We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

5,000
Open access books available

125,000
International authors and editors

140M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Chapter

Secure and Energy-Efficient Communication in IoT/CPS

Saad Alharthi, Princy Johnson and Martin Randles

Abstract

Secure and energy efficient routing protocol is fairly an open research despite a plethora of routing protocols has been proposed in the literature. However, most routing protocols specifically designed for resource constrained wireless devices, if not all, follow from the same perspective and almost have reached the maximum improvements. This chapter describes the design of cross-layer secure multi-hop zone routing protocol (MZRP) and a hybrid energy-efficient medium access control (MAC) featuring the benefits from both carrier sense multiple access (CSMA) and time-division multiple access (TDMA). MZRP employs the intelligent artificial neural network (ANN) self-organizing map (SOM) algorithm, which is performed at the coordinator or the base station (BS) to divide the area into multi-level zones. Then cluster heads (CHs) are chosen using k-medoids in each zone. The performance of MZRP is better in terms of energy efficiency compared to dual-hop and HT2HL as it extends the network lifetime using hybrid MAC and the security algorithm employed has less message update.

Keywords: multi-hop zone routing protocol (MZRP), self-organizing map (SOM), aggregation, internet of things (IoT), 6LoWPAN, artificial intelligence (AI), machine learning (ML)

1. Introduction

The architecture of the global network "Internet" will expand drastically to accommodate the connections of billion IP-enabled or non-IP smart wireless devices "things" at the network edge which brings up the era of the Internet of Things (IoT). Depending on the application, the data model can either be simple as small "things" are connected (e.g., wearables, smart home, etc.) or it can be complex as big "things" are connected (e.g., automotive, smart city, etc.). Hence, new architecture and technologies have been developed in the fifth generation (5G) to meet the sky-rocketing growth of the IoT [1].

The non-IP network edge utilizes an IoT architecture supported by IPv6 over low-power wireless personal area networks (6LoWPAN) to achieve seamless integration of different heterogeneous networks which enable the interaction between network edge "things" and the outside world "internet" [2]. A typical 6LoWPAN network consists of few hundreds or even thousands of low-cost and tiny intelligent sensor nodes (SNs) embedded with sensing transducers, microcontroller, and radio transceiver units, and all these units are powered by battery or other source of energy [3].

They form an ad hoc network among themselves and a gateway or 6LoWPAN edge router which acts as a centralized network coordinator or a base station (BS). The BS refers to gateway or 6LoWPAN edge router throughout this chapter. This type of network is known as wireless sensor network (WSN), which forms the major hardware devices of the IoT. Different WSNs can be seamlessly connected by routers to provide tunnels to the backbone [4].

The SNs in many applications have no fixed power source. Hence, they are powered by batteries where the replacement either be infeasible or might not be possible. The WSN's lifetime depends on the lifetime of batteries that operate the SNs. Thus, energy saving is the most important factor in designing WSNs, which mandates the necessity for energy efficient techniques to prolong the network lifetime of WSNs [5].

The WSN's lifetime maximization and the individual SN's energy conservation have been investigated by researchers, and several approaches have been proposed in the literature. The overall energy consumption in the SNs is due to sensing, processing, and communication. But radio transceiver has the highest energy expenditure, which involves transmit, receive, idle, and sleep modes. The energy consumption in sleep mode or low power listening (LPL) is very small; hence, the radio transceivers of SNs can be put in sleep mode, which can significantly increase the network lifetime as will be shown later.

This is governed by the performance of the protocols built across all layers of the open systems interconnection (OSI) protocol stack especially routing and medium access control (MAC) protocols within the SNs. Hence, routing and MAC protocols have critical impact on the network lifetime of WSNs. Therefore, careful design of energy efficient routing and MAC protocols is critical to conserve the wasteful energy and to utilize the useful energy wisely.

In a single-hop scenario, SNs can either send or receive messages to/from destination directly if they are within the transmission ranges of each other. If they are far away, i.e., the distance between a SN and a destination is more than the transmission range, and indirect communication using multi-hop is chosen where the message is relayed by several intermediate relays from a SN to a destination.

A simple approach is flooding where a SN sends a query packet for route discovery which propagates over the network until destination is reached. However, this results in broadcast storm due to the propagation of message even after route has been discovered. Thus, it is not suitable for energy constrained SNs as the energy consumption is hug. Data fusion employing passive clustering is another approach to achieve energy savings by processing data in network using machine learning and artificial intelligence (ML/AI) algorithms. It is an intuitive that the traffic and the energy consumption will be reduced significantly.

Hierarchical clustering has been proven to be an effective method for energy optimization in which SNs are organized into clusters. Each cluster has a cluster head (CH), which aggregates the data from cluster member nodes (MNs), and the CHs communicate directly to the BS using single-hop routing or relay the data through intermediate nodes using multi-hop routing. This combines the proactive approach within cluster (intra-cluster) and reactive approach across clusters (inter-cluster).

In battery-powered SNs, the design of low duty-cycle MAC protocol is crucial for energy savings. Most wireless technologies uses CSMA as channel access mechanism. Thus, the MAC layer of a SN is based on the IEEE 802.15.4 standard which defines the specifications of the lowest two layers of the OSI protocol stack; that is, the physical (PHY) and MAC layers. The PHY layer of the IoT protocol stack is based on the IEEE 802.15.4 standard; however, MAC layer is time-slotted channel hopping (TSCH) based on IEEE 802.15.4e standard to ensure high robust and reliable requirements in industrial applications [6]. Hence, these intelligent wireless

devices provide the backbone infrastructure for cyber-physical system (CPS) to monitor physical processes [1].

The distribution of SNs at different places and trying to connect them via wireless links make WSNs vulnerable to attacks. The types of attacks can be internal or external. External attacks can be prevented using link-layer encryption and authentication using global key (GK). However, internal attacks are difficult to defend since a compromised node inside the network is hard to detect as its identity can be verified using its private key (PK).

Hence, routing and forwarding packets can cause security problems as routing protocols are designed to exchange network topology between SNs to establish routes but not to provide defense against malicious attackers. Security in WSNs is still an open research as many questions remain unanswered. The existing network security approaches are either computationally complex, or resources are not efficiently utilized which makes the core security issue a big challenge under great resource constrained SNs.

The challenge is to design energy efficient routing and MAC protocols to prolong the network lifetime of WSNs and considers aspects related to security and data mining using artificial intelligence (AI) and machine learning (ML) algorithms under resource constraints. Thus, a careful design of routing and MAC protocols is required to enhance the data collection, improve security, and increase the lifetime of WSNs in thing-fog-cloud IoT architecture [6].

Our contribution is the design of a cross-layer secure multi-hop zone-based routing protocol (MZRP) and a hybrid energy-efficient MAC called X-SREM. MZRP is a hierarchical clustering routing and hybrid MAC which switches CSMA and TDMA based on data traffic. Low-duty cycle operation is achieved using cooperative strategies by shutting down the radio transceivers of SNs all times except during their assigned time slot. This novel design is useful to potentially achieve security and huge energy savings by eliminating the interference among densely deployed SNs and collision-free data transmission within clusters and reduces the traffic over the network by removing redundancy using data fusion algorithms.

The remainder of this chapter is organized as follows: Section 2 presents the related work. In Section 3, the problem is described. In Section 4, the models are defined. Section 5 describes our proposed cross-layer MZRP and hybrid MAC protocol. Section 6 presents the performance evaluation and analysis of the proposed protocol compared to two benchmark heterogeneous protocols dual-hop and HT2HL. The conclusion of this research is presented in Section 7.

