An energy efficient authentication scheme based on hierarchical IBDS and EIBDS in grid-based wireless sensor networks

Article *in* International Journal of Information and Computer Security · January 2020

DOI: 10.1504/IJICS.2020.108127

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

An energy efficient authentication scheme based on hierarchical IBDS and EIBDS in grid-based wireless sensor networks

Handenahalli Channareddy Kantharaju*

Department of CSE,
Vemana Institute of Technology,
Bengaluru, Karnataka, India
Email: hc.kantharajuvit@gmail.com
*Corresponding author

K.N. Narasimha Murthy

Faculty of Engineering,
Christ (Deemed to be University),
Mysore Road, Bengaluru, Karnataka, India
Email: murthy_knn@yahoo.co.in

Abstract: Wireless sensor network is a peculiar kind of ad hoc network, consists of hundreds of tiny, resource constrained as sensor nodes. Clustering is a demanding task in such environment mainly due to the unique constraints such as energy efficiency and dynamic topology. In this paper, a novel energy efficient cluster-based routing algorithm is proposed on which Hierarchical identity-based digital signature (IBDS) and enhanced-identity-based digital signature (EIBDS) scheme is concerning in grid-based wireless sensor networks. Firstly we form clusters using multi-parameters-based type-2 fuzzy logic algorithm. This paper proposes an improved ant colony optimisation algorithm, which optimises the energy consumption on data transfer in a WSN. Each node in a sensor network is authenticated using elliptic curve cryptography (ECC). After a set of simulation tests on NS-3 simulator, our proposed work achieves good performance for various metrics.

Keywords: grid-based WSN; security; hierarchical identity-based digital signature; elliptic curve cryptography; ECC; clustering and routing.

Reference to this paper should be made as follows: Kantharaju, H.C. and Murthy, K.N.N. (2020) 'An energy efficient authentication scheme based on hierarchical IBDS and EIBDS in grid-based wireless sensor networks', *Int. J. Information and Computer Security*, Vol. 13, No. 1, pp.48–72.

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

K.N. Narasimha Murthy is a Professor of Faculty of Engineering, Christ (Deemed to be University), Bengaluru-560074, KA, and India. He is 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.

1 Introduction

Wireless sensor network is a great solution for solving many real-time and non-real-time applications like observing environmental pollutants, tracking and detecting the passage of tanks and troops on a battle field, tracking the location of personnel in a building and estimating traffic flows on roads. The sensor nodes are highly capable in individual to send data to its neighbouring. Due to this consideration, security is a major concern in wireless sensor networks. In order to provide secure and efficient data transmission, there are still some challenges to be addressed. The individual sensor nodes in the network are capable of sensing, transmitting and receiving information about their environments. Secure data transmission is mandatory and demanded in many WSNs. To provide security, wireless communication should be encrypted and authenticated. Key management is a challenging issue in wireless sensor networks when concentrated on security. Due to resource constraints, obtaining such key agreement is nontrivial. There are five critical issues for key management authenticity, confidentiality, integrity, scalability and flexibility. A sensor node has limited scalability so need effective key management for secure communication. In Kantharaju and Murthy (2017a), authors have discussed about the routing in wireless sensor networks. These schemes highly support the energy efficient, and security aware applications. In order to enhance the security, and minimises the energy consumption and end-to-end delay rate. There exist a number of key management schemes. In typical applications, there exist three categories of general key agreement schemes: trusted server, key pre-distribution and self-enforcing scheme. In trusted-server scheme, key agreement between nodes is depends on a trusted server like Kerberos. But this type of scheme is not suitable for WSN since there is no trusted infrastructure in it (Anbarasi and Gunasekaran, 2015). In self-enforcing scheme, asymmetric cryptography that is public certificates is used. However, a sensor node has limited power and computational resources (Azarderakhsh et al., 2008). The third type of key agreement scheme is key pre-distribution. This scheme distributes the key information among all sensor nodes. Due to the random node deployment, identifying the set of neighbours might not be possible (Du et al., 2004). Therefore, secure communication is a very important requirement in WSN (Zhang et al., 2009). In recent times, digital signature is one of the most critical and feasible security approach provided by cryptography in asymmetric key management system. To handle this problem, identity-based cryptography (ID-based signature – IBS) and online/offline signature schemes (IBOOS) have utilised to authenticate a user and then generates a session key for the secure communication. However, they used an insecure identity-based online/offline signature in Yasmin et al. (2012), Li et al. (2012), and Patle and Satao (2015) respectively. Other major constraints in WSN are listed and illustrated as follows: energy constraints, memory constraints, unattended operation of network, higher latency in communication, and unreliable communication (Sen, 2013). Currently, researchers have investigated two common problems in wireless sensor networks, i.e., energy consumption problem and routing problem. Clustering the sensor nodes keep the network lifetime as long and minimise the delay and energy consumption (Hassan and Selim, 2015). Cluster-based key management schemes of a WSN keep the data safe and forward in secure manner. However, the key management schemes require less energy computation and computation (Walid et al., 2017). On the other hand, several grid-based wireless sensor networks are proposed which improves the resiliency and connectivity (Mohaisen

et al., 2009). In most of the WSNs, nodes are often randomly distributed across a given environment. In such cases, grid-based clustering techniques are adopted for efficient clustering where the given geographical area is divided into several virtual grids. A different energy efficient grid-based WSNs have been proposed in Messai et al. (2016), Farman et al. (2016) and Jan et al. (2017), but still energy efficiency and network life time are open issues due the randomised nature of WSN. The iterative process of cluster formation and cluster head (CH) selection will results in better energy consumption of the sensor nodes and leads to better performance of the network. This paper focuses on a technique that can ensure security by applying identity-based digital signature (IBDS), enhanced-IBDS (EIBDS) to maximise the network performance.

1.1 Major contributions of the paper

In this paper, we propose hierarchical-based IBDS and EIBDS scheme

- We propose an energy efficient grid-based clustering technique in WSNs using multi-parameter-based type-2 fuzzy logic system (T2FLS) that selects the CHs to create a connected network since clustering is a backbone of WSN. The decision of each sensor is based on their position, residual energy (RE), the number of nodes neighboring CHs, and an estimate of distance between nodes will benefit from being a CH.
- We propose a routing technique in clustered WSNs. We form an energy efficient path using improved ant colony optimisation technique.
- Furthermore, each sensor node is authenticated and verified by digital signature. For that authenticator and authenticator server are used in hierarchy manner. Authenticator server is responsible for generating private key. This key is generated using ECC algorithm.
- Finally, hierarchical IBDS and EIBDS are compared to the other schemes by using extensive simulations.

The rest of paper is organised as follows: Section 2 reviews the recent research to various protocols and algorithms whose aim is to optimise the energy consumption and network lifetime. The problem definition is presented in Section 3. Section 4 describes the architecture of our proposed WSN with hierarchical structure while Section 5 performs a series of proof of concept simulation experiments in order to prove the efficiency of the proposed system and compare it results with the existing approaches. Finally we concluded paper in Section 6.

2 Review of literature

This section focuses on existing literature where many researchers have discussed different key management techniques, clustering techniques and routing techniques but still issues such as energy consumption, security, and network lifetime exist. In addition, network topology management is also very important to uniformly distribute the nodes in grid and make the network efficient. Keeping in view the aforesaid issues, recent relevant existing approaches are briefly discussed below.

