs) are the wireless networks which involve spatial distributed tiny autonomous devices which cooperatively monitor the environment conditions and this information are sending to destination node or to sink node based on wireless channels. These small devices are communication devices are collectively called as sensor node and it has sensor, a wireless communication device, small microcontroller and energy source. Usually sensor devices are unique characteristics such as large scale deployment, mobility of nodes, node failures, communication failures and dynamic network topology (Zhang and Varadharajan, 2010). WSN have several applications that are commonly in health care monitoring, military environment sensing that includes air pollution monitoring, green house monitoring, landslide detection, forest fire detection (Matin and Islam, 2012). There are some recent applications in WSN that are traffic monitoring, activity monitoring, health fitness-based applications, habitat monitoring, etc. Normally WSN always works with basic nature i.e., sensing + radio + CPU, based on this mechanism every user can develop more application on the real world and using this mechanism WSN has five types of network such as, underground WSN, mobile WSN, multi-media WSN, terrestrial WSN, underwater WSN (Prasad, 2015). Figure 1 describes the nature for developing WSN application.

Figure 1 Basic nature of WSN (see online version for colours)



Security on WSN involves the several goals which are confidentiality, integrity and availability (Haas et al., 2014). Nowadays many application are developed in WSN that are still focusing on security elements that includes such as:

- authentication: this element provides the ability of party for verifying the identity of another communication party or parties
- privacy: this provides the ability for hiding the large number of data about information generation entity which is generated between transmitted data

- authenticity: this specifies the ability for verifying the information which is created or altered by the owner of the data
- non-repudiation: this involves the maintaining the data of particular parties information
- authorisation: this last element allows the access of information by the specific authorised persons of their data.

Elliptical curve cryptography (ECC) is an asymmetric cryptographic technique that provides key establishment and digital signature for secure communication. Multi-resource elliptical curve signature (MRECS) is proposed in paper (Chuchaisri and Newman, 2012) which results in higher computation cost and the verification process takes more time. Communication on WSN is a major work on WSN that must satisfy the quality of services on the network. Here the data delivery is mainly focused for critical applications like real time monitoring applications because a few errors like link breakage, data loss provide a major limitation on the network. So that real time data communication capacity is verified on the WSN. The real time capacities limits that are earliest deadline first and deadlines monotonic are specified for every application. The limits are derived between extreme traffics, load balancing topology and many-to-one topology (Virmani and Jain, 2012). Secure communication on WSN involves the key distribution mechanism that is based on combinatorial design (Çamtepe and Yener, 2007), this analysis involves several advantages that increase probability with two different nodes which has a shared key and it helps in decreasing the average key path lengths. The key path is defined as that the path between two different nodes that has a wireless links which is called as key-path. Routing is an important process in WSN that helps to reduce congestion, increasing throughput, etc. A traffic aware routing algorithm is allowed for routing packets that are allowed in congested area based on nodes with loads free. Thus it helps in constructing two independent gradient fields with distance cost and traffic loading (Gholipour et al., 2015). This process lacks in QoS performance which is not suitable to the WSN.

To solve aforementioned problems, we propose a grid-based energy efficient clustering and routing for effective sensor networks. Grid-based network provide the full coverage of a sensor nodes and it solves the routing overhead with minimum number of nodes. Our proposed framework involves clustering, routing and security for enhancing the performance of WSN. Here we initially segment the network into grids of equal size (G * G). Here the segmentation of network is based on transmission ranges of sensor nodes. Every cell in a grid has a sensor node and demand points. The clustering process is based on genetic algorithm and particle swarm optimisation. We select the cluster head (CH) based on several metrics such as residual energy, distance from base station and relay node position in the cluster. Using TDMA scheduling, the sensor nodes transmits its data to the CH. Routing is performed in our proposed framework which is based on QoS-based explicit routing algorithm. This provides the optimal route from source node to base station. For providing secure communication we involve IBDS and EIBDS that increases the performance of WSN against different adversaries. We also provide data security based on advanced encryption standard (AES) at packet transmission. This is focused and performed by base station, cell-coordinator and sensor nodes.

Our major contribution of our work is:

- we propose a new routing algorithm named 'QoS-based explicit routing algorithm', for transmitting data between source nodes and sink nodes
- we allow genetic algorithm and particle swarm optimisation for effective clustering process
- we propose a new digital signature algorithm named 'IBDS and EIBDS' with keys refreshment for enhancing security
- we finally improve quality of service on the WSN.

1.1 Paper organisation

Our proposed work is elaborately discussed in following the sections: Section 2 describes the literature survey of existing routing algorithms, secure algorithms and clustering process which are proposed in WSN. Section 3 describes the problem statement, Section 4 describes the overall proposed framework for WSN, Section 5 describes the comparative analysis with graphical results and we conclude our proposed work in Section 6.

2 Literature survey

Mansourkiaie et al. (2016) was involved in maximising the lifetime in WSN that mainly allowed for structural health monitoring. Here the author proposed optimisation framework for maximising the network lifetime that mixed with integer nonlinear programming problem and it was solved by branch and bound algorithm which is augmented with reducing the search space. For reducing the computational complexity, a heuristic routing algorithm is proposed selects power levels from the optimal power allocation of sensor node. The proposed mathematical model formulates the maximum life time problem and reduces the computational complexity and Rerouting is required when the critical nodes depletes their energy level.

Bhatti and Kaur (2017) proposed a virtual grid-based routing algorithm (VGDRA) to improve the energy consumption. The network is divided into grids of k-cells and a cell header is elected for each and every cell. The algorithm proves QoS in terms of energy by minimising route construction. The problem of this paper was each cell is equally sensing data from sensor node but the data aggregation was a major problem. Here this research needs higher performance in QoS metrics and collected data are not aggregated during data routing.

Sun et al. (2016) proposed an improved routing algorithm based on ant colony optimisation (ACO). This heuristic function is considered the parameters of the node communication transmission distance, residual energy and transmission direction. Thus the ACO algorithm solves the problem of energy consumption and improves the network life time. The limitation of this paper is considering the transmission direction where it can be accurately defined on the network, so this is not sufficient for routing.

Rani and Ahmed (2017) presented a new big data gathering algorithm for collecting the big data in sensors. When collecting data from sensor nodes, energy is a major and more important factor. To attain this cluster communication was established between

sensor nodes based on the value of RSSI. Results of network life time and data transmission time for data gathering algorithm are not effective because if any of the CH is failed due to low energy, the routing path is break.