2. Related work

Hierarchical clustering routing and low duty cycle MAC protocols have been proven methods to reduce the energy consumption of SNs and to eliminate the interference among them. Heinzelman et al. [7] proposed low energy adaptive clustering hierarchy (LEACH) and LEACH centralized (LEACH-C) [8], and they are the reference routing protocols in homogeneous hierarchical clustering category. LEACH has provided the basis for many later studies.

For instance, threshold sensitive energy efficient sensor network protocol (TEEN) and adaptive TEEN (APTEEN) are proposed in [9, 10], respectively. The election of CHs in these protocols is a random process. TEEN and APTEEN combine the hierarchical and data-centric approaches. Both reduce data transmission by performing data fusion at CHs, hence achieving large energy conservation. Hybrid energy efficient distributed clustering (HEED) was introduced in [11]. In HEED protocol, CHs are elected periodically based on the residual energy of the SNs and

the intra-cluster communication cost which incorporates cluster radius to adjust the transmission power for inter-cluster broadcast. The previous protocols and their variants are classified as homogeneous scheme protocols.

A stable election protocol (SEP) was proposed in [12] and distributed energy-efficient clustering (DEEC) proposed in [13] are the two well-known protocols for heterogeneous WSNs. In SEP and DEEC, the SNs are assumed to have different energy levels and processing power. Both assume m fraction of the total SNs are equipped with a factor α of additional resources compared to the normal SNs. Although both follow the same approach, DEEC considers the residual energy of SNs in the CHs selection process whereas SEP does not. SEP and DEEC and their variants are classified as heterogeneous scheme protocols.

Alharthi and Johnson [14] suggested HT2HL to deal with some drawbacks in LEACH. Abu Shiba et al. [15] proposed CH-LEACH which uses k-means algorithm to select the CHs, and Park et al. [16] proposed an efficient CH selection using k-means to maximize the energy efficiency of WSNs. Abdul Latiff et al. [17] compared the performance of optimization algorithms for clustering in WSN and validated that particle swarm optimization (PSO) achieves better network lifetime. The CHs are responsible to perform data fusion like typical artificial neural network (ANN) as we will discuss later.

The previous protocols and many of their variants [18] and a plethora other in the literature are single-hop hierarchical clustering routing for WSNs. This assumption is not realistic as the sink might not be reachable by all CHs or the network lifetime is drastically reduced as more energy is consumed in long distance. Multi-hop has more advantages and can solve this problem by choosing optimal routes in the tree formed between the leaves (CHs) and the root (BS).

Multi-hop LEACH finds paths using multi-hop approach like two-level LEACH [19] and MR-LEACH. In [20, 21], the authors proposed new routing techniques to minimize the next hop distance which reduces the energy. Al-Sodairi and Ouni [22] proposed EM-LEACH for load balancing and extended lifetime of WSNs. Modified RPL was proposed by Alharthi et al. in [23].

Routing protocols based on intelligent algorithms like ANN, fuzzy logic, PSO, genetic algorithm (GA), etc. have been surveyed in [24] for network lifetime optimization. A review given in **Table 1** is some existing single-hop and multi-hop and intelligent routing for WSNs.

Routing protocol	Clustering	No. of hops	Location aware	Scalability
LEACH	Distributed	Single-hop	No	Low
LEACH-C	Centralized	Single-hop	Yes	Medium
TL-LACH	Distributed	Two-hop	No	High
MR-LEACH	Distributed	Multi-hop	NO	Medium
HT2HL	Distributed	Two-hop	NO	Medium
CH-LEACH	Centralized	Single-hop	Yes	Medium
EM-LEACH	Distributed	Multi-hop	NO	Medium
BAR	Ant colony	Either-hop	Yes	Medium
GA-EECP	GA	Either-hop	Yes	Medium
FCH	Fuzzy logic	Either-hop	Yes	Medium
SIR	ANN	Either-hop	Yes	High

Table 1.
A summary of routing.

3. Problem statement

The design of energy efficient routing and MAC protocols aims to maximize the network lifetime (Tnet). The battery of a SN i will drain out under flow $\mathbf{f} = \{f_{i,j}\}$ in a time (T_i). Hence, the objective is to minimize the total energy consumption Etot. The energy consumption in one cycle is the sum of energy in the active period (E_a) which depends on (e.g., transmit, receive or idle) and the sleep period (E_s). For n number of cycles, the Etot $= \sum_{i=1}^{n} E_a + E_s$.

Most, if not all, previous protocols are based on LEACH and they inherited its drawbacks. Some drawbacks are highlighted in [14] and other important are discussed here. First, though there are enough CHs in some rounds, some rounds have larger, fewer or no CHs are elected. Second, the separation and compactness due to the randomness employed in the election of CHs. Finally, re-clustering consume large amount of energy but it is unnecessarily performed every round resulting in SNs with less remaining energy be elected as CHs after 1/p rounds where p is the percentage of CHs. This lowest energy rout will result in energy depletion of the nodes along the path and may lead to network partitioning [20].

The data aggregation is simple, which aims to reduce the number of messages. Hierarchical routing protocols play significant role to choose the SNs to perform data aggregation by constructing a loop-free spanning-tree. Hence, the latency decreases as the path length is decreased, and the accuracy and energy efficiency are increased. The resilience of aggregation can be improved using hierarchal techniques which provide defense against routing and aggregation attacks.

4. System models

The following section describes the network model for three-tier heterogeneous WSNs and defines the radio energy model which is used to compute the energy dissipated by the SNs.

4.1 Network model

Consider three-tier thing-fog-cloud IoT architecture as shown in **Figure 1** and WSN containing N nodes in tier-0 and fog nodes in tier-1. They are distributed uniformly at random in a 2D grid or a square sensor field (area A = LxL) to monitor the environment as shown in **Figure 1**.

There are two or more types of SNs might exist inside WSNs; i.e., full function devices (FFD), reduced function devices (RFD) and coordinator in Zigbee and Class A, B, and C in LoRA networks. Let S be the set of FFD SNs such that $S = \{S_1, S_2, \ldots, S_i\}$ where S_i denotes the i-th SN, $1 \leq i \leq N$ represents the decimal ID of the SN. A SN can be equipped with one or more same or different types of sensors (e.g., temperature, pressure, etc.). The BS is static and located at the center with no limited energy. The SNs are unaware about their location and fixed after deployment and each has a unique ID as shown in **Figure 2(a)**.