2.1 Review on authentication and key management

A wireless sensor network is more vulnerable to various attacks due to their nature of dynamic topology. However, providing authenticity in WSN poses variant issues and thus it requires power saving and lightweight cryptographic algorithms to efficiently support WSN security. Tawalbeh et al. (2017) have extensively reviewed the lightweight cryptography algorithms. These algorithms are specifically designed for resolving the security problems in sensor networks. Liu et al. (2010) have presented an online/offline identity-based signature for the WSN. An identity-based cryptography is eliminates the necessity for validating of certificates. This paper reduces computation cost and communication overhead, especially, when new node added to the network, other nodes in the network do not need to have its certificate. In addition, computational cost is further reduced by checking online/offline signature. In the offline signing algorithm, secret information does not invoked by any trusted third party. Around 160 group elements are considered and pre-computed for signing a few messages. Thus, this proposed scheme is applicable for small-scale network. Rossi and Schmid (2015) discussed the building and implementation of identity-based signature schemes which make use of bilinear pairings to get shorter signatures. Special mappings between groups known as bilinear pairings in which DL problem (Diffie-Hellman problems) over elliptic curves transferred. Bilinear pairing provided some special properties include bilinearity, not-degeneracy, and computability. With this property, authors obtained computation system. The elliptic curve cryptography (ECC) working on elements which defined over finite fields. Pairing of two groups decreases the network life time. Qin et al. (2016) have proposed two-identity-based signature schemes with the application to group communications. In the first identity-based scheme, users and key generation centre (KGC) performs the following steps: setup, key generation, signing and verification whereas the second identity-based signature follows the same procedure of IBS-1. Both identity-based signature schemes are insecure against forgery attacks. Moon et al. (2016) authors proposed ECC-based digital signature algorithm (ECDSA) for a resource constrained network, i.e., wireless sensor network. Mutual entity authentication protocol is incorporated between the entities (CHs, nodes and base station) are required before the sensor data is exchanged. The proposed ECDSA algorithm contains two parts: signature generation and signature verification while mutual authentication protocol comprised of following phases: initialisation phase, signature generation phase, signature verification phase, and mutual authentication phase. Let us assume that sensor nodes i and j authenticate each other and their mutual authentication can be obtained by using their respective signatures and public certificates. Individual sensor nodes should be authenticated with their unique identities. It also requires some extensive testing and verification processes. Song and Zhao (2017) have illustrated the concept of code-based cryptography against security attacks. Compared to other code-based IBS schemes, the proposed code assumptions-based IBS improve the security which depends on the Bleichenbacher attack. The master key extraction and user key extraction are the major phases involving in this paper. Gandino et al. (2017) have presented symmetric encryption-based security scheme is for wireless sensor networks. The major concern of this paper is to establish the symmetric keys. For this purpose, proposed Q-S composite (QSC) that exploits the best features of random predistribution and enhance its lower requirements in to upper. The QSC working procedure follows random key distribution and also it uses bitwise XOR operation instead of using a hash function. In this operation,

very limited number of predistributed keys are used for pairwise key generation. Another novelty presented in this paper is storing organisation using advanced encryption standard (AES). The selection of parameter s is based on the parameters of the network. Initially s is increasing but after a maximum, it decreases again so that the best configuration of QSC is required. Mensah et al. (2017) presented tamper aware authentication framework for wireless sensor networks. In wireless sensor networks, energy efficient authentication is intended but it is difficult to adequately meet the security requirements and resource limitations. Various security algorithms such as SHA-1, SHA-224, MD-5, SHA-384, and SHA-512 are reviewed and finally conclude that the SHA-224 is the most energy efficient option for authentication. The main motive of this paper is to protect the sensor nodes sensitive information from the internal memory of the micro controller. The authentication tokens of suspected nodes in the field are revocated in the deployment. Kantharaju and Murthy (2017b) have presented two different approaches such as IBDS and enhanced IBDS (EIBDS) for online and offline signing. These approaches reduce communication and computation overhead compare to existing protocol LEACH.

2.2 Review on clustering and grid-based clustering

Due to the limited battery power and the difficulty in recharging the batteries, sensors need to be deployed with a high density. Various distributed clustering algorithms and techniques are more useful in WSNs. Gupta et al. (2015) proposed clustering-based routing in sensor networks. The presented clustering technique is homogeneous and the CHs elected based on the number of neighbours and node RE. Then the route optimisation technique is proposed to obtain an energy efficient path from source to the destination. The lifetime of the network increases due to the optimum path in clustered WSNs. The random number is considered at the beginning of each round that range between (0, 1). When the random number is less than the probability of sensor i in region, then the sensor i is elected as a CH-candidate so that the maximum number of sensors are elected as a CH-candidates. However, the large size of CHs with average hop count of routing path will not improve the performance in terms of energy consumption and network life time. Li et al. (2017) have introduced fuzzy power-optimised algorithm for clustering and routing. Based on the node degree, sensor nodes are categorised into different categories. After that CH is elected in the same category using multi-parameter iteration. In last, transmission control of cluster nodes are adjusted by fuzzy control algorithm. Distance between the nodes will be considered as input for fuzzy control. The fuzzy rules are follows:

1 if receiving power of a node is weak, then the distance nodes is far

2 if receiving power of a nodes is medium, then the distance between nodes is medium

3 if receiving power of a node is strong, then the distance between the nodes is near.

Therefore, this paper reduces the energy consumption by fuzzy power control and multi-parameter iteration. Zhang Y et al. (2017) presented fuzzy logic approach with non-uniform distribution in wireless sensor networks. This paper is based on multi-hop communication with proposed energy efficient clustering algorithms for wireless sensor

networks. Nodes RE, degree and neighbour nodes energies are taken as input parameters for CH election and also computes the probability of being as CH with aid of FIS in a distributed manner. Fuzzy logic can able to handle uncertainties in the wireless sensor networks but does not consider the location of the base station. This factor affects the clustering along with the CH election process. Bing Zeng et al. (2017) presented an energy efficient clustering and routing scheme for WSNs called improved harmony search clustering and routing (IHSCR). Thus, this paper consists of clustering and routing and the main contributions are as follows:

1 clusters are formed using discrete encoding scheme

2 gateway is chosen by a roulette wheel selection method

3 new harmony is improvised based on the harmony memory considering rate

4 during the iterations of harmony memory, a local search scheme is designed to enhance the best harmony.

Harmony search optimisation is effectively solves the energy consumption problem, but the global harmony search optimisation is required for large scale network. Thus, this proposed scheme is suitable for small scale network. Kantharaju and Murthy (2018) have presented secure QoS-based explicit routing algorithm for secure data transmission. Initially cluster is formed using genetic algorithm and particle swarm optimisation (GA and PSO) algorithm. After the CH selection, IBDS and EIBDS is proposed to establish the secure communication. To ensure security, AES is proposed which avoids the hacking of data by intruders.

2.3 Review on routing

For energy conservation, various energy efficient routing approaches are employed to reduce the energy computing of the system. The energy efficient routing protocols are low energy adaptive clustering hierarchy (LEACH) (Patel et al., 2011), LEACH-multilayer (LEACH-MF) (Yan and Liu, 2011), LEACH-centralised (LEACH-C) (Sharma et al., 2015), modified LEACH (MODLEACH) (Yan and Liu, 2011), power efficient gathering in sensor information systems (PEGASIS) (Pandya et al., 2015), energy efficient PEGASIS-based protocol (EEPB) (Nehra and Sharma, 2013), mobile sink improved energy-efficient PEGASIS-based routing protocol (MIEEPB) (Singh and Kaur, 2014). Amjad et al. (2017) proposed QoS aware cluster-based routing for heterogeneous WSNs. This scheme supports the delay sensitive, time-critical, bandwidth hungry applications. In order to minimise the delay, the network considered to be stable. To route the packets, multiple paths are provided. This paper intends to provide energy harvested paths to improve the network lifetime, throughput and stability. But still the energy conservation rate is low. Warrier and Kumar (2016) reviewed that the routing techniques in wireless sensor networks which are energy harvesting in nature. In WSN, each and every sensor node should meet the scalability and energy efficient issues. For this reason, hierarchical architecture is constructed to provide the scalability and also extend the network lifetime. In this paper, the variants of hierarchical protocols have compared that are LEACH, LEACH-C, PEGASIS, TEEN, BCDCP, HEED, APTEEN, etc.