Chatterjee et al. (2017) proposed a new load balancing coverage with graded node deployment. This load balancing coverage was deployed in WSN. Data streaming was proposed to gather the streams of data in static WSNs. Authors proposed a novel, load balanced data gathering algorithm to transmit a packets to the sink node through BS by minimum-hop paths. This will help to limit the problem of network traffic and overcomes the problem of energy consumption. An average case probabilistic analysis is done with help of perfect matching of random bipartite graphs that helps to establish a theoretical lower bound with several numbers of nodes that are deployed on the network. This method results in cost effective manner.

Yenke et al. (2016), multithreading model for an efficient data delivery in WSNs that help in effective manner. To limit the energy resources in sensor nodes, operating systems are developed 'Contiki' is used. The simulation is performed by using COOJA simulator which is integrated with Contiki OS. The results of this hybrid system show that ratio of message reception and energy consumption is better than existing approaches and multihop transmitting approach is allowed for simulating multitasking Contiki environment. The major limitation of this process was results in threads crashing.

Li et al. (2012) proposed an authentication mechanism which is essential security requirement in WSNs. In this paper, authors proposed a practical identity-based signature scheme for providing authentication in WSNs. There are two phases are involved on this scheme: offline phase and online phase. High loaded and heavy computations have been done in offline part and light loaded computation is done in online part. Here the limitation is that it results in higher computational cost.

Lu et al. (2014) proposed a cluster-based WSN for enhancing the secure and efficient data transmission. Clustering-based WSNs enhances their system performance in terms of energy efficiency and security. Here, two secure and efficient data transmission (SET) protocols were proposed for secure data transmission such as SET-identity-based signature (SET-IBS) and SET-identity-based online/offline digital signature (SET-IBOOS). The main idea is to authenticate encrypted data from sensor node based on applying security with help of key management. Here the SET-IBS involves ID-based cryptography and user public keys are based on ID information whereas the Set-IBOOS is proposed for further reduction of computation overhead in terms of security. Thus this process solves the orphan nodes problem on the network.

Shruthi and Hemavathi (2016) are involved for key management based on digital signature with effective data transfer. Here the key management was focused in WSN. Secure data transferring in dynamic sensor networks play vital role in the field of military sensing and tracking applications. Digital signature algorithm (DSA) is used for key distribution mechanism and which is used for security. This algorithm achieves better results with reduction of computation overhead.

Liu et al. (2012) proposed PKC-based broadcast authentication with the help of signature amortisation. This also exploits elliptic curve digital signature algorithm which achieves less overhead and retains high security while broadcasting messages. The proposed novel PKC-based broadcast scheme meets the following criterions: low overhead, high and strong security and authenticity, immediate authentication, resilience

and no time synchronisation. But this algorithm lacks in term of a memory overhead. Since the code size and RAM size of the sender side and receiver side is too high.

Diop et al. (2012) presented a secure key management scheme which involves authentication, secrecy, resilience, revocation and fresh node addition and efficiency requirement must satisfy the properties such as network connectivity, maximum supported network size, low computation overhead, low communication overhead and maximum supported network size. When a network satisfies all the above mentioned criterions, the system is highly scalable. In this paper secure key management scheme was proposed in WSN. In this scheme keys distributed over the cluster and update the pre-deployed keys to mitigate the node. Le et al. (2009) authors proposed an energy efficient access control mechanism with help of ECC. But the process takes more execution time for processing. High energy consumption is severely degrades the performance and increase the system cost and efficiency (Zhang et al., 2017).

3 Problem statements

WSN allows secure data communication and reliable data transfer services which are more important for several applications. Due to power constraints, data transmission was mainly focused for WSN. In order to improve data transmission, effective routing was mainly needed for WSN. To provide these facilities in WSN, ACO was proposed for selecting optimum result (Sun et al., 2016). Here the parameters used for selecting optimal route are not effective because the values must change all time. So that result of this paper was not effective. An efficient and secure key management scheme which was based on symmetric key management scheme which allows two type's keys are used for key management scheme called 'network key' and 'pairwise key' (Diop et al., 2012). Network key is distributed globally for all the nodes in network where it is also used for cluster formation and pair wise keys are established between two communicating parties. ECC is a digital signature-based asymmetric algorithm (Chuchaisri and Newman, 2012) that supports multi resolution signatures. Digital signature is one the asymmetric key management scheme which offers security services. This signature scheme results that it requires less space and also have a long key life time. Here the signature verification process takes more time to complete it.

4 Proposed systems

Our proposed framework is mainly focused for enhancing performance of WSN network with data delivery. Our framework involves mainly three phases for enhancing the performance of WSN they are:

1 clustering

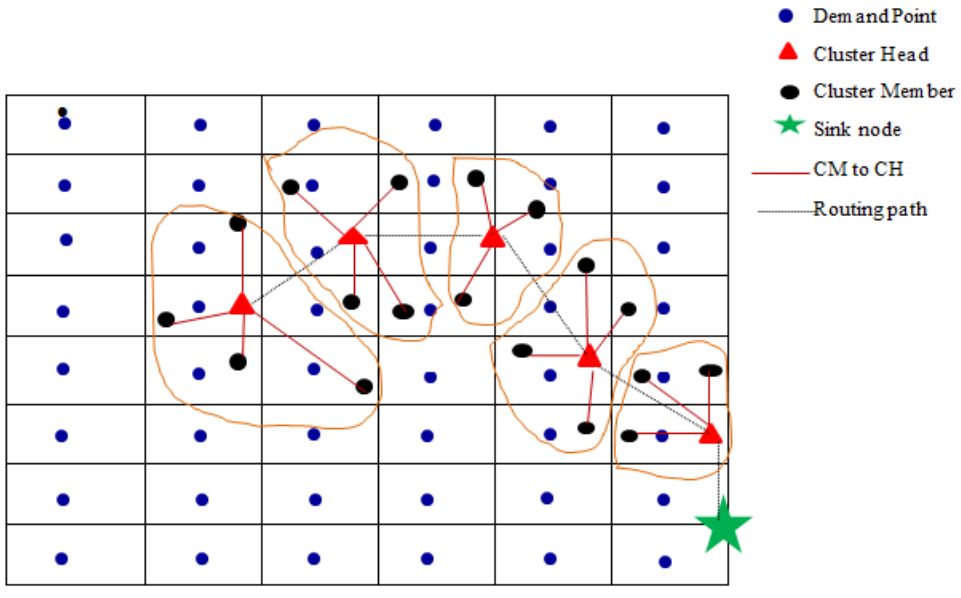
2 routing

3 security.

Initially we describe the system of our proposed framework. Here we involve a smart grid which is size of (G * G) which are separated equally. This whole network is

segmented based on transmission range of sensor nodes. Here each cell from grid has demand points. Figure 2 specifies the grid model of our proposed system.