The network in tier-0 can be denoted as a graph G = (V, E), where V is a set of vertices representing the SNs such that |V| = N and E $\subseteq$ V^2 is a set of edges that signify the bidirectional wireless links between a pair of SNs v_i and v_j. Hence, edges $(v_i,v_j) \in$ E if v_i and v_j are neighbors; i.e., the distance between them d (v_i,v_j) is less than the range of each other as shown in **Figure 2(b)**. Thus, E = $\{(v_i,v_j) \in$ V^2 | $v_i \neq v_j \wedge$ d $(v_i,v_j) <$ R$\}$, where R is the communication range. We define $c_{i,j}$ (v_i,v_j) as the cost of energy on the edge between v_i and v_j assuming that the links are symmetric. That is, $c_{i,j}$ $(v_i,v_j) = c_{j,i}$ (v_j,v_i).
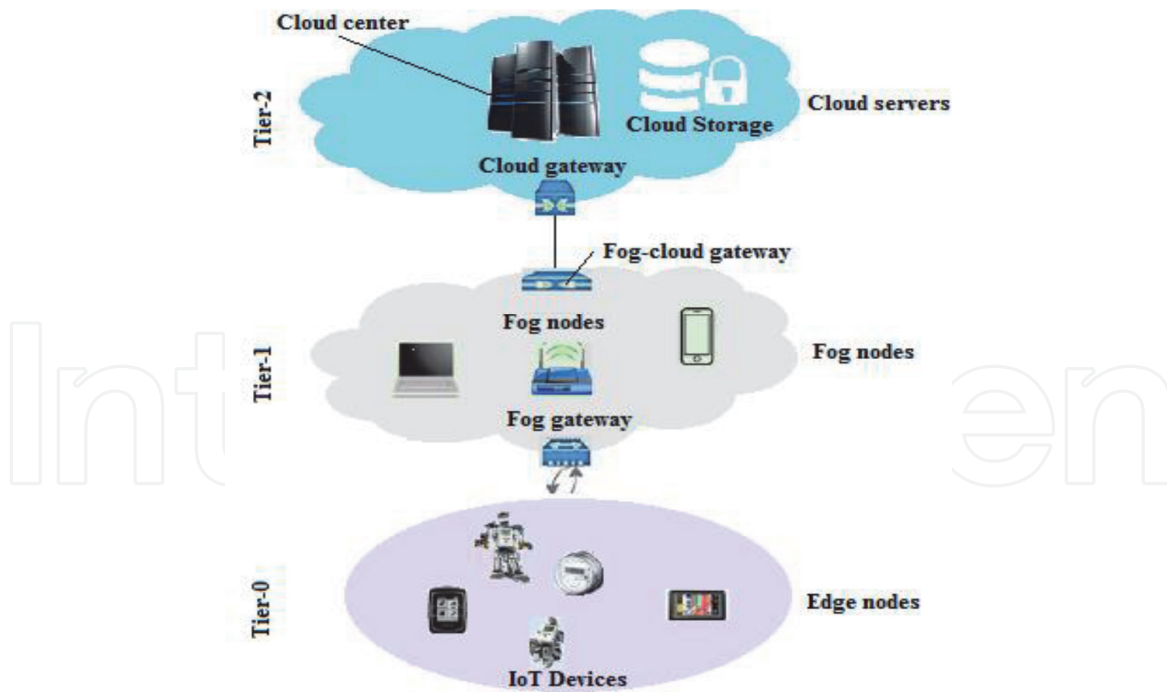
Figure 1.
The three-tier thing-fog-cloud IoT architecture.

(a)   (b)
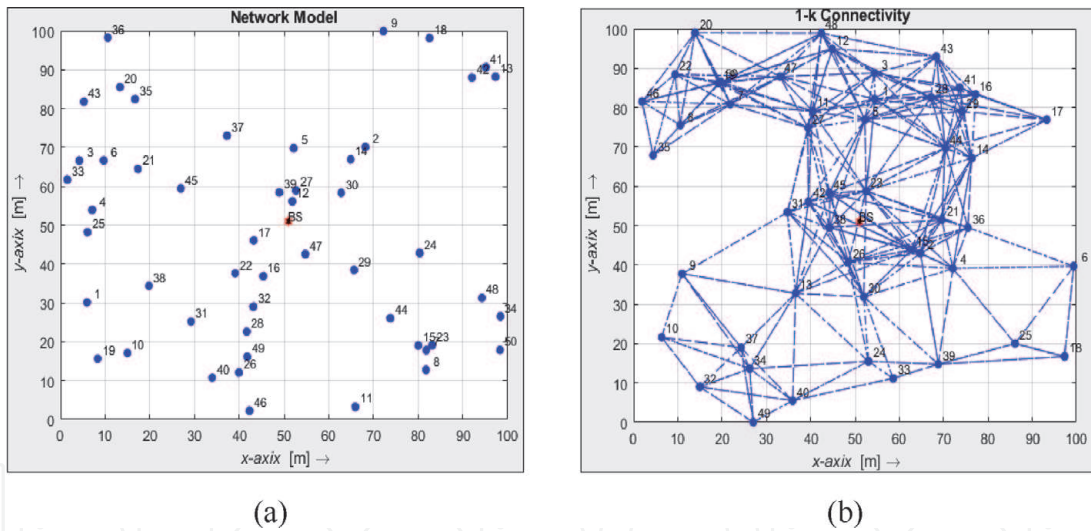
Figure 2.
Network model (a) deployment (b) connectivity.

Let G' = (C, E') be a subgraph, where C is a set of vertices representing the CHs such that |C| = k and E' ⊆ C² is a set of edges that show the bidirectional wireless links between a pair of CHs C_i and C_j. Let $P(v_i, v_j) = (v_i, v_1, ..., v_j)$ is the set of multiple paths in G' from C_i to C_j since other FFD SNs are in sleep mode and neither involve in routing nor act as fog nodes at this moment as shown in **Figure 3**.

4.2 Radio energy model

There are various models for radio energy consumption, though most of the researchers have used the energy model in [8]. The model for communication between SNs is depicted in **Figure 4**.

The energy consumption in the transmitter circuit E_{Tx} (B,d) to transmit B-bit message is given by
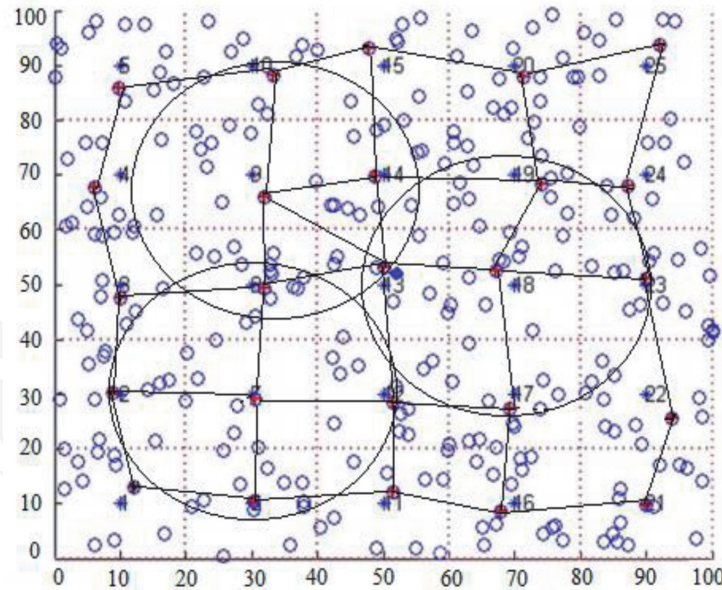
Figure 3.
Connectivity between clusters in multi-path.

$$E_{Tx}(B, d) = E_{elec} * B + \mathcal{E}_{amp} * B \tag{1}$$

The E_{elec} depends on electronic circuits of the transceiver used in digital coding, modulation, demodulation, and other circuits. The $\mathcal{E}_{amp}$ is the energy dissipation in power amplifier, and it depends on power loss (PL) in the channel model used. The PL in free-space and log-distance models can be described using Friis equation as the ratio of the power transmitted to the power received (Pt/Pr) as given below:

$$\frac{P_t}{P_r} = \left[\frac{\sqrt{\lambda G}}{4\pi d}\right]^{\delta} \tag{2}$$

where λ is the wavelength, G is the product of equal gains of transmit and receive antennas, d is the distance between antennas, and δ is the PL exponent which depends on the propagation environment. **Table 2** gives the typical values of δ.