3 Problem statement

In Sharma et al. (2017), authors contributed the concept of authentication through digital signature. For authentication, message signing takes high computational cost. For this reason, in this paper authors presented a pairing-free IBDS (PF-IBS) algorithm in WSN which outperforms against adaptive chosen message attack. The proposed IBDS not follows its basic nature due to this the public key cannot generated for users identity but users retrieve the private key first. The role of PF-IBS is follows: system initialisation, key-generation, signature generation, and signature verification. In this algorithm, the private keys are computed by all sensor motes with corresponding identity. This paper overwhelms the problem of computational complexity on sensor device. PF-IBS generates private key using master secret key and then computes its public key. And also it is very complex in key generation and storage. So that the authentication is not efficient and not scalable. In Ferng and Khoa (2016), authors presented digital signature scheme to enhance the data authenticity. The proposed scheme overcomes the problem during end-to-end data authentication by digital signature. This paper depicted by a cluster-based wireless sensor network with large number of static sensor nodes and stationary sink. An adversary model could eavesdrops the channel which injects false packets and response with older data packets. Using digital signature, an en-route filtering mechanism with end-to-end authentication could prevent forgery from intermediate nodes. Moreover, the proposed approach uses two secret keys for end-to-end data authentication which leads to large storage overhead. In Lu et al. (2014) authors have referred to a secure data transmission for cluster-based WSNs. Forming clustering is a challenging issue, but in this paper authors formed clusters in dynamic and periodic manner. Authors introduced SET protocols, i.e., SET-IBS and SET-identity-based online/offline scheme (SET-IBOOS) in cluster-based WSNs. The SET-IBS reduces the computational overhead by resolving the problem of Diffie-Hellman (DH) in the pairing domain. Subsequently, the SET-IBOOS further reduces the computational complexity with respect to the security requirements. To mitigate the aforesaid issues, we proposed a novel algorithm for improving security in WSN.

4 Proposed work

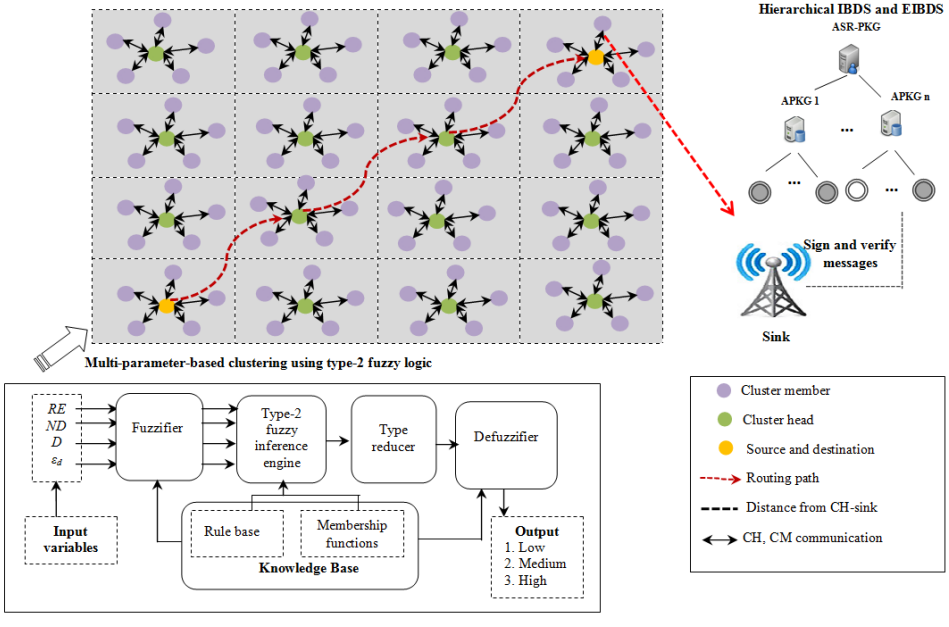
4.1 Overview

In this paper, hierarchical IBDS and EIBDS is proposed in grid-based clustered WSNs, which ensures proper selection of CH among all the eligible nodes in the network. The overall architecture is shown in Figure 1.

All sensor nodes are homogenous and after deployment, all nodes are stationary. To avoid the delay in data transmission and more energy consumption, we select a sensor node as the CH which has minimal distance from sink. Our proposed work is divided into following steps: Initialisation, set-up, routing and security, which are described subsequently. In initialisation phase, sensor nodes are deployed in a grid structure. In the set-up phase, cluster formation and CH selection takes place. In each cluster, we select CH which has minimal distance from sink node, high RE, and also node degree is considered for CH election. In the routing phase, optimal forwarding node is selected using forwarding probability function. We proposed Multi-Parameter-based Clustering

using T2FLS algorithm to reduce the total distance for data transmission. The components of T2FLS are fuzzifier, type 2 fuzzy interface engine, type reducer, defuzzifier and output. Enhanced Ant Colony Optimisation is proposed for routing. To overcome the mutual authentication, bilinear pairings, and public key generation, we presented hierarchical-based IBDS and EIBDS scheme. In our proposed work, ECC is used for initial key generation for a particular sensor node. Here we used authentication server root private key generator (ASR-PKG) and authenticator private key generator (APKG). IBDS is a key management scheme in WSN for security. For that issue, we invoke individual authentication scheme. Once the CH finished the data preparation for report forwarding, it uses private key (generated by elliptic curve), identity and time stamp for signing the message before being sent to sink node. Sensor nodes are dynamic. If any new node added in to any cell on the grid, CH verified its authentication and aggregates the data from new nodes. In EIBDS, private keys are regenerated using ECC and forwards to each node.

Figure 1 System architecture (see online version for colours)



4.2 Construction of the grid structure

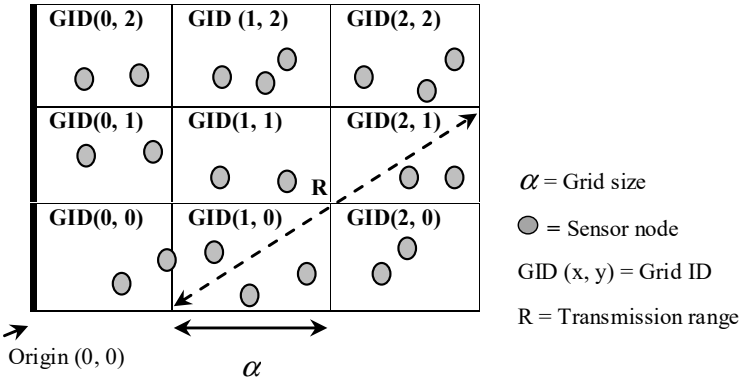
In this paper, we divide the monitored area into a number of grid cells of equal size. The grids are constructed with a unique pair of numbers [grid identification (GID)] based on the sensor node transmission range which is used to identify each grid cell, such as is shown in Figure 2. Figure 2 shows the construction of grid structure. In order to compute the grid size, we proceed as follows. The geographic position of the origin indicates (X_0, Y_0). After setup of origin, grid size is defined α is determined using transmission range

$R\left(\alpha = R/\sqrt{2}\right)$. Once sensor nodes are deployed, each node computes the GID of the grid cell to which it belongs with its geographic coordinates (x, y)

$$GID(x, y) = \left\{(x, y) | x = \left[\frac{X - X_0}{\alpha}\right], y = \left[\frac{Y - Y_0}{\alpha}\right], \right. \\ \left. (X_0, Y_0) \in origin(0, 0)(X_0 \le X) \wedge (Y_0 \le Y); \alpha : Grid\ Size\right\} \quad (1)$$

The connectivity between sensor nodes to the neighbour sensor nodes claimed from equation (1). If the node is from any corner of the grid then also it can communicate with its neighbour node.