Figure 2 Proposed grid model for WSN framework (see online version for colours)



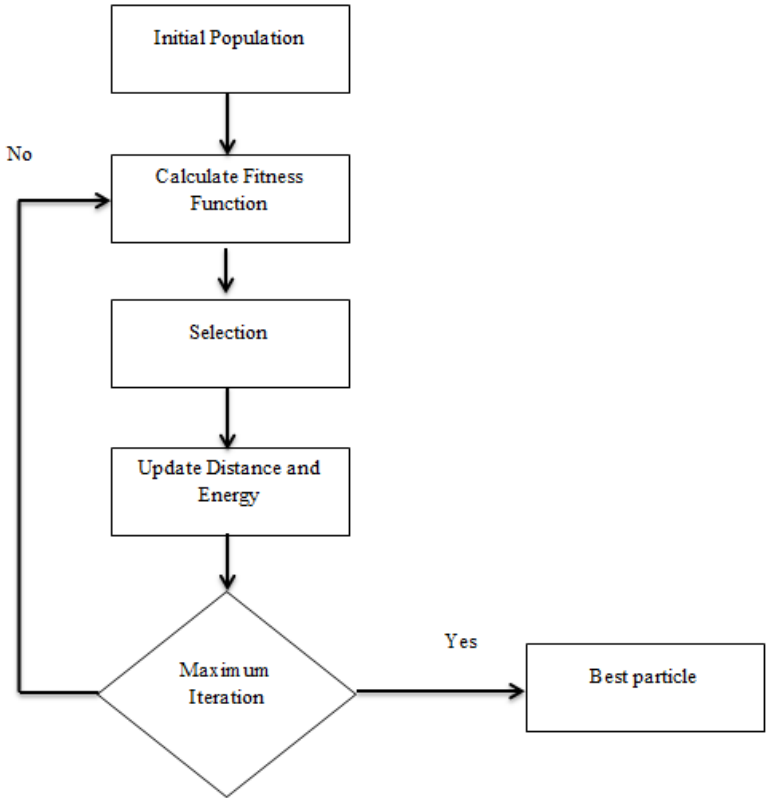
After the system initialisation, we involve clustering process using GA and PSO algorithm (which is a combination of both genetic algorithm and particle swarm optimisation), a routing algorithm for effective data delivery which is QoS-based explicit routing algorithm and finally we involve a secure communication with the help of IBDS and EIBDS which is a digital signature algorithm that provides private signature to access the information. We also involve the AES cryptographic algorithm that is useful to transmit the data to the sink node. This procedure is done by sink node, cell coordinator and sensor nodes. In next further section, we discuss about clustering, security and routing process.

4.1 Clustering

Clustering is more important work in WSN that involves increasing the network lifetime. Our proposed work involves the clustering mechanism based on GA and PSO algorithm. Based on this mechanism we group the nodes and mention as cluster. Initially we involve the random particles and then we calculate fitness function for each particle. The fitness function is evaluated using total number of nodes. The fitness function is calculated by:

$$FF = \frac{Concate(Node\,1,\ Node\,2,\ Node\,3, \ldots)}{Total\ nodes} \tag{1}$$

Figure 3 Flowchart for GA and PSO



Based on this evaluated fitness function we involve particle swarm optimisation for getting effective result, based on updating the energy and distance of every node. Consider X_i represents the particular solution, every node may change the position and its energy may vary based on its distances. The PSO operator effectively updates the distances that take that as the best position based on the fitness value that are reached by all nodes. During iteration (Kaveh and Rad, 2010), the updated information of all nodes is:

$$N_i^{t+1} = \omega N_i^t + C_1 r_1^t \left(P_i^t - X_i^t\right) + C_2 r_2^t \left(P_g^t - X_i^t\right) \tag{2}$$

$$X_i^{t+1} = X_i^t + N_i^{t+1} \tag{3}$$

Here N_i^t is the Node vector at iteration t, r_1 and r_2 represents the random numbers in between the range [0, 1] and P_i^t denotes the best node at other nodes I, P_g^t is the global best node in the iteration t, C_1 and C_2 represents the trust parameters that have higher confidence of every node by itself and finally ω is the inertia weight where the larger inertia weight allow for wider velocity which updates providing the global exploration of the search space whereas the smaller inertia value specifies the updation of nodes to nearby regions. Finally at global iteration, the clustering is formed. Figure 3 describes the

flowchart for GA and PSO clustering mechanism. We describe the algorithm for GA and PSO clustering mechanism.

Algorithm 1 GA and PSO

Input	$N_i = \{N_1, N_2, N_3 \ldots\}$, ND and NE.
Output	Cluster formation
Start	
Step 1	Calculate FF using equation (1)
Step 2	select best N_i
Step 3	update ND and NE for N_i using equation (3) and (2)
Step 4	if (Max iteration)
	Best individual
	Else
	Goto step 2
	End if
End	

Here N_1, N_2, N_3 … are the nodes in WSN and ND is the distance of nodes and NE is the energy of nodes. FF is the fitness function for all nodes. By updating the information of all nodes, we finally select the best individual for clustering.

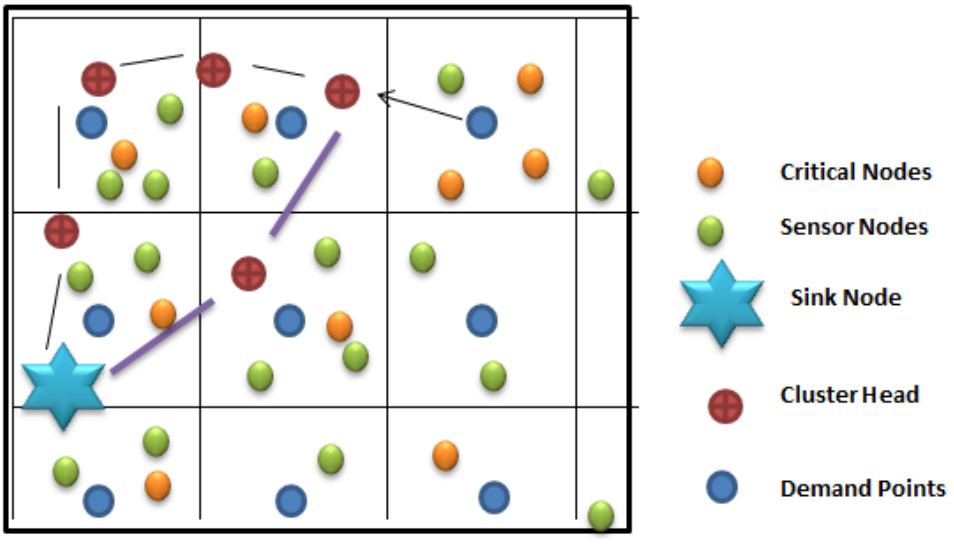
4.1.1 CH selection and working

A node is selected as the CH that satisfy several metrics such as residual energy, distance of BS and relay nodes positions on the cluster. Here the cluster members are joined in the cluster within its coverage range. Every member forwards its sensed data to CH within the allocated time slot that is done by TDMA scheduling. Then CH aggregates the collected data and it is forwarded to sink node and to base station. We involve reconfiguration process for CH to solve the problem of CH failure during routing process. The reconfiguration is processed when a CH's energy is reduced below the threshold, then it needs to change by another member node that has energy which is above the threshold. Here the original CH is set as normal member node in the cluster.