Hence, d^2 is the power loss in free space ($\mathcal{E}_{fs}$) and d^4 is the power loss in two-ray or multipath fading ($\mathcal{E}_{amp}$).

$$\mathcal{E}_{amp} = \begin{cases} \mathcal{E}_{fs} * d^2, & d < d_o free - space \\ \mathcal{E}_{mp} * d^4, & d \geq d_o multi - path \end{cases} \tag{3}$$

$$do = \sqrt{\frac{\mathcal{E}fs}{\mathcal{E}mp}} \tag{4}$$

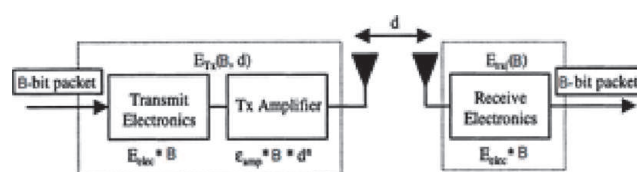The values of $\mathcal{E}_{fs}$ = 10pJ/bit/m^2 and $\mathcal{E}_{amp}$ = 13fJ/bit/m^4.

Figure 4.
The radio energy consumption model.

Propagation environment	Value of δ
Free-space	2
Urban area LOS	2.7–3
Urban area no LOS	3–5
Indoor LOS	1.6–1.8
Buildings no LOS	4–6

Table 2.
Typical values of δ.

The energy dissipated for receiving B-bit message E_{Rx} (B) is given by

$$E_{Rx}\,(B) = E_{elec} * B \tag{5}$$

The E_{elec} by transmitter and receiver circuits are equal and can be set to 50 nJ/bit. The CH and its MNs can communicate provided that the received power will be greater than the sensitivity of the receiver.

The process of data aggregation is same as the concept of feed-forward multi-layer perceptron (MLP) in ANN or fuzzy logic as depicted in **Figure 5**.

The set of input data xi (x1, x2, … , x_n) are measured by groups of SNs xi in each cluster. The CHs aggregate the data from inputs xi using quantization techniques to process the input data locally, which results in quantized data (q1, q2, … , qn) before sending them to the fusion center. A weight value wi is assigned to each SN and a bias bk as described in Eq. (5).

$$y_i = f(\mathbf{x}, \mathrm{t}) = f\left(\sum_{j=1}^{i} w_{kj}\boldsymbol{x}_j + b_k\right) \tag{6}$$

The energy consumption due to data aggregation (E_{DA}) is 5pJ/bit.

The CHs can perform sensing (e.g., temperature, pressure, etc.) and compare the readings with data aggregated from other SNs. The sensed signal is analog which will be converted to binary of size D bits using analog-to-digital converter (ADC). If the readings from the SNs fall in the interval $[-M, M]$, their readings will be aggregated, compressed, and sent to upper level CHs or zone gateways which have lower variance (i.e., Da [Da1, Da2] where Da1 ≥ -D and Da2 < D). However, they are identified as outliers since the readings do not match the aggregated confidence interval [Da1, Da2].

The aggregated data are compressed into a single fixed-length packet by applying some sort of transforms on the source bit like discrete wavelet transform (DWT) and discrete cosine transform which achieve signal-to-noise-ratio (SNR) of 20 dB or better to reduce the number of transmitted bits. Relay nodes do not aggregate data as it has less correlation.
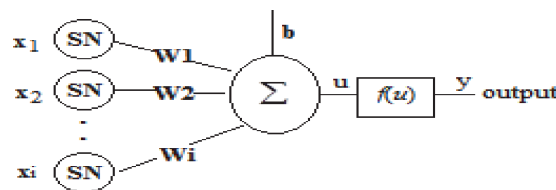

Figure 5.
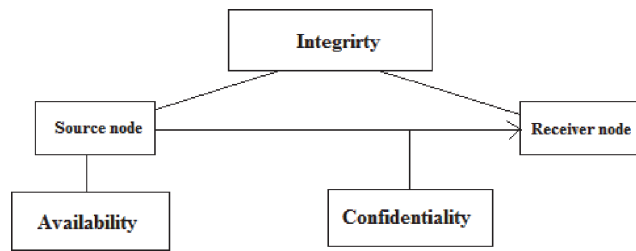*Data aggregation process in AI model.*

Figure 6.
The attacks on CIA model.

4.3 Security model

Wireless links are susceptible to passive eavesdropping or active impersonation in which the former violates confidentiality by eavesdropping exchanged messages without being detected while later try to inject erroneous messages, drop packets or change routing information.

Symmetric cryptography or group key management is common security scheme for WSNs. Each SNs including the sink needs pairwise cryptographic keys for authentication. The global keys (GKs) are shared among SNs in the network; however, private keys (PKs) are shared between the sink and individual SNs only.

To build the security mechanism, confidentiality, integrity, and availability (CIA) triad model with passive attacks is assumed as shown in **Figure 6.**

5. Proposed protocol

The proposed cross-layer secure MZRP and a hybrid energy-efficient MAC (X-SREM) have three phases: intelligent network configuration phase (INCP), the clustering and rotation of CHs phase (CRCP), and the steady-state phase (SSP). MZRP is a hybrid protocol which divides the sensing field into multi-level hierarchy to solve the minimum transmit power topology control problem faced in multi-hop wireless network. Each level is divided into zones using self-organizing map (SOM) neural network, and zones are further divided into regions which are composed of a group of clusters led by cluster heads (CHs). The BS calculates the proximity of all SNs and those that can communicate directly with the BS will be assigned zone-0 identifier and serve as border gateways (BG); and the CHs in zone-1 forward their data directly to the zone-0 gateways. The CHs in the lower level zones choose the least cost multi-hop paths to forward their data to the BS using multihop.

5.1 Intelligent network configuration phase (INCP)

The initial phase is the network configuration that begins with "hello" message from the BS with the TDMA schedule to all SNs to advertise themselves. Based on the distance, the neural network clustering using SOM is performed in the BS. The input layer of the neural network is the three-element vectors (3×100 matrix) which define the x- and y-coordinates of the SNs and the distance to the BS. The SOM layer is 1-by-10 hidden layers of neurons to classify SNs to zone in a 2D-grid as illustrated in **Figure 7** and described in Algorithm 1.
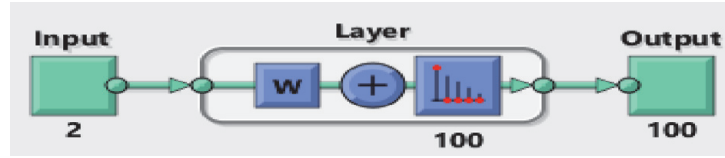
Figure 7.
Self organizing map network diagram.

ALGORITHM 1: INCP to create zones.