Figure 2 Construction of the grid structure



4.3 Clustering using T2FLS

The CH selection using T2FLS will dynamically elects the CH in a grid. Each sensor node individually calculates its own output value based on the four different variables that are inputs of the type-2 fuzzy system. The input variables of the T2FLS are the following:

- *Residual energy (RE)*: RE is an important factor for selecting a node as CH. It is measured as a percentage of the maximum battery of the sensor node. The CH is responsible to send the data to sink node. Before that, it collects data from members, aggregates the collected data, and then it forwards to the sink node. For this reason, RE of each sensor node is required for a CH. The RE (RE) of node is calculated as given below.

$$RE = E^{Initial} - \left(E^T(k, d) + E^R(k) + \sum_{S_i=1}^{N} E^R(k) + E^{agg}\right) \quad (2)$$

where $E^{Initial}$ represents the initial energy level for node S_i, $E^T(k, d)$ is the energy required to transmit k number of bits to a distance d, where d is the maximum transmission range of sensor node S_i, $E^R(k)$ is energy spent for receiving a packet and E^{agg} is the amount of energy spent to aggregate number of packets

- *Node degree (ND)*: ND is the current position of the sensor node within the communication range R. The transmission power is depends on the node degree. It is also an important parameter in a sensor network since un-optimised transmission power of a node either fails link to neighbouring nodes or drop the packets.
- *Distance from sink node (D)*: D is the distance between a sensor node to the sink and computed using Euclidean distance as follows:

$$D(S_i, Sink) = \sqrt{(x_i - x_{sink})^2 + (y_i - y_{sink})^2} \tag{3}$$

  where x_i and y_i are the geographical coordinates of sensor node whereas x_{sink} and y_{sink} are the coordinates of the sink.
- Expected delay (ε_d): ε_d is defined as the expected amount of time needed to successfully transmit a packet

The output variable has one possibility. For all constraints (energy, memory, and delay) perspective, output variable is a crisp output value to which CH capability of a sensor node is determined. A sensor node which is having the greater RE, minimal distance and large node degree will have the more probability to be elected as a CH. The output variable has three output linguistic variables and they are 'low', 'medium' and 'high'. The higher possibility value represents higher chance of a node in electing as a CH. The input variables are converted into fuzzy linguistic variables which are based on the fuzzy inference system (FIS) membership function. Mamdani method is used to develop the fuzzy 'IF-THEN' rules. These fuzzy rules are generated by mapping the input variables to the corresponding fuzzy output variables. In total, 81($3^4 = 3 \times 3 \times 3 \times 3$) fuzzy rules are computed based on the three output linguistic variables ('Low', 'Medium', and 'High') and four input variables ('RE', 'ND', 'D', and 'ε_d'). Few of the fuzzy IF-THEN rules are presented in Table 1.

Table 1 Fuzzy if-then rules

Input variables				*Output variables*
RE	*D*	ε_d	*ND*	
High	High	High	High	Low
High	Medium	Medium	Medium	Medium
high	Low	Low	Low	High
high	Medium	High	High	Low
Medium	Low	Medium	Medium	Medium
Medium	Low	Low	Low	Medium
Medium	High	High	High	High
Medium	Medium	Medium	Medium	Medium
Low	Low	Low	Low	Medium
Low	High	High	High	Low
Low	Medium	Medium	Medium	Low
Low	Low	Low	Low	Medium

In this paper, once the final CH has been elected, the non-CH members join the CH based on the four input variables. Some of the fuzzy IF-THEN rules of determining the CH possibility are

Rule 1 IF the distance to the CH is close (*low*), RE is *high*, expected delay is *low*, and node degree is *low*, THEN the possibility is very *high*

Rule 2 IF the distance to the CH is close (*high*), RE is *low*, expected delay is *high*, and node degree is *high*, THEN the possibility is very *low*.

Algorithm 1 For clustering using T2FLS

```
1   Begin
    Input    A number of nodes in Grid-based WSNs
    Output   Clustered WSN
2   for k =1 to n do //'n' number of grids
3   for i =1 to m do //'m' number of sensor nodes
4   for all nodes in the grids. Computes
      i.   Residual energy (RE)
      ii.  Node degree (ND)
      iii. Distance from sink node (D)
      iv.  Expected delay (ε_d)
/*Find possibility using IF-THEN rules*/
5   Possibility = FuzzyPossibility (RE, ND, D, ε_d)
6   if (y < Possibility_threshold) //y = output value
        m_k(i) elected as CH //CH = cluster head
    else
        elected as CM //CM = cluster member
7   for all cluster members
8   Send Join_Request to nearest CH
9   end for
10  end for
11  end for
12  end
13  exit
```

Algorithm 1 describes the procedure of T2FLS. The T2FLS is used for clustering the nodes. The possibility value is computed for each node (after the IF-THEN rule). The possibility value range is from 0–1 and the possibility threshold value becomes >0.75.

4.4 Hierarchical IBDS and EIBDS in grid-based CWSNs

In this paper, we presented a three-level IBDS with support of batch verifications of the sink node. It is hierarchical structure (i.e., tree-based structure), where the level-0 node is the root authenticator server which also acts as a private key generator (PKG), which play a significant role. The hierarchical structure has improved the network scalability and

lifetime. The root PKG keeps the master key pair (M_{SK}, M_{PK}) which will be used to generate using ECC. The level-1 nodes are authenticators, each with an identity like ID_A. The authenticators are the second level PKGs which can generate the secret signing keys for the bottom level nodes. The level-2 nodes are the sensor nodes each with an identity like ID_S. Our proposed Hierarchical-based IBDS and EIBDS scheme consists of the following phases:

- *Setup phase*: on input a security parameter *C*, ECC algorithm allows the root PKG to generate the master secret key M_{SK} and the master public key M_{PK}.
- *Extract phase*: on input of the master secret key M_{SK} and an authenticator ID_A, a secret key SK_{ID_A} for ID_A.
- *Key phase*: on input of the secret key SK_{ID_A} for an authenticator identity ID_A and sensor node ID_S. Here we generates a secret key SK_{ID_S} for ID_S belonging to ID_A with the help of ID and master key pair.
- *Sign phase*: on input of secret key SK_{ID_S} and a message m. In this phase, we generate a signature *S* of *m*.
- *Verify phase*: on input of a signature *S* on messages *m* with respect to authenticator identity ID_A and node identity ID_S. In this phase, outputs either 0 or 1, where 1 represents that the signature is valid.
- *BVerify phase*: on input of a list of signatures such as $S_1, S_2, S_3, \ldots, S_n$ on messages $m_1, m_2, m_3, \ldots, m_n$ with respect to authenticator identities $ID_{A_1}, ID_{A_2}, ID_{A_3}, \ldots, ID_{A_n}$ and node identities $ID_{S_1}, ID_{S_2}, ID_{S_3}, \ldots, ID_{S_n}$. This BVerify phase produce outputs either 0 or 1, where 1 represents that all of the m signatures are valid.

Definition 1: Hierarchical IBDS scheme with batch verification is said to true, if for any master key pair (M_{SK}, M_{PK}) ← setup, the following conditions hold:

- For any identity ID_A, ID_S and any message *m*,
  1 If $S \leftarrow Sign(SK_{ID_S}, m)$ where $SK_{ID_S} = Extract(SK_{ID_A}, ID_S)$
  2 $SK_{ID_A} \leftarrow Extract(M_{SK}, ID_A)$
  3 Verify $(S, ID_A, m, ID_S) \leftarrow 1(\therefore Valid)$ /*If($0 \leftrightarrow invalid$)*/.
- For all identities of authenticators $\{\Sigma_{i=1}^{N} ID_{A_i}\}$, $nodes\{\Sigma_{i=1}^{N} ID_{S_i}\}$, and messages $\Sigma_{i=1}^{N} m_i$
  1 If $S_i \leftarrow Sign(SK_{ID_{S_i}}, m_i)$ where $SK_{ID_{S_i}} = Extract(SK_{ID_{Si}}, ID_{S_i})$
  2 $SK_{ID_{A_i}} \leftarrow Extract(M_{SK}, ID_{A_i})$
  3 $BVerify(\Sigma_{i=1}^{N} m_i, \sum_{i=1}^{N} ID_{A_i} \Sigma_{i=1}^{N} ID_{S_i}, \Sigma_{i=1}^{N} S_i) \leftarrow 1(\therefore Valid)$ /*If ($0 \leftrightarrow invalid$)*/.