4.2 Routing

Routing is defined as the selection of optimal path on the traffic or between multiple optional paths on the network which leads to increasing lifetime of network. Our proposed work involves QoS-based explicit routing algorithm for acquiring higher quality of service. According to our WSN framework we involve a demand point on each grid cell and this specifies the urgency of packet transmission and we calculate the criticality of nodes on the network. Here the criticality of nodes is specified based on residual energy of nodes and path length. In any grid cell, two or more critical nodes are initialised and then the demand point forwards a message to the nearer CH for packet transmission.

Figure 4 QoS-based explicit routing algorithm (see online version for colours)



Then urgency nodes packets are collected by corresponding CH and it forwards its aggregated packets nearer CHs and to sink node. Figure 4 describes the routing procedure of all nodes in the network and we also involve the algorithm for QoS-based explicit routing algorithm.

Algorithm 2 QoS-based explicit routing algorithm

Input	$N_i = \{N_1, N_2, N_3 \ldots\}$, $CH_i = \{CH_1, CH_2, CH_3 \ldots\}$, $CN_i = \{CN_1, CN_2, CN_3 \ldots\}$, SN, PL and RE.	
Output	Optimal routing	
	Start	
		$CN_i \rightarrow$ PL and RE
	Step 1	DP $\rightarrow CN_i$
	Step 2	if ($CN_i > 2$)
		DP $\rightarrow$ CHi
		If (CH_i found)
		CN (P) $\rightarrow CH_i$
		End if
		End if
	Step 3	$CH_i \rightarrow$AG (P)
	Step 4	$CH_i \rightarrow$ nearer CH_i
	Step 5	$CH_i \rightarrow$ SN
	End	

In above algorithm DP specifies the demand point, PL is the path length, RE is the residual energy, CN_1, CN_2, CN_3 … is the critical nodes, N_1, N_2, N_3 … is the normal sensor nodes, CH_1, CH_2, CH_3 … is the CHs, P is the packet and SN is the sink node. We

calculate the critical nodes based on path length and residual energy. DP on each cell searches the CN_i, when there is two or more CN_i on the cell; DP forwards a message to CH_i and it collects the packets from CN_i. Then it aggregates the packets and sends to near CH and followed by sink node.

4.3 Secure communication

Secure communication is a need for WSN that provides a key role for solving various attacks and also providing secure communication. In order to provide secure data transmission on cluster wireless sensor network (CWSN), a key management technique is needed without introducing the computational overhead and increases the resilience against several adversaries. Here the problem of WSN was that intruders can hack the data when the data is transferred from sensor node to CH. In order to tackle these problems, our proposed framework involves a digital signature-based security measures such as IBDS and EIBDS. This security mechanism in our proposed framework works with cluster-based secure communication with digital signature scheme. This IDBS has setup, key extraction, signatures signing and signature verification. In enhanced IDBS we introduce the key refreshment procedure. Thus our proposed IDBS and EIDBS security has:

- setup: the base station creates the master key 'M' and public parameters 'PARA' for the private key generator (PKG) and gives them to every sensor nodes
- key extraction: in a given ID, a sensor node can create the private key (Pkey) that are associated with ID using M
- signature signing: with a message MSG, time stamp T and a signing key α, the sensor node generates the signature S
- signature verification: based on ID, MSG and S, the sink node while receiving results 'ACCEPT' message if signature is valid otherwise it outputs 'reject' message
- key refreshment: at every time stamp T, the base station gets all the keys from the network and refreshes the keys and transmits it the sensor nodes.

Algorithm 3 IBDS and EIBDS

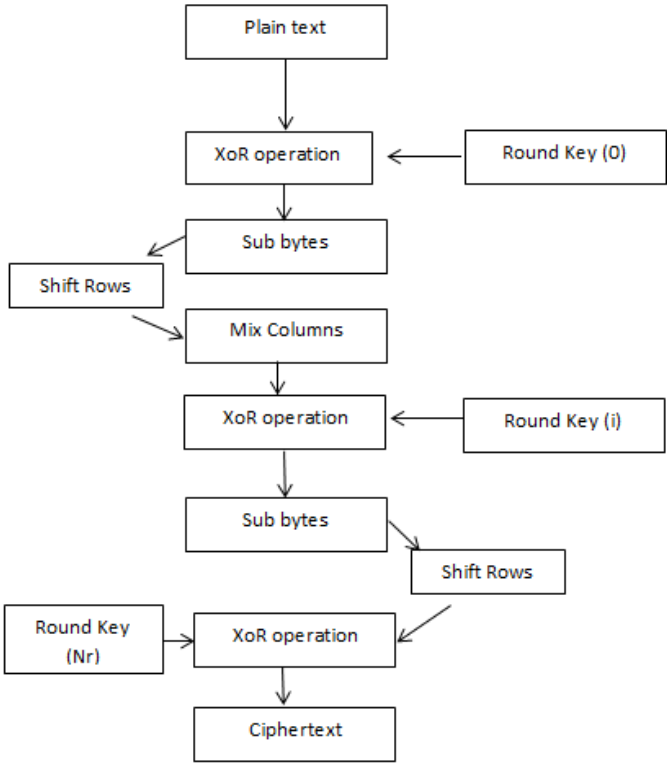
Input $N_i = \{N_1, N_2, N_3 \ldots\}$, message msg., signature (θ), master key (M), private key generator (PKG) and timestamp (T), private key (P_{key}), Signing key (α) and base station (BS).