Input: N, number of sensors; Z, number of zones; S(x,y), locations of sensors in 2D plane; d, distance to the BS

Output: the zone ID
function Zone (N)
// Perform (SOM) to partition the field into zones using Selforgmap
1: idx (Z)←Selforgmap (x,y,d)
//Assign zone ID to each node
2: **for** each node Nj where j = 1, 2,.., N
3:     S(j).zone ← idx(j)
4: **end**
5: return (Zone)
6: **end** function

5.2 Clustering and rotation of CH phase (CRCP)

Once SNs are assigned to zones, the BS runs ML algorithm (e.g., k-medoids) to determine k CHs in each zone that minimizes the cost function described in [17].

$$\text{cost} = \beta \times f1 + (1 - \beta) \times f2 \tag{7}$$

$$f1 = \max_{i=1,2,..k} \sum_{\forall n_i \epsilon C_k} d(n_i, C_k)/|C_k| \tag{8}$$

$$f2 = \sum_{i=1}^{N} E(n_i) / \sum_{j=1}^{k} E(C_k) \tag{9}$$

The BS broadcasts "hello" message again to all SNs which includes information of the elected CHs. Once the CHs are selected, the clusters are fixed for the entire network lifetime and members are sorted in a list to become CHs based on the distance from the BS if the energy level of CHs fall below a threshold value defined as f2/k. The zones created around the BS based on the distance using SOM and CHs using k-medoids are shown in **Figure 8(a)** and data aggregation in **Figure 8(b)**.

5.3 Steady-state phase (SSP)

The SSP breaks the data transmission into frames using hybrid TDMA/CSMA where member nodes (MNs) send the data to their CHs in the time slots allocated to them. Hence, SNs have periodic sleep with duty-cycle equals $T_A/(T_A + T_S)$ where T_A and T_S are the active and sleep time, respectively. This is repeated periodically to save SN's energy.

The CHs aggregate the data and send them to the BS or ZG using carrier sense multiple access (CSMA) and fixed spreading codes. Based on traffic, CHs switch between TDMA and CSMA to transmit the data. For instance, when the energy
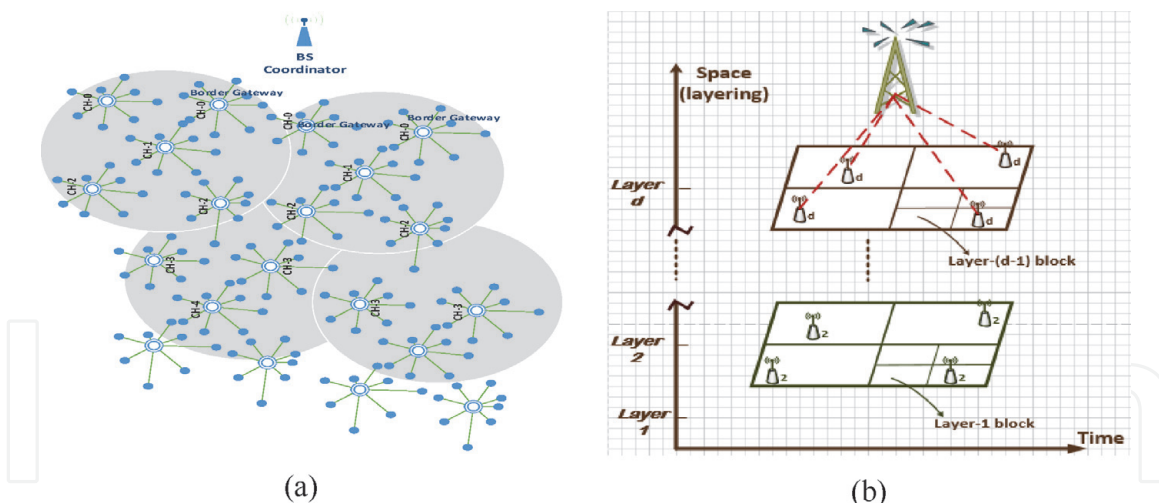
Figure 8.
Zone formation (a) network topology (b) data aggregation.

threshold is reached, the SNs with highest energy will be elected as CHs and this process continues to manage the routing using the AI algorithm in entirely distributed fashion. The round structure is shown in **Figure 9**.

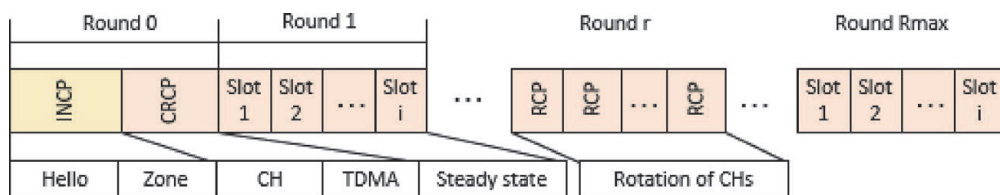The flow chart of MZRP is shown in **Figure 10**.

Figure 9.
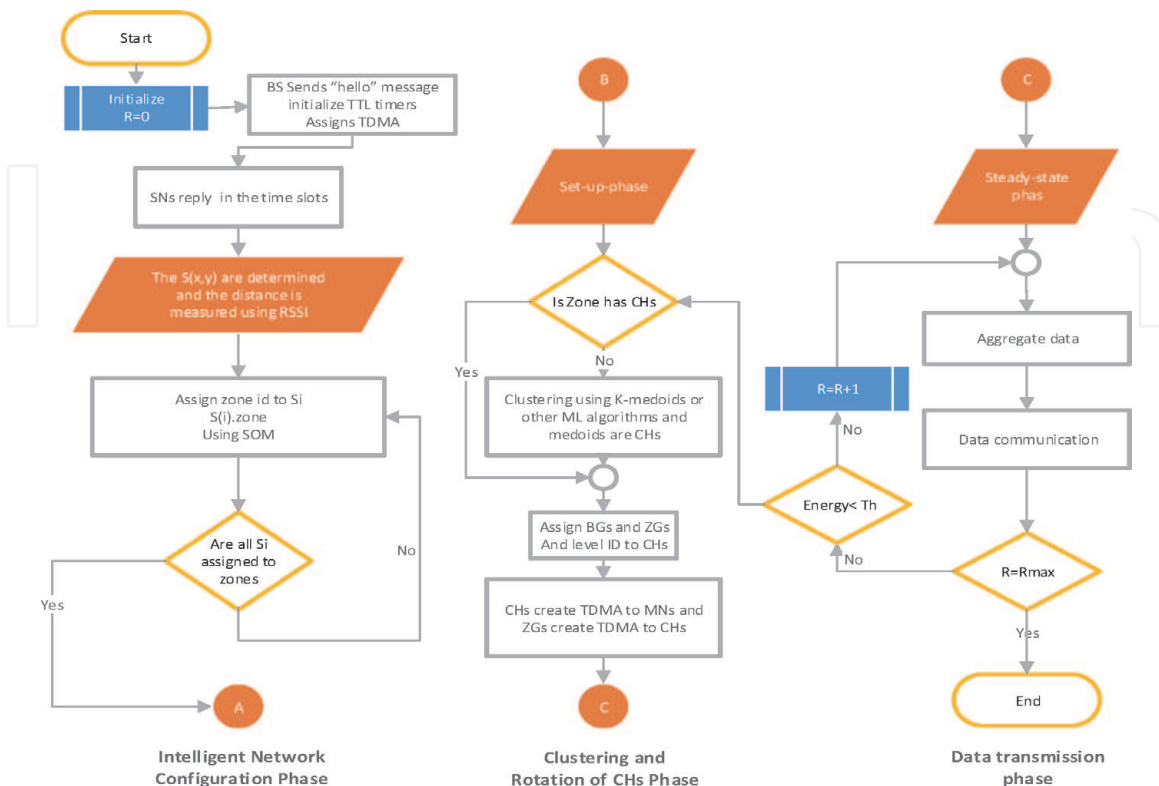*Round structure in MZRP network model (a) deployment (b) connectivity.*