In verify phase, we have check the single signature as valid or not whereas in Bverify phase we have check for the list of signatures for a list of messages. Here we check all lists of signatures as valid or not. Figures 3 and 4 describe the representation of hierarchical IBDS and sign and verify phases respectively.

Figure 3 Representation of hierarchical IBDS (see online version for colours)

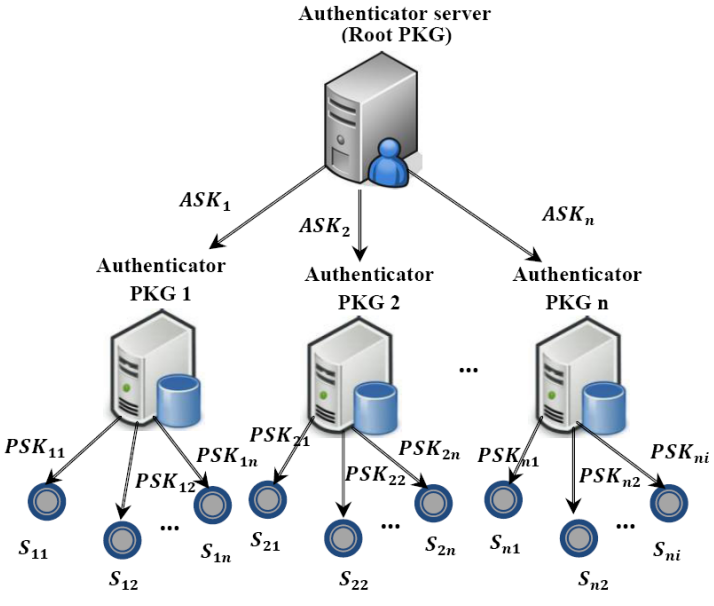
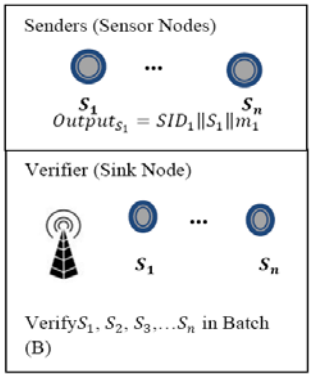


Figure 4 Sign and verify phases (see online version for colours)



4.5 *Routing using I-ACO*

Efficient data routing in energy constrained WSN is a demanding tasks. For energy consumption perspective, we find the optimal path of data transmission using Improved ant colony optimisation algorithm. In I-ACO routing model, routing could be described by the heuristics function. Based on the improved heuristic function, we considering various criterions from the source to the destination node. It could maximise the initial efficiency of algorithm and ensures the stability. The criterions employed in our approach are the following

1 minimum distance from network nodes

2 sum of distances from network nodes

3 maximum forwarding probability from CHs.

For ant colony optimisation, each ant selects the next path according to a probabilistic decision, which is written by,

$$\rho_{ij}^{m} = \begin{cases} \dfrac{(\tau_{ij}(t))^{\alpha}(\delta_{ij}(t))^{\beta}}{\sum_{t \in allowed_t}(\tau_{ij}(t))^{\alpha}(\delta_{ij}(t))^{\beta}}, & j \in allowed_t \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where t is the iteration number and $\tau_{ij}(t)$, $\delta_{ij}(t)$ are the pheromone and heuristics function laid on edge (i, j), m is ID (m = 1, 2, …, k) for ants and α, β are relative importance of accumulation information and inspired information respectively.

4.5.1 Forwarding probability computation $(\mathbb{P}_{ij}(t))$

In order to find energy consumption of the node, in this paper we find the probability of neighbour nodes in the transmission range. It improves the performance of the network. Thus, the forwarding probability is calculated by,

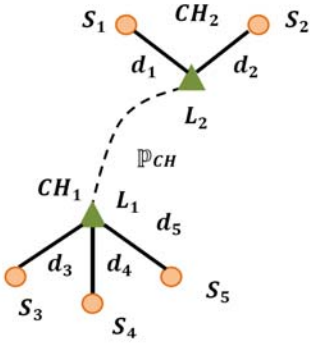
$$\mathbb{P}_{ij}(t) = \frac{L_{ij}}{\sum_{S_i=0}^{N} L_{ij}} \tag{5}$$

From Figure 5, we distance between the sensor node to CH and the probability between two CHs computed by

$$\mathbb{P}_{CH}(t) = \frac{L_2}{L_1 + L_2} \tag{6}$$

where L_1 and L_2 are distance between sensor node to CH 1 and CH 2.

Figure 5 Forwarding probability calculation (see online version for colours)



4.5.2 Pheromone update improvement

In the tradition ACO algorithm, it is often considered too large pheromone for finding the shortest path. To avoid such issues, pheromone is updated. It may results in a relatively faster local convergence, the pheromone is limited by a threshold.

$$\tau_{ij}(t+1) = \begin{cases} \mu, & \tau_{ij}(t+1) > \mu \\ (1-P)\tau_{ij}(t) + \sum_{m=1}^{k} \Delta\tau_{ij}{}^{m}, & \text{else} \end{cases} \tag{7}$$

where μ denotes the threshold value between 0–1, σ represents the pheromone strength, m is the total number of ants, l_m is the path length of the m^{th} ant, P is the coefficient of the pheromone volatilisation, $P \in (0, 1)$. When all ants reach the destination, each individual ant corresponds to a route. In this paper, we find a fitness function for optimal route election. Thus, the fitness value of each route can be computed by the following equation.

$$F_m^k = avg_E \times \min_E \times \varphi / l_m^k \tag{8}$$

where avg_E represents the average node RE, $\min_E$ refers to the node minimal energy of ants passing towards the route and φ represents the number of nodes. l_m^k denotes the route length for m^{th} ant and k^{th} iteration. Here we consider the larger fitness value is the more optimal route. After finds the fitness value, pheromone concentration on this particular route is updated. In this way, the route with higher fitness value will be chosen after several t and finally the energy consumption of the network will be improved.

4.5.3 Improved heuristics function

The general ACO and some modified versions of the ACO algorithms consider only the transfer distance to the next node j, but do not consider the distance from the node j to the Sink. This affects the network performance especially in energy consumption. Within the transmission communication range, selecting the node closer to the sink node the smaller energy consumption of the network will be reached. Therefore, the heuristic function should not only consider the distance to the next node but also the distance to the sink.

$$\delta_{ij}(t) = \frac{1}{D_{ij}w_0 + D_{js}(1-w_0)}, w_0 \in (0, 1) \tag{9}$$

where w_0 is the parameter that controls the relative weight of D_{ij} and D_{js} indicates the distance from the next node j to the Sink.

5 Simulation and performance analysis

In this section, we evaluate the performance of our proposed algorithms under various simulations, The goal of the simulation is to compare the performance of our proposed system with the exiting methods.

5.1 Simulation environment

We simulated our proposed method using NS-3 simulator. Our simulation scenarios have set of simulation parameters and values. Simulation settings will be shown in Table 2. Nodes are responsible for sensing data and sending data to the Sink node. The nodes are distributed within the region of 300 m × 250 m. The total number of node (N) is 25. The initial energy of nodes is 800 Joule. The transmission range of a sensor node is set to be m with a data rate of 10 kbps. The sensing range of a sensor node is 40 m. The packet length is 1,024 bytes. We created a WSN network have CHs, cluster members, sink node, authentication server, source and destination node. The simulation scene representation is shown in Figure 6. Table 3 describes the different key management schemes in wireless sensor networks.