Start

1 Ni →WSN // (IBDS)
2 Ni → M and PKG (by BS)
3 Ni (ID and M) → P_{key}
4 For (N_i = 1, 2, …)
{
Msg, α, T → θ
5 If (valid θ)
N_i → Accepts msg.
Else

$N_i \rightarrow$ Rejects msg.
} End For
6 For T, //Key refreshment (EIBDS)
{
BS collects $M \rightarrow N_i$
Refresh (M)
BS sends $M \rightarrow N_i$
} End For

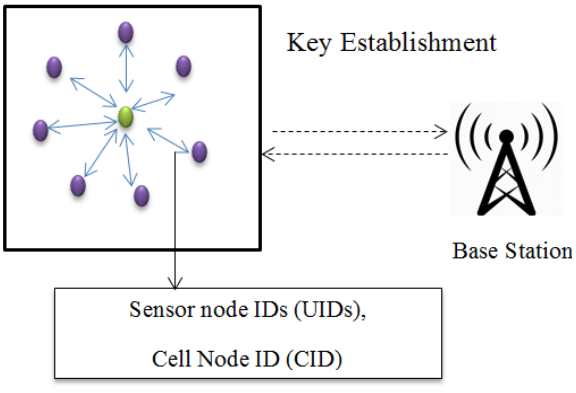
Figure 5 AES cryptographic mechanism



Algorithm 3 describes the overall operation of IBDS and EIBDS. The base station is the only node who can establish the keys for several nodes based on setup phase of signatures. Every CH is allowed for signature signing and verification procedures process for accessing the information. Here we introduce a key refreshment process is introduced at base station that is done within a specific time, for providing secure communication. We also involve a cryptographic technique called AES (Selent, 2010) for effective packet transmission between sensor node and sink node. This AES cryptographic mechanism is described in Figure 5. Figure 6 describes secure communication for the proposed WSN framework. This AES encryption mechanism involves several operations for encryption such as:

- Sub bytes: this section is used for byte-by-byte substitutions on the forward process. This has 16 * 16 lookup table for identifying the replacement byte for a given byte on the input state array. The entries on this table are created based on notions of multiplicative inverses and bit scrambling in order to eliminate the bit-level correlations.
- ShiftRows: this is done on forward process while shifting the rows of the state array and the main objective of this transformation is scrambling the byte codes inside each bit blocks.
- MixColumn: this section is mainly used for mixing the bytes for each column that separately. Here the ShiftRows along with MixColumn step leads to each bit of cipher text for depending on every bit of original text, after the completion of ten rounds.
- AddRoundKey: this section allows the addition of round key for the output of MixColumn.

Figure 6 Proposed IBDS and EIBDS (see online version for colours)



These four operations are inversely done for the decryption process for obtaining the original text from the plain text. Thus our proposed framework is stronger against several attacks like reply attacks and man in the middle attacks. In the following section we discuss the comparative results of our proposed system.

5 Performance evaluations

Our proposed framework is evaluated with various performance metrics and it is compared with some existing protocols such as LEACH and Sec-LEACH. We focus on enhancing the performance of proposed system based on routing, clustering and secure communication provided on the environment. This section involves:

- simulation environment
- performance metrics
- comparative analysis.

5.1 Simulation environment

Our proposed framework is implemented by the open source software network simulator-3 (NS-3). This is a discrete event network simulator that mainly focuses on educational purpose and research purpose. NS3 is licensed based on GNU GPLv2 and it allows an effective environment for both research and development. NS3 uses the C++ or Python programs for simulations and it also allow developing the advanced network research. This open source software is installed in Ubuntu 12.04 LTS operating system. Based on our proposed framework for WSN, we design network with several simulation parameters. Here Table 1 specifies the simulation parameters that are used for proposed system implementation. We use 25 sensor nodes for the system and the initial energy of sensor node is initialised at 800 J. Further, the energy varies based on their simulation time and based on their movements. Here the demand use the constant velocity mobility model whereas the sensor nodes uses the random way point model.

Table 1 Simulation parameters

Parameters	*Values/ranges*
Network simulator	NS3
Simulation time	15s
Simulation area	300 m × 250 m
Number of nodes	25
MAC protocol	IEEE 802.15.4 (sensor nodes)
	IEEE 802.11P (demand points)
Packet size	1024 bytes
Initial energy of node	800 J
Mobility model	Random way point model (sensor nodes)
	Constant velocity model (demand points)

5.2 Performance metrics

Performance metrics is considered for analysing the performance of our proposed framework. Our network is analysed for improvement of our proposed work. This section considers several performance metrics that are taken in account for further improving the proposed work. We evaluate our proposed WSN framework based on some performance metrics such as,

- network life time
- data transmission time
- reliability
- throughput
- delay
- packet delivery ratio
- routing overhead

- energy consumption.

These metrics are compared with existing system such as LEACH and Sec-LEACH in the upcoming section.

5.3 Comparative analysis

This section compares our proposed framework with existing work based on the performance metrics which are listed in above section. Parameters are evaluated and examined against existing implemented metrics. For understanding the better results in our proposed system these parameters are plotted that specifies the overall effectiveness of proposed framework. First we briefly see the existing systems such as,

- Improved LEACH routing communication protocol (Zhao et al., 2012): this communication protocol includes a traditional equation that is mainly used for selecting CHs. This considers the dynamic changes of energy of every node. Here, a CH is elected for each cluster on the communication which helps to reduce the energy consumption that spent on re-clustering and increasing the network life time.
- Modified Sec-LEACH (Essam and Shaaban, 2011): this technique works with a secure clustering mechanism that involves security-based clustering mechanism for sensor networks. This clustering is an extension of LEACH protocol with a combination of symmetric key methods (blowfish cryptographic mechanism). This scheme involves the node authentication between CH and between cluster members.
- Secure routing protocol for cluster-based WSN using group key management (Zhang et al., 2008): this paper focuses on adding security for cluster-based routing protocols for WSN that consists of sensor nodes with several limited resources and it involves the security solution for LEACH protocol. This process involves the light weight scheme named random pair wise key (RPK) scheme for security. This technique is safer for node-to-node authentication and saves energy.

5.4 Graphical results

In this section, we discuss the results of our proposed framework that are analysed with above mentioned performance metrics. We discuss our results in one by one.

5.4.1 Network life time

The network lifetime is defined as the amount of time, a sensor node is operated. In other words, network lifetime is the time at which the first node runs out of energy for passing a packet based on node failure which has certain network functionalities. The network lifetime is calculated by:

$$T_n^n = \min_{v \in V} T_v$$

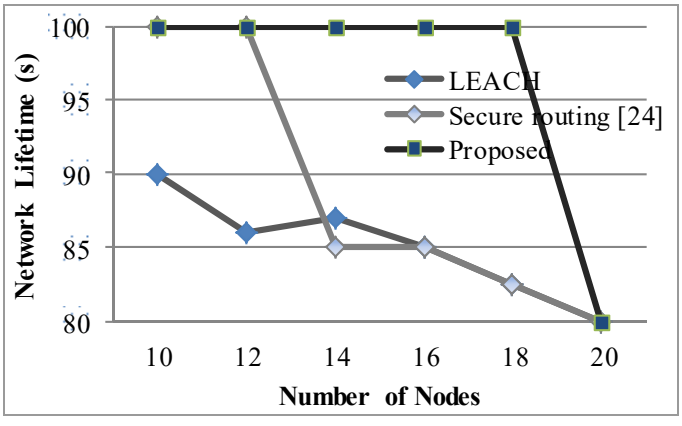
where,

T_v lifetime of node v

n is the number of nodes on the network.