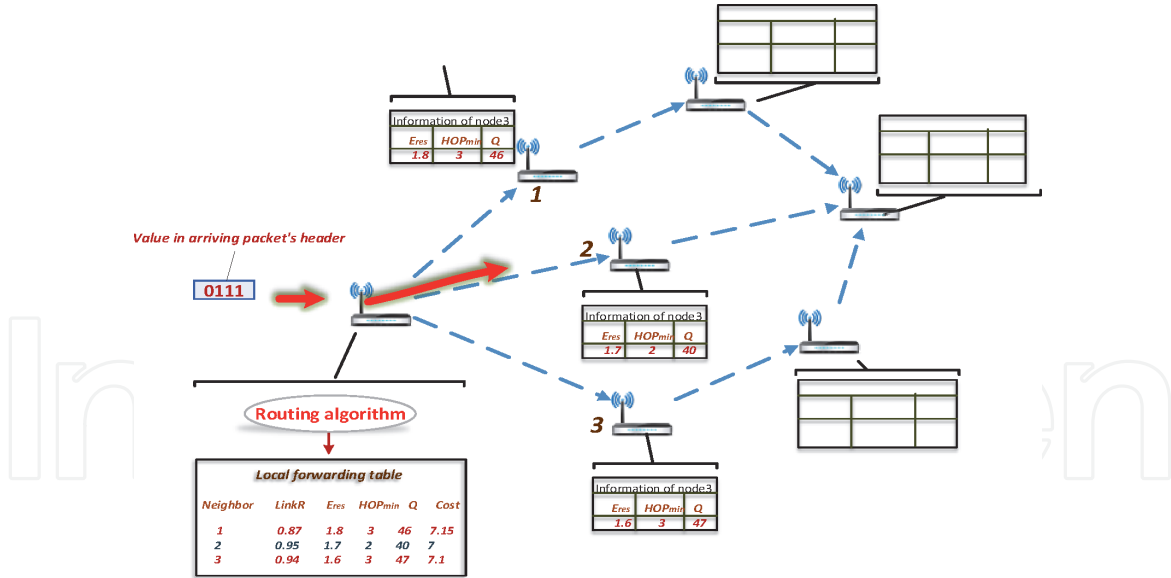

Figure 10.
Three phase of MZRP.

Figure 11.
Route selection in inter-CHs for each zone.

A single-hop inter-cluster communication happens between the MNs and their CHs and between CHs and BS as well if the distance between the BS and the CHs is less than their communication range, otherwise data are relayed from lower-level CHs through intermediate CHs at upper levels until it reaches the sink using multi-hop with minimum cost based on zone ID, remaining energy and link quality with minimum hop-count as shown in **Figure 11**.

The cost of a link (i,j) is given by

$$c_{i,j} = e \times \frac{E_{res,j}}{E_{init,j}} + q \times \frac{Q_{empt,j}}{Q_{init,j}} + l \times R_{i,j} \qquad (10)$$

where E_{res} is the initial energy E_{init} minus the energy consumption $(E_{Tx} + E_{Rx} + E_{DA})$ defined before and e, q, and l are constants. The route selection is described in Algorithm 2.

ALGORITHM 2: Optimal next-hop route

Require: ni, CH neighbors; ZID, zone IDs; HOP, hop count; Eres, remaining energy; R, link quality, Q, queue

Ensure: NH, next-hop ID
1: **while** (the zone ID of $n_i \leq$ zone ID of CH)
2: **repeat**
//calculate the link $c_{i,j}$ for all neighbors of CHs
3: **for** all $j \in n_i$ do
4:    $c_{i,j} \leftarrow$ use eq (10)
5: if $E_{res,j} - c_{i,j} < E_{thr,j}$
6:    rotate the CHs
7: end if
8: **endfor**
9: **endwhile**
//list of ni is created
10: j← top of the list
11: **while** (not end of the list ni)

12:    if (HOP next element equals HOP of the CH) then
13:      add j to ni
11:    end if
14: j← next element in the list
15: **endwhile**
16: sort n_i according to $c_{i,j}$ in descending order NH
17: NH← top of the list n_i

Now, logical key tree is produced using topology key hierarchy (TKH) algorithm [25] based on the model shown in **Figure 12**. The algorithm is described below.

The total number of messages in d degree key tree is $\sum_i^{h-1}(di - 1) - 1$ [26].

The total cost of key update is sum of cost of revoked subtree (RS) (tree$_i$) plus the sum of cost of subtrees $\notin$ RS given by

$$c_{tot} = \sum_{treei \epsilon RS} Ctree_i + \sum_{treei \notin RS} Ctree_j \qquad (11)$$

ALGORITHM 3: Secure routing and aggregation in MZRP

Require: network topology

Ensure: key tree

Function keytree (G, V_m)
  for each tree **do** {
    if (|tree$_i$| = 1) // the BGs
    {attach the root$_i$'s PK to the GK}
    elseif (|tree$_i$| ≥ 2)
    {generate ZG key (TK) and attach the root$_i$'s PK to the GK}
    current_parent← root$_i$
     for each non-leaf node in tree$_i$ **do** {
      set {sibling set} ← children of current_parent
      if (CH set = 1)
      {attach the sibling's PK to the ZG key (TK$_i$}
       elseif (|sibling set | ≥ 2)
      {generate the CH key SK (Sibling Key) and attach it to the TK$_i$, attach all PKs to the SK}
      current_parent← unvisited non-leaf node in tree$_i$
      endif
     endfor
    endif
  endfor return keytree

end function

The model in **Figure 12** is a novel mechanism for security in WSNs to defend against aggregation and routing attacks. The subtrees are rooted at T1, T2, and T3 or BGs.

The sink uses a public function F to generate a key chain K_i where $K_i = F(K_i + 1)$. Each SN had stored an initial key K_0 before its deployment where $K_0 = F_n(K)$. Hence, the sink's first message will be encrypted using $K_1 = F_{n-1}(K)$ and transmitted. Once they have been received by all SNs, the sink reveals K_1 and each SN computes $F(K_1) = F(F_{n-1}(K))$ to validate this matching its initial key (i.e., K_0). Similarly, the consecutive keys can be revealed until $K_n = K$ is reached.

Further processing on the sensed data and when decision has to be made, fog nodes have data base storage to store the data generated temporarily and perform AI/ML to make decision on what to do next and send commands to the BS to
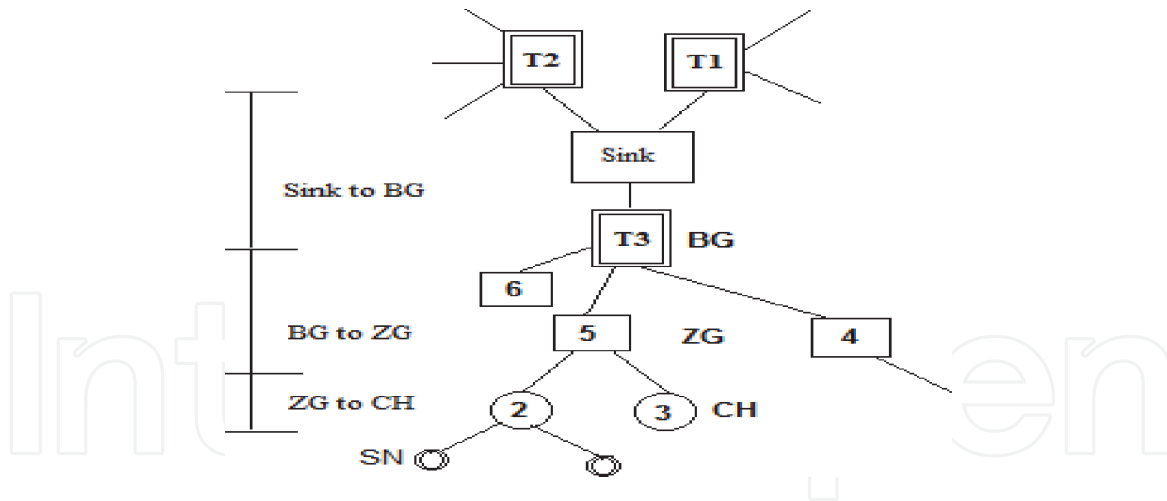
Figure 12.
Secure multicast routing and data aggregation.