Figure 6 WSN snapshot representation (see online version for colours)

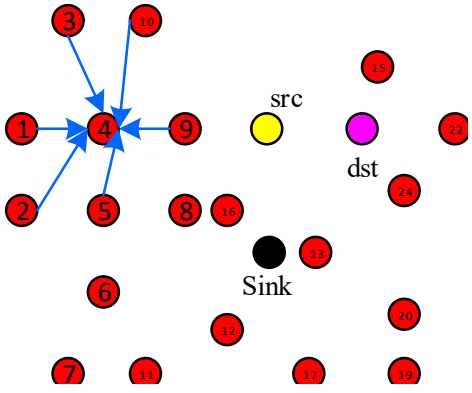


Table 2 Parameters of simulation

Parameters	*Values/units*
Area of the sensor field	300 m × 250 m
Number of nodes	25
Initial energy of sensor nodes	800 Joule
Communication range	40m
Energy of elected CH	800 Joule
Packet size	1,024 bytes
Sink node range	40m
Sink node location (x, y)	800 Joule
Probability of selecting a CH	0.9
Simulation time	15 seconds
MAC protocol	IEEE 802.15.4
Mobility model	Random waypoint model

Table 3 Different key management schemes in WSN

Schemes/measurement	*Patle and Satao (2015)*	*Sharma et al. (2017)*	*Proposed*
Security agent	CH	Sensor node	CH
Key independence	Medium	Low	High
Key refresh	No	No	Periodically and each session
Data authentication	Associated key	Pairing free authentication	Associated key
Forward secrecy	Medium	Medium	Strong
Backward secrecy	Medium	Medium	Strong
Efficiency	Lower	Greater	Greater
Static/dynamic	Static	Static	Dynamic
Scalability	Low	Medium	Yes

5.2 Performance metrics

Performance of our proposed system can be evaluated in terms of average energy consumption, average end-to-end delay, packet delivery ratio (PDR), throughput, normalised routing load (NRL), network life time and security strength.

5.2.1 Average energy consumption

It shows the average energy consumption during data transmission and helps to determine the life span of the entire wireless sensor network. Energy consumption of a node is analysed which is consumed by: packets reception, packet transmission and event sensing. Thus, the average energy consumption is computed by:

$$Avg_{E(C)} = \sum_{S_{i=1}}^{n} E_{sensing}\Delta(t) + E_R + E_T + N(r)_{dp} \tag{10}$$

where

$E_{sensing}\Delta(t)$ the energy consumed for sensing an event at time t

E_R the energy consumed for packets reception

E_T the energy consumed for packet transmission

$N(r)_{dp}$ the energy consumed for packet reception which depends only on the number of received messages

5.2.2 Average end-to-end delay

The end-to-end delay plays a vital role during the performance evaluation at a time limit data communication system. Therefore, the average end-to-end delay is defined by the following equation:

$$Avg_{E(d)} = \sum_{S_{i=1}}^{n} N\left(DP_S \Big/ R\right) \tag{11}$$

where N represents number of packets, DP_S denotes data packets size, and R is the transmission rate.

5.2.3 Packet delivery ratio

PDR is defined as the ratio of number of packets successfully delivered at the all the receivers to the number of data packets. The PDR rate is computed by the following formula

$$PDR = \frac{\sum_{S_{i=1}}^{N} Dp(R)}{\sum_{S_{i=1}}^{N} Dp(S)} \tag{12}$$

where $\Sigma_{S_{i=1}}^{N} Dp(R)$ represents the packets delivered at the receivers and $\Sigma_{S_{i=1}}^{N} Dp(S)$ denotes the packets successfully sent by all the senders.

5.2.4 Throughput

Throughput is defined by how much data packets can be transferred from the source to the receivers in a given amount of timeslots (t). It is computed by:

$$Throughput = \frac{No.\ of\ \ packets\ sent}{Time\ taken} \tag{13}$$

5.2.5 Normalised routing load

NRL is refers to the ratio of total no. packets received to the total no. of routing packets received. Thus it can be computed by:

$$NRL = \frac{No.\ of\ \ data\ \ packets\ received}{No.\ of\ \ routing\ \ packets\ received} \tag{14}$$

5.2.6 Network lifetime

Each sensor node has initial energy (E_0), a sensing radius (S_R) and we have also computed energy consumption rate of i-node (E_i). Thus the network lifetime (N_L) can be defined by:

$$\text{Network Lifetime } (N_L) = \frac{\sum_{S_{i=1}}^{N} B_i}{q_j} \tag{15}$$

where B_i represents life of node which is computed by $B_i = \frac{E_0}{E_i}$ and q_j represents coverage.

5.2.7 Security strength

Network system with cryptography will induce increased overhead causing decreased message throughput, increased power consumption, and increased latency in wireless sensors. Due to these constraints, we important to carefully tune and monitor the security strength and also in this paper we analysed and determined the security strength.

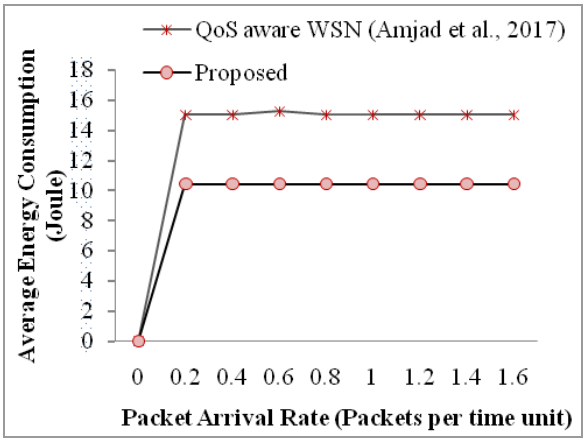
5.3 Comparison analysis

We evaluate and compare the performance of our proposed methods with other existing approaches using a number of quantitative metrics.

5.3.1 Average energy consumption

It is the most important parameter to evaluate the performance of the WSN. The average energy consumption in the proposed versus existing approach is illustrated in Figure 7.

Figure 7 Average energy consumption (see online version for colours)



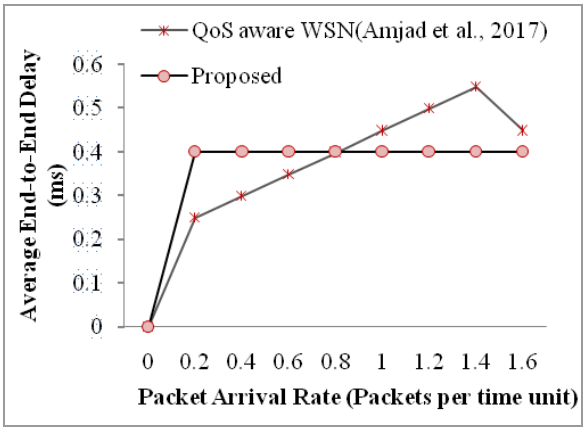
From Figure 7, we can say that our proposed algorithm has given better energy efficiency that the existing QoS aware WSN scheme. This improvement is mainly due to the clustering and routing approaches. T2FLS will reduce the uncertainty and improves the energy efficiency. In the case of QoS aware WSN, clustering is poorly performed. Our various CH election metric will improves the energy efficient than QoS aware WSN.

5.3.2 Average end-to-end delay

The end-to-end delay is the time from the packet generated by the source till it is delivered to the destination. The average end-to-end delay in the network is illustrated in Figure 8. As compared to existing scheme, i.e., QoS aware WSN, our proposed system has better performance and less average delay in case of large number of nodes.

From Figure 8, we can observe that the existing protocol gives poor performance. This is due to the transmission of large number of route request messages in the time t and this approach also inefficient when the time-critical data are sent.