Here in Figure 7, the network lifetime of both proposed framework and existing protocol such as LEACH and secure routing (Zhang et al., 2008) with proposed framework. The graphical results are plotted with number of nodes with network lifetime. Here in securing routing process and LEACH when the number of nodes gets increased the life time of network decreases whereas in our proposed framework, the counting of nodes below 18 we acquire same level of network lifetime and then it decreases.

Figure 7 Graphical representation of network lifetime with proposed, LEACH and secure routing (see online version for colours)



Source: Zhang et al. (2008)

Table 2 Comparison of average network lifetime

Average network lifetime (seconds)		
LEACH	*Secure*	*Proposed*
85.083	88.75	96.66

5.4.2 Data transmission time

Usually, in networks data transmission time is defined as the amount of time from the beginning of network to the end of message transmission. Data transmission time is measured in seconds. The data transmission time is calculated by,

$$Transmission\ time = \frac{L}{B}$$

where,

L is the frame length in bits

B is the data rate in bits per second.

Figure 8 presents the graphical representation of data transmission. This graph describes the data transmission time of proposed framework that compared with LEACH and Sec-LEACH. Our proposed framework results excellent for time taken for data transmission whereas the existing protocols take more time for data transmission.

Figure 8 Graphical representation of data transmission time with proposed, LEACH and SEC-LEACH (see online version for colours)

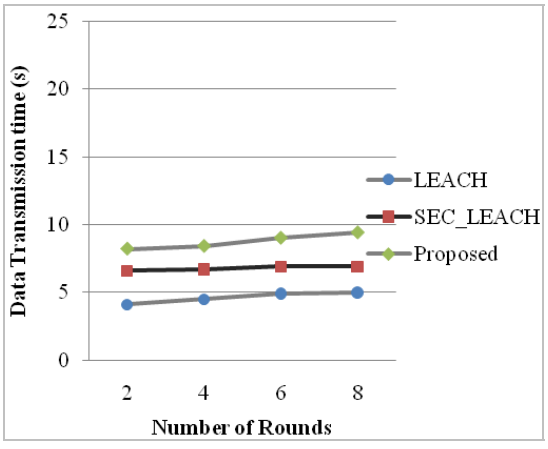


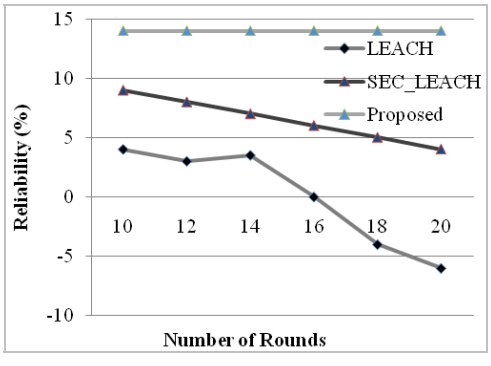
Table 3 Comparison of average data transmission time

Average data transmission time (seconds)		
LEACH	*SEC_LEACH*	*Proposed*
5.42 s	6.37 s	10.22 s

5.4.3 Reliability

The reliability is defined as the concern which is the capability of a network which helps to carry a desired operation like communication, data transmission, routing, etc. In other words, the reliability of the network is that all the network components are communicating with other nodes without any faults.

Figure 9 Graphical representation of reliability with proposed, LEACH and SEC-LEACH (see online version for colours)



Here, we describe the comparison of existing protocol such as LEACH and SEC-LEACH, with proposed framework. Figure 9 describes the graphical representation

of reliability. This graph specifies overall operation of proposed framework when compared with effective existing protocol for number of rounds.

Table 4 Comparison of average reliability

Average reliability (%)		
LEACH	*SEC_LEACH*	*Proposed*
0.5	6.5	14

5.4.4 Throughput

Throughput is important factor and plays a major role for analysing the performance of a network. Hence it is defined as the number of packets that are successfully transmitted with respect to amount of time taken by every node and in other words, as that total number of data that are moved successfully from one place to another place within a short time. It is measured in terms of bits per second (bps). This can be calculated as:

$$Throughput = P_{SD} - P_{RD}$$

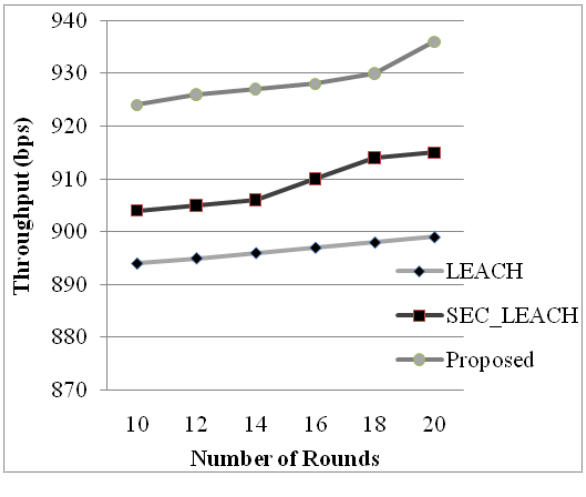
where,

P_{SD} is the number of packets send

P_{RD} is the number of packets received.

Figure 10 describes the graphical representation of throughput. This compares the existing schemes such as LEACH and SEC-LEACH with proposed framework and provides the excellent result; here the transmission of packets at every round represents the higher result of proposed framework.

Figure 10 Graphical representation of throughput with proposed, LEACH and SEC-LEACH (see online version for colours)



5.4.5 Delay

Delay is a major factor that is defined for time taken for packet that it is to be transmitted over the network from its source node to destination. This is common in IP-based monitoring on network.

$$E2ED = TD + PD + P_{QT}$$

where

P_{QT} is described as queuing time of packet

TD is the transmitting delay

PD is the propagation delay.

Figure 11 describes the graphical representation of delay which represents the higher result of proposed framework when compared with existing protocol LEACH. Our proposed framework involves reduced delay according to load factors on the network.