instruct it what action needs to be taken. The big data will be sent to the cloud for storage and higher power computation. **Figure 13** illustrates the relationship between IoT, AI/ML and Big data.
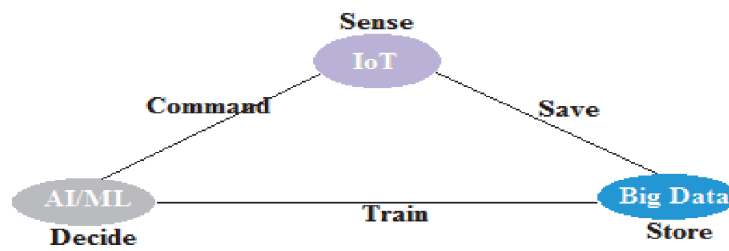

Figure 13.
The IoT, AI/ML and big data relationship.

6. Simulation

MATLAB R2019a is used to evaluate the proposed cross-layer MZRP and a hybrid MAC protocol based on the model described in Section 4.1. The BS performs SOM to create the zones and k-medoids to elect CHs. Other simulation parameters are listed below.

Description	Parameter	Value
Energy in electronics	E_{elec}	50 nJ/bit
Energy of path loss parameters	$\mathscr{E}_{fs,adj}$	10pJ/bit/m^2
	$\mathscr{E}_{mp}$	0.0013pJ/bit/m^4
Initial energy	E_0	0.5 J
Data aggregation	E_{DA}	5nJ/bit/signal
Message size	B	4000 bits
Optimal probability	P_{opt}	0.05

The average remaining energy in MZRP is higher compared to dual-hop and HT2HL as shown in **Figure 14(a)**.
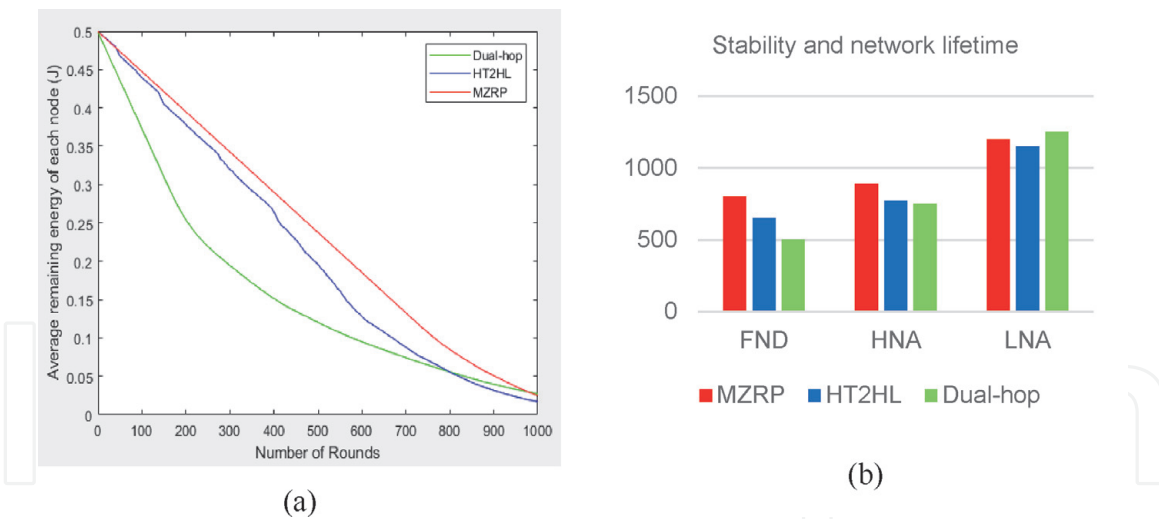
Figure 14.
The average remaining energy (a) and network lifetime (b).

The simulation of MZRP, dual-hop, and HT2HL are repeated, and the average values for the deaths of first node, half nodes, and last node (FND, HND and LND) are shown in the histogram of **Figure 14(b)**. Obviously, MZRP outperforms dual-hop and HT2HL in terms of network lifetime. Hence, it is more energy efficient.

The MAC protocol is responsible for active/sleep schedule. The average power consumption of a SN can be approximated by the following expression:

$$P_{avg} = \left[\frac{T_A \times I_A}{T_{cycle}} + I_S\right].V \qquad (12)$$

where T_{cycle} is the cycle period (i.e., $T_A + T_S$), I_S is the current drawn in the sleep mode, and V is the battery voltage [27].

Figure 15(a) compares the remaining energy in CSMA and TDMA for different numbers of SNs accessing the channel. TDMA is better when the number of SNs is increased as it offers collision free media. Hence, SNs transmit in the time slot and turn their transceivers off. Thus, SNs have less active time in TDMA compared to CSMA as shown in **Figure 15(b)**.

The TKH cryptographic algorithm [25] is used in the MZRP, and the key management is static (i.e., no update) since re-clustering does not happen until the threshold value of the energy of CHs are reached. As the topology will have changed as new CHs are elected, the keys will be updated. Hence, dynamic key management
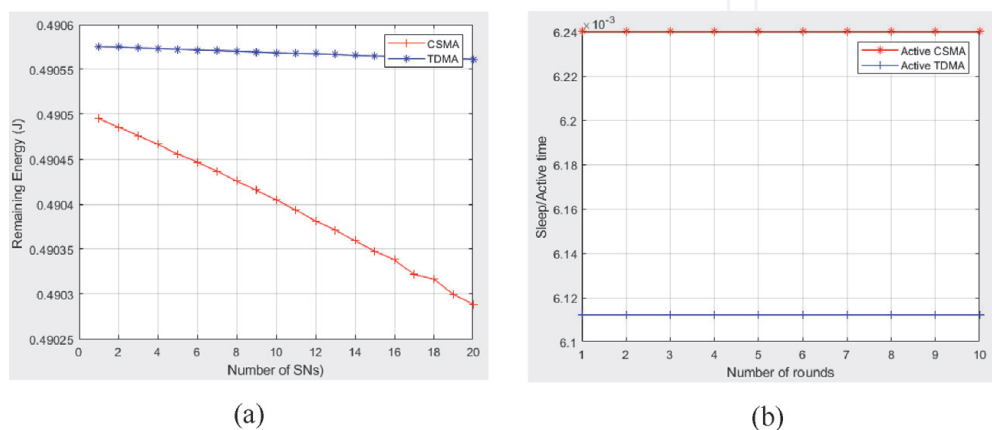