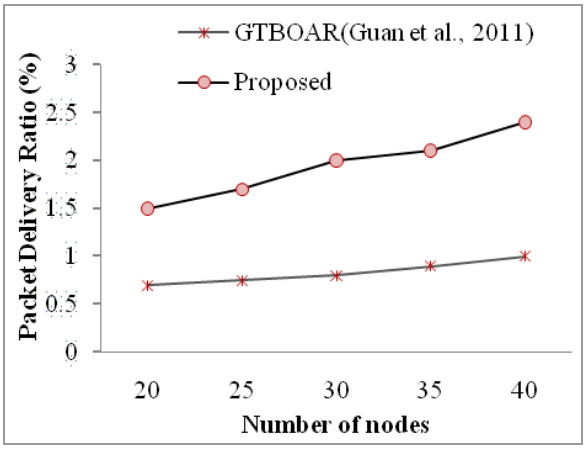
Figure 8 Average end-to-end delay (see online version for colours)



5.3.3 Packet delivery ratio

PDR is the ratio of successful packet transmission rate. We compare our proposed system with the existing, i.e., game theory-based obstacle avoidance routing (Guan et al., 2011) in terms of PDR, which is illustrated in Figure 9.

Figure 9 Packet delivery ratio (see online version for colours)

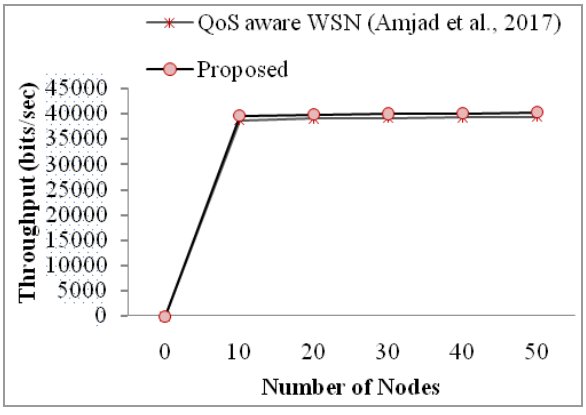


With the increase packet transmission delay, GTBOAR does not improve the packet delivery rate. In our proposed system, the process of forwarding node selection probability rate is greater than the GTBOAR so that the PDR of our proposed system does not decrease significantly with the increase of node.

5.3.4 Throughput

The throughput is defined as the total number of data packets successfully received at the sink node. Throughput performances are presented in Figure 10. Improvements in the throughput is achieved by the proposed algorithms

Figure 10 Throughput (see online version for colours)



From Figure 10, we can observe that the proposed system improved in the throughput than the QoS aware WSN approach. This improvement is mainly due to the minimisation of end-to-end delay and the availability of optimal path. This is also due to the easy transmission of packets to the destination since we have applied clustering approach. In the case of QoS aware WSN, end-to-end delay rate is high in the networks.

5.3.5 Normalised routing load

NRL is an important metric for evaluating the performance of routing. The small value of this parameter indicates that the system provides faster routing.

Figure 11 Normalised routing load (see online version for colours)

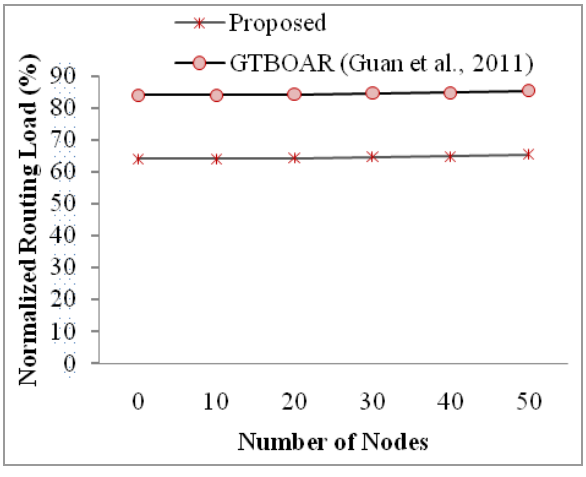
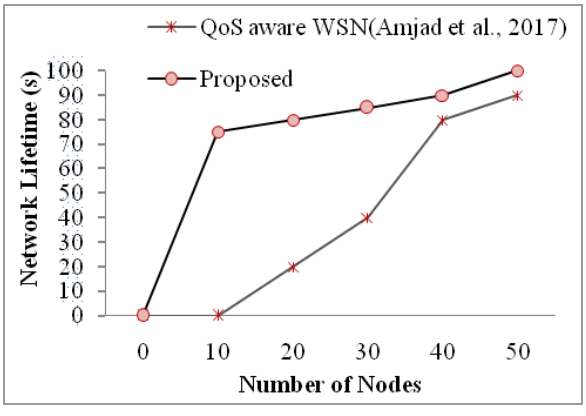


Figure 11 shows that the NRLs of the proposed versus previous approach [i.e., GTBOAR (Guan et al., 2011)]. Our proposed T2FLS system shows that the less routing load than the GTBOAR.

5.3.6 Network lifetime

Network lifetime can be defined in different ways as follows: This is the time duration/number of nodes until the first/last node dies or until certain percentage of nodes dies. Figure shows the comparison of the algorithms in terms of the network lifetime.

Figure 12 Network lifetime (see online version for colours)



From Figure 12, it is obvious to note that the proposed algorithms perform better than QoS aware WSN approach. At start of simulation, energy of node is calculated. If the energy level of node is drained, a node will automatically die. This enhancement is due to the optimal clustering and presence of the energy value. In the case of QoS aware WSN approach, energy conservation is not improved and the clustering process taken high execution time.

5.3.7 Security strength

Security strength is an important metric which is used in cryptographic analysis. It is varied depending on the algorithm and the key size used.

Figure 13 Security strength (see online version for colours)

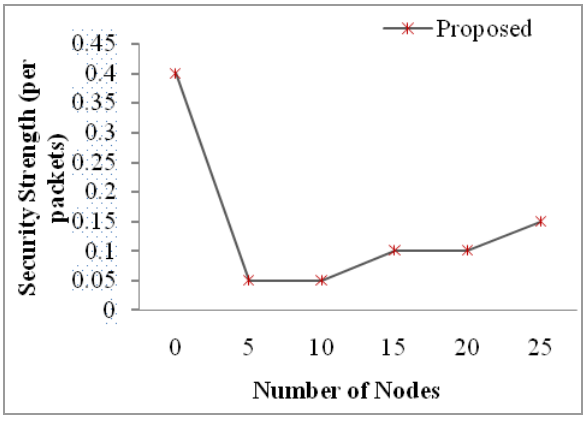


Figure 13 shows the results of our proposed security algorithms such as hierarchical-based IBDS and EIBDS scheme and ECC algorithm. To the best of our knowledge, we are the first in proposing hierarchical IBDS and EIBDS in WSN.

6 Conclusions and future enhancement

The wireless sensor network has differentiating characteristics such as energy limited node and weak node calculation ability, so we should make it efficiency and save sources in the design of wireless sensor network. Therefore, this paper puts forward into grid-based clustered WSN which is inspired by various novel algorithms. In this paper, we presented an efficient Hierarchical IBDS and EIBDS scheme designed for grid-based clustered WSN. To conserve the energy, type-2 fuzzy logic is proposed where we elect the CH based on the four input variables: RE, node degree, expected delay, and distance from the node to sink. Then we presented I-ACO for energy efficient routing. Through the simulations using NS-3, the proposed system is evaluated. From the simulation results, our proposed system outperforms than the existing systems. We have also proved the security of the scheme obtained best results such as strong security and lightweight computation.

In our future study, the proposed protocol needs to improved and tested to adopt the real-time dynamic environment. The proposed network model needs to be used symmetric key algorithms to efficiently manage the users associated key.

References

Amjad, M., Afzal, M.K., Umer, T. and Kim, B-S. (2017) 'QoS aware and heterogeneously clustered routing protocol for wireless sensor networks', *IEEE Access*, Vol. 5, pp.10250–10262.

Anbarasi, R. and Gunasekaran, S. (2015) 'Enhanced secure data transmission protocol for cluster based wireless sensor networks', *IEEE Sponsored 9th International Conference on Intelligent Systems and Control*, pp.1–4.

Azarderakhsh, R., Reyhani-Masoleh, A. and Abid, Z-E. (2008) 'A key management scheme for cluster based wireless sensor networks', *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp.222–297.