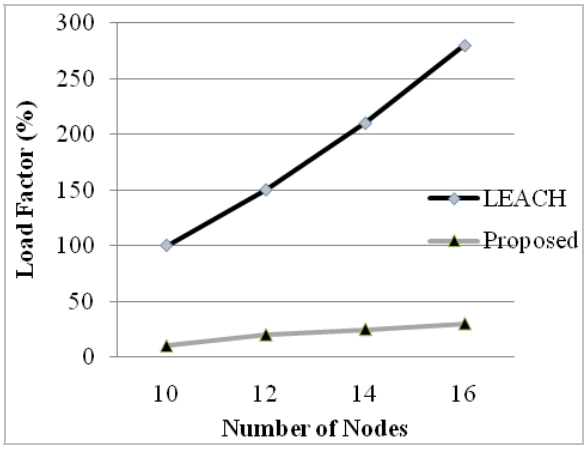
Table 5 Comparison of average throughput (bps)

Average throughput (bps)		
LEACH	*SEC_LEACH*	*Proposed*
896.5	909	928.5

Table 6 Comparison of average delay

Average delay (%)		
LEACH	*SEC_LEACH*	*Proposed*
240	240	25.8333

Figure 11 Graphical representation of delay with proposed and LEACH protocol (see online version for colours)



5.4.6 Packet delivery ratio (PDR)

The packet delivery ratio is defined as that ratio of packets generated by source node that are transmitted to destinations. In other words, PDR specifies the total number of packets that are received to receiver. PDR is calculated by:

$$PDR = \frac{\sum PSD}{\sum PRD}$$

where,

PSD is the packet send by source node

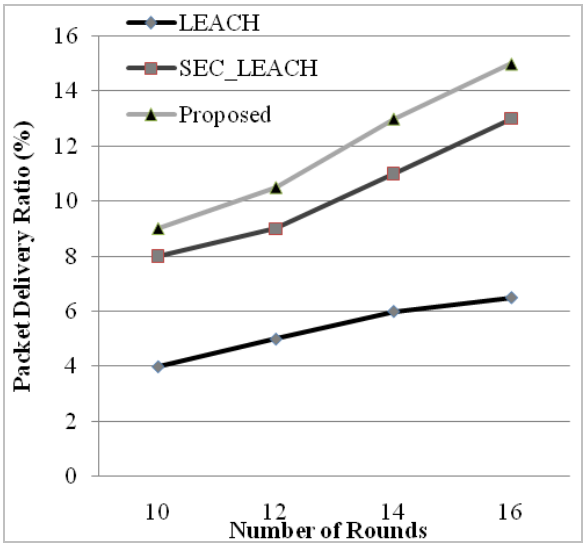
PRD is the packet received by destination node.

Our proposed framework results in higher packet delivery ratio and it is compared with existing protocols like LEACH, Sec-LEACH. When the packet delivery ratio gets higher the overhead on routing reduces on the network. If the number of rounds increases the PDR gets increased. Figure 12 describes the graphical representation of packet delivery ratio.

Table 7 Comparison of average packet delivery ratio (%)

Average packet delivery ratio (%)		
LEACH	*SEC_LEACH*	*Proposed*
6.0833	11.83	13.75

Figure 12 Graphical representation of packet delivery ratio with proposed, LEACH and SEC-LEACH (see online version for colours)



5.4.7 Routing overhead

A 'hello packet' is allowed for checking the number of active neighbour nodes and here both routing and data packets must share same network bandwidth and this is considered as the routing overhead. The routing overhead is calculated by:

$$Routing\ overhead = \frac{N(P)}{PT}$$

where

N is the number of packet (P) send

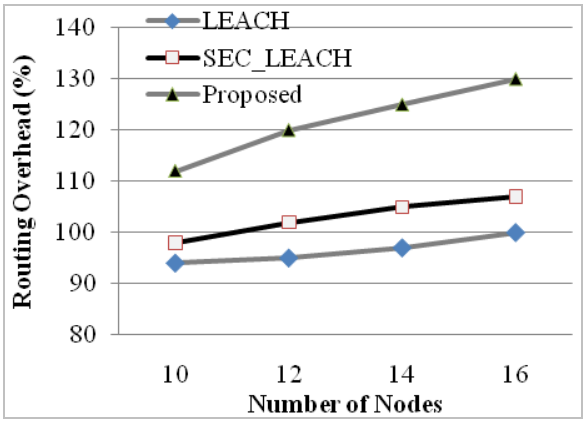
PT is the optimal path.

Figure 13 describes the graphical representation of routing overhead based on comparison with existing protocols such as LEACH and Sec-LEACH. The routing overhead in our proposed work is higher because of the transmission between CHs and sink node, when number of nodes increases the PDR gets increased then automatically the overhead reduces.

Table 8 Comparison of average routing overhead (%)

Average routing overhead (%)		
LEACH	*SEC_LEACH*	*Proposed*
101.5	105.6	126

Figure 13 Graphical representation of routing overhead with proposed, LEACH and SEC-LEACH (see online version for colours)



5.4.8 Energy consumption

Energy consumption is defined as energy consumed by the sensor node in WSN. It is calculate based on its power consumption states such as sleep, idle and active. Total power consumption is defined by:

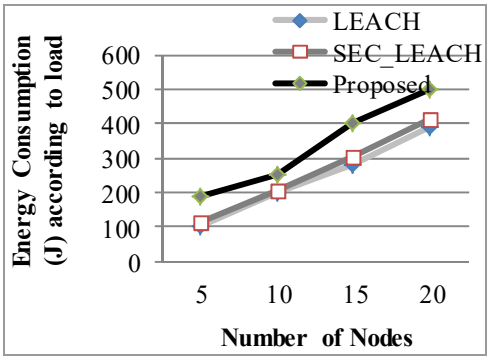
$$TE = E_{SP} + E_{ID} + E_{AC}$$

E_{SP} is the sleep state of sensor

E_{ID} is the idle state of sensor

E_{AC} is the active state of sensor.

Figure 14 Graphical representation of energy consumption according to load with proposed, LEACH and SEC-LEACH (see online version for colours)



Our proposed work is compared with existing protocols like LEACH and Sec-LEACH protocols. This protocol has the lower energy consumption when compared with proposed framework but according to load factor these protocol lead to lead dead line condition whereas the our work involves the active sensor nodes when the load increases. Figure 14 describes the graphical representation of energy consumption.

Table 9 Comparison of average energy consumption (J)

Average energy consumption (j)		
LEACH	*SEC_LEACH*	*Proposed*
242.5	258.5	335

6 Conclusions

WSN is a wireless autonomous network that provides effective running environment for developers to create several applications that must provide effective quality of service to end users. To solve these problems, we propose a new WSN framework with grid modelling. This framework includes several processes like:

1 Clustering is done based on GA and PSO which includes distance and energy consumption of nodes and here CH is selected based on residual energy, distance from BS and relay nodes positions on the corresponding cluster. We also involve CH reconfiguration procedure for solving the packet loss during data transmission.