Figure 15.
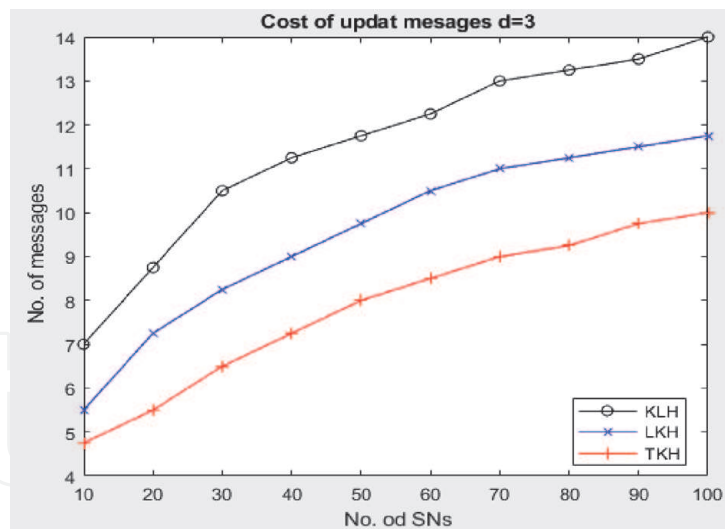*Performance comparison (CSMA/TDMA).*

Figure 16.
Comparison of key management algorithms.

is required. The TKH algorithm has low cost compared to logical key hierarchy (LKH) and key link tree (KLT) [26] as shown in **Figure 16**.

Clearly, the TKH has the least key update messages; hence, energy consumption of SNs using TKH is less.

7. Conclusion

The cross-layer energy efficient multi-hop zone-based routing MZRP and hybrid MAC (X-SREM) is proposed in this paper. The AI/ML are at the heart of our design where SOM is used to divide the area into zones and k-medoids algorithm is used for clustering and ANN is used to aggregate data by CHs. MZRP protocol extends the network lifetime; hence, its performance of is better than dual-hop and HT2HL. The load balancing is achieved through rotation of CHs within clusters when the threshold value of the energy level is 50% of the initial energy since this has been tested to be the optimum threshold for reclustering. The fog nodes provide data analytics near the network edge and relay big data to cloud for further processing and storage. Enhanced lifetime is our future work to improve MZRP.

Author details

Saad Alharthi[1*], Princy Johnson[1] and Martin Randles[2]

1 Department of Electronics and Electrical Engineering, Liverpool John Moores University, Liverpool, UK

2 Department of Mathematics and Computer Science, Liverpool John Moores University, Liverpool, UK

*Address all correspondence to: ieeeeng@yahoo.com

IntechOpen

References

[1] Alharthi S et al. IoT/CPS ecosystem for efficient electricity consumption. In: Tenth International Green and Sustainable Computing Conference (IGSC), Alexandria, VA, USA. 2019. pp. 1-7

[2] Gupta A, JHA RK. A survey of 5G networks: Architecture and emerging technologies. IEEE Access. 2015;**3**: 1206-1232

[3] Mouradian C et al. A comprehensive survey fog computing: State-of-the-art and research challenges. IEEE Communication Surveys and Tutorials. 2018;**20**(1):416-464

[4] Whitmore A, Agarwal A, Da Xu L. The internet of things: A survey of topics and trends. Information Systems Frontiers. 2015;**17**:261-274

[5] Zhou F et al. Energy-efficient NOMA heterogeneous cloud radio access networks: Enabling techniques and challenges. IEEE Network. 2018;**32**(2): 152-160

[6] Taneja M, Davy A. Resource aware placement of data analytics platform in fog computing. Procedia Computer Science. 2016;**97**:153-156

[7] Heinzelman W, Chandrakasan A, Balakrishnan H. Energyefficient Communication Protocol for Wireless Microsensor Networks. Maui, HI, USA: Proceedings of the IEEE Hawaii International Conference on System Sciences; 2000. pp. 1-10

[8] Heinzelman W, Chandrakasan A, Balakrishnan H. An application specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications. 2002;**1**(4):660-670

[9] Manjeshwar A, Agrawal DP. TEEN: A protocol for enhanced efficiency in wireless sensor networks. In: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing. San Francisco, USA; 2001

[10] Manjeshwar A, Agrawal DP. APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireles sensor networks. In: Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing. San Francisco, USA; 2002

[11] Younis O, Fahmy S. HEED: A hybrid, energy- efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing. 2004;**3**(4):366-379

[12] Smaragdakis G, Matta I, Bestavros A. SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. In: 2nd International Workshop on Sensor and Actor Network Protocols and Applications (SANPA 2004). 2004. pp. 1-11

[13] Qing L, Zhu Q, Wang M. Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Computer Communications. 2006;**29**:2230-2237

[14] Alharthi SA, Johnson PA. Threshold sensitive heterogeneous LEACH protocol for wireless sensor networks. In: 24th Telecommunications Forum (TELFOR). Belgrade; 2016. pp. 1-4

[15] Abushiba W, Johnson P, Alharthi S, Wright C. An energy efficient and adaptive clustering for wireless sensor network (CH-leach) using leach protocol. In: 13th International Computer Engineering Conference (ICENCO). Cairo; 2017. pp. 50-54

[16] Rekha PA. Energy efficient of inter cluster multihop routing protocol for wireless sensor network. In: International Conference on Interactive and Advanced Communication Technology (ICIACT2016). 2016. pp. 1-8

[17] Latiff NA, Tsimenidis C, Sharif B. Performance comparison of optimization algorithms for clustering in wireless sensor networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems. Pisa; 2007. pp. 1-4

[18] Palan NG, Barbadekar BV, Patil S. Low energy adaptive clustering hierarchy (LEACH) protocol: A retrospective analysis. In: International Conference on Inventive Systems and Control (ICISC), Coimbatore. 2017. pp. 1-12

[19] Loscri V, Morabito G, Marano S. A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). In: VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference. Dallas, TX, USA; 2005. pp. 1809-1813

[20] Kumar S et al. Resource efficient clustering and next hop knowledge based routing in multiple heterogeneous wireless sensor networks. International Journal of Grid and High Performance Computing (IJGHPC). 2017;**9**(2):1-20

[21] Khurnan S, Rekha KA. Energy efficient of inter cluster multihop routing protocol for wireless sensor network. In: International Conference on Interactive and Advanced Communication Technology (ICIACT2016). 2016. pp. 1-8

[22] Al-Sodairi S, Ouni R. Reliable and energy-efficient multi-hop LEACH-based clustering protocol for wireless sensor networks. Sustainable Computing: Informatics and Systems. 2018;**20**:1-13

[23] Alharthi SA, Johnson P, Alharthi MA. IoT architecture and routing for MV and LV smart grid. In: Saudi Arabia Smart Grid (SASG). Jeddah; 2017. pp. 1-6

[24] Guo W, Zhang W. A survey on intelligent routing protocols in wireless sensor networks. Journal of Network and Computer Applications. 2014;**38**: 185-201

[25] Son J, Lee J, Seo S. Energy efficient group key management scheme for wireless sensor networks. In: 2nd International Conference on Communication Systems Software and Middleware. Bangalore; 2007. pp. 1-9

[26] Li G, Wang Y, He J. Efficient group key management scheme in wireless sensor networks. In: Third International Symposium on Intelligent Information Technology and Security Informatics. Jinggangshan; 2010. pp. 411-415

[27] López M et al. Software management of power consumption in WSN based on duty cycle algorithms. In: Eurocon. Zagreb; 2013. pp. 399-406