Du, W., Deng, J., Han, Y.S., Chen, S. and Varshney, P.K. (2004) 'A key management schene for wireless sensor networks using deployment knowledge', *Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, *IEEE INFOCOM*, pp.586–597.

Farman, H., Javed, H., Ahmad, J., Jan, B. and Zeeshan, M. (2016) 'Grid based hybrid network deployment approach for energy efficient wireless sensor networks', *Journal of Sensors*, Vol. 2016, pp.1–14, Hindawi Publishing Corporation.

Ferng, H-W. and Khoa, N.M. (2016) 'On security of wireless sensor networks: a data authentication protocol using digital signature', *Wireless Networks*, Vol. 23, No. 4, pp.1113–1131.

Gandino, F., Ferrero, R. and Rebaudengo, M. (2017) 'A key distribution scheme for mobile wireless sensor networks: q-s-composite', *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 1, pp.34–47.

Guan, X., Wu, H. and Bi, S. (2011) 'A game theory obstacle avoidance routing protocol for wireless sensor networks', *Sensors*, Vol. 11, No. 10, pp.9327–9343.

Gupta, H.P., Rao, S.V., Yadav, A.K. and Dutta, T. (2015) 'Geographic routing in clustered wireless sensor networks among obstacles', *IEEE Sensors Journal*, Vol. 15, No. 5, pp.2984–2993,.

Hassan, T.A.H. and Selim, G. (2015) 'A novel energy efficient vice cluster head routing protocol in wireless sensor networks', *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15)*, pp.313–320.

Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M. and Ali, S. (2017) 'Energy efficient hierarchical clustering approaches in wireless sensor networks: survey', *Wireless Communications and Mobile Computing*, Vol. 2017, pp.1–14.

Kantharaju, H.C. and Murthy, K.N.N. (2017) 'A survey on enhancing system performance of wireless sensor network by secure assemblage based data delivery', *IEEE International Conference on Recent Advances in Electronics and Communication Technology*, March, pp.289–296.

Kantharaju, H.C. and Murthy, K.N.N. (2017a) 'Enhancing energy efficiency of cluster wireless sensor networks by secure data transmission', *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 9, No. 17, pp.582–597.

Kantharaju, H.C. and Murthy, K.N.N. (2018b) 'Enhancing performance of WSN by utilising secure QoS based explicit routing', *International Journals of Computer Aided Engineering and Technology*, pp.1–24.

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.637–641.

Li, J., Hou, X., Su, D. and Munyemana, J.D.D. (2017) 'Fuzzy power optimized clustering routing algorithm for wireless sensor networks', *IET Wireless Sensor Systems*, Vol. 7, No. 5, pp.130–137.

Liu, J.K., Baek, J., Zhou, J. and Yang, Y. (2010) 'Efficient online/offline identity based signature for wireless sensor network', *International Journal of Information Security*, Vol. 9, No. 4, pp.287–296.

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.

Mensah, H.N., Boateng, K.O. and Gadze, J.D. (2017) 'Tamper aware authentication framework for wireless sensor networks', *IET Wireless Sensor Systems*, Vol. 7, No. 3, pp.73–81.

Messai, S., Boukerram, A. and Seba, H. (2016) 'Energy efficient data collection in grid based wireless sensor networks using a mobile sink', *IFIP Wireless and Mobile Networking Conference*, pp.1–6.

Mohaisen, A., Nyang, D.H., Maeng, Y.J., Lee, K.H. and Hong, D. (2009) 'Grid based key pre-distribution in wireless sensor networks', *KSII Transactions on Internet and Information Systems*, Vol. 3, No. 2, pp.195–208.

Moon, A.H., Iqbal, U. and Bhat, G.M. (2016) 'Mutual entity authentication protocol based on ECDSA for WSN', *Procedia Computer Science*, Vol. 89, pp.187–192.

Nehra, V. and Sharma, A.K. (2013) 'PEGASIS-E: power efficient gathering in sensor information system extended', *Global Journal of Computer Science and Technology Network, Web and Security*, Vol. 13, No. 15, pp.15–20.

Pandya, N.K., Kathiriya, H.J., KAthiriya, N.H. and Pandya, A.D. (2015) 'Design and simulation of advance MODLEACH for wireless sensor network', *IEEE International Conference on Computer, Communication and Control*, pp.1–6.

Patel, D.K., Patel, M.P. and Patel, K.S. (2011) 'Scalability analysis in wireless sensor network with LEACH routing protocol', *International Conference on Computer and Management*, pp.1–6.

Patle, R.R. and Satao, R. (2015) 'Aggregated identity based signature to transmit data securely and efficiently in clustered WSNs', *International Conference on Computing Communication Control and Automation*, pp.138–142.

Qin, Z., Yuan, C., Wang, Y. and Xiong, H. (2016) 'On the security of two identity based signature based on pairings', *Information Processing Letters*, Vol. 116, No. 6, pp.416–418.

Rossi, F. and Schmid, G. (2015) 'Identity based secure group communications using pairings', *Computer Networks (Science Direct)*, Vol. 89, No. 4, pp.32–43.

Sen, J. (2013) 'Security in wireless sensor networks', in Khan, S., Pathan, A-S.K. and Alrajeh, N.A. (Eds.): *Wireless Sensor Networks: Current Status and Future Trends*, pp.407–460, CRC PressILlc Publishing Corporation.

Sharma, G., Bala, S. and Verma, A.K. (2017) 'PF-IBS: pairing-free identity based digital signature algorithm for wireless sensor networks', *Wireless Personal Communications*, Vol. 97, No. 1, pp.1185–1196.

Sharma, I., Singh, R. and Khurana, M. (2015) 'Comparative study of LEACH, LEACH-C and PEGASIS routing protocols for wireless sensor network', *IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA)*, pp.842–846.

Singh, B. and Kaur, E.S. (2014) 'An improved energy-efficient BBO-based PEGASIS protocol is wireless sensor network', *International Journal of engineering Research and Applications*, Vol. 4, No. 3, pp.470–474.

Song, B. and Zhao, Y. (2017) 'Provably secure identity-based identification and signature schemes from code assumptions', *PLoS ONE*, Vol. 12, No. 8, p.e0182894, pp.1–15.

Tawalbeh, H., Hashish, S., Tawalbeh, L. and Aldairi, A. (2017) 'Security in wireless sensor networks using lightweight cryptography', *Journal of Information Assurance and Security*, Vol. 12, pp.118–123.

Walid, E., Newe, T., O'Connel, E., Fraifer, M., Mathur, A., Toal, D. and Dooly, G. (2017) 'Implementing secure key coordination scheme for line topology wireless sensor networks', *Advances in Security in Computing and Communications*, pp.125–146, Intechopenscience.

Warrier, M.M. and Kumar, A. (2016) 'An energy efficient approach for routing in wireless sensor networks', *Procedia Technology*, Vol. 25, pp.520–527.

Yan, J-F. and Liu, Y-L. (2011) 'Improved LEACH routing protocol for large scale wireless sensor networks routing', *International Conference on Electronics, Communications and Control*, pp.3754–3757.

Yasmin, R., Ritter, E. and Wang, G. (2012) 'An authentication framework for wireless sensor networks using identity based signatures: implementation and evaluation', *IEICE Transactions on Information and Systems*, Vol. E95-D, No. 1, pp.126–133.

Zeng, B., Dong, Y., Li, X. and Gao, L. (2017) 'IHSCR: energy-efficient clustering and routing for wireless sensor networks based on harmony search algorithm', *International Journal of Distributed Sensor Networks*, Vol. 13, No. 11, pp.1–20.

Zhang, Y., Wang, J., Han, D., Wu, H. and Zhou, R. (2017) 'Fuzzy logic based distributed energy efficient clustering algorithm for wireless sensor networks', *Sensors*, Vol. 7, No. 7, pp.1–21.

Zhang, Z., Deng, J. and Jiang, C. (2009) 'ID-based key management strategies of clustering wireless sensor networks', *5th International Conference on Wireless Communications, Networking and Mobile Computing*, pp.1–4.