2 Routing is based on QOS-based explicit routing that allows data transmission from sensor nodes to sink node with the help of CHs and finally.

3 Security based on IDBS and EIDBS technique which involve the key refreshment process.

Finally, we attained 25.833% delay and 13.75% packet delivery ratio than the previous approaches. Thus our proposed framework works effectively that are verified by the graphical representation when compared with existing system such as LEACH and Sec-LEACH.

7 Future works

In future work, we aim to implement our proposed work in real time application environment like military environment, smart city applications. We also aim to introduce newer mechanism for solving and identifying malicious node in our network.

References

Bhatti, R. and Kaur, G. (2017) 'Virtual grid based energy efficient mobile sink routing algorithm for WSN', *11th International Conference on Intelligent Systems and Control (ISCO)*, pp.30–33.

Çamtepe, S.A. and Yener, B. (2007) 'Combinatorial design of key distribution mechanisms for wireless sensor networks', *IEEE/ACM Transactions on Networking*, Vol. 15, No. 2, pp.346–358.

Chatterjee, P., Ghosh, S.C. and Das, N. (2017) 'Load balanced coverage with graded node deployment in wireless sensor networks', *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 3, No. 2, pp.1–18.

Chuchaisri, P. and Newman, R.E. (2012) 'Multi-resolution elliptic curve digital signature', *IEEE Conference on Local Computer Networks*, pp.93–101.

Diop, A., Qi, Y., Wang, Q. and Hussain, S. (2012) 'An efficient and secure key management scheme for hierarchical wireless sensor networks', *International Journal of Computer and Communication Engineering*, Vol. 1, No. 4, pp.1–6.

Essam, M. and Shaaban, E. (2011) 'Enhancing S-LEACH Security for Wireless Sensor Networks', *International Journal of Applied Computing*, Vol. 4, No. 2, pp.101–107.

Gholipour, M., Haghighat, A.T. and Meybodi, M.R. (2015) 'Hop-by-hop traffic-aware routing to congestion control in wireless sensor networks', *EURASIP Journal on Wireless Communications and Networking*, Vol. 15, pp.1–13.

Haas, Z.J., Yang, L., Liu, M-L., Li, Q. and Li, F. (2014) *Current Challenges and Approaches in Securing Communications for Sensors and Actuators*, pp.2–38, Springer-Verlag Berlin Heidelberg.

Shruthi, G. and Hemavathi, J. (2016) 'Digital signature based key management protocol for secure data transfer in dynamic sensor networks', *IEEE International Conference On Recent Trends in Electronics Information Communication Technology*, pp.20–21.

Kaveh, A. and Rad, S.M. (2010) 'Hybrid genetic algorithm and particle swarm optimization for the force method-based simultaneous analysis and design', *Iranian Journal of Science & Technology, Transaction B: Engineering*, Vol. 34, No. B1, pp.15–34.

Le, X.H., Lee, S., Butun, I., Khalid, M., Sankar, R., Kim, M., Han, M., Lee, Y-K. and Lee, H. (2009) 'An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography', *Journal of Communications and Networks*, Vol. 11, No. 6, pp.599–606.

Li, F., Zhong, D. and Takagi, T. (2012) 'Practical identity-based signature for wireless sensor networks', *IEEE Wireless Communications Letters*, Vol. 1, No. 6, pp.637–640.

Liu, Y., Li, J. and Guizani, M. (2012) 'PKC based broadcast authentication using signature amortization for WSNs', *IEEE Transactions on Wireless Communications*, Vol. 11, No. 6, pp.2106–2115.

Lu, H., Li, J. and Guizani, M. (2014) 'Secure and efficient data transmission for cluster-based wireless sensor networks', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 3, pp.750–761.

Mansourkiaie, F., Ismail, L.S., Elfouly, T.M. and Ahmed, M.H. (2016) 'Maximizing lifetime in wireless sensor network for structural health monitoring with and without energy harvesting', *IEEE Access, Special Section on Energy Harvesting and Scavenging: Technologies, Algorithms, and Communication Protocols*, Vol. 5, pp.2383–2395.

Matin, M.A. and Islam, M.M. (2012) 'Overview of wireless sensor network', *Intech OpenScience, Wireless Sensor Networks – Technology and Protocols*, pp.1–23, ISBN: 978-953-51-0735, DOI: 10.5772/49376.

Prasad, P. (2015) 'Recent trend in wireless sensor network and its applications: a survey', *Sensor, Emerald*, Vol. 35, No. 2, pp.229–236, DOI: 10.1108.

Rani, S. and Ahmed, S.H. (2017) 'Can sensors collect big data? An energy efficient big data gathering algorithm for WSN', in Talwar, R. and Malhotra, J. (Eds.): *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 4, pp.1–8.

Selent, D. (2010) 'Advanced encryption standard', *Rivier Academic Journal*, Vol. 6, No. 2, pp.1–14.

Smys, S. and Bala, G.J. (2012) 'Stab-WIN: self organized, topology control ability backbone node in wireless networks', *Wireless Personal Communications*, 1 April, Vol. 63, No. 3, pp.529–548.

Smys, S., Bala, G.J. and Raj, J.S. (2010) 'Self-organizing hierarchical structure for wireless networks', in *2010 International Conference on Advances in Computer Engineering (ACE)*, IEEE, 20 June, pp.268–270.

Sun, Y., Dong, W. and Chen, Y. (2016) 'An improved routing algorithm based on ant colony optimization in wireless sensor networks', *IEEE Communications Letters*, Vol. 21, No. 6, pp.1–4.

Virmani, D. and Jain, S. (2012) 'Real time communication capacity for data delivery in wireless sensor networks', *Research Gate Articles*, Vol. 4, No. 2, pp.1–11.

Yenke, B.O., Sambo, D.W., Ari, A.A.A. and Gueroui, A. (2016) 'MMEDD: multithreading model for an efficient data delivery in wireless sensor networks', *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 8, No. 3, pp.179–186.

Zhang, J. and Varadharajan, V. (2010) 'Wireless sensor network key management survey and taxonomy', *Journal of Network and Computer Applications*, Vol. 33, No. 2, pp.63–75, Elsevier.

Zhang, K., Wang, C. and Wang, C. (2008) 'A secure routing protocol for cluster-based wireless sensor networks using group key management', *IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp.1–5.

Zhang, Y., Wang, H. and Xie, Y. (2017) 'An intelligent hybrid model for power flow optimization in the cloud-IOT electrical distribution network', *Cluster Computing*, pp.1–10.

Zhao, F., Xu, Y. and Li, R. (2012) 'Improved LEACH routing communication protocol for a wireless sensor network', *International Journal of Distributed Sensor Networks, Research Article*, pp.1–6.