Computers, Materials & Continua
DOI:10.32604/cmc.2022.023478
Research Article

Tech Science Press

An Experimental Simulation of Addressing Auto-Configuration Issues for Wireless Sensor Networks

Idrees Sarhan Kocher*

Energy Engineering Department, Duhok Polytechnic University, Duhok, 42001, Kurdistan Region, Iraq
*Corresponding Author: Idrees Sarhan Kocher. Email: idrees.hussein@dpu.edu.krd

Received: 09 September 2021; Accepted: 15 October 2021

Abstract: Applications of Wireless Sensor devices are widely used by various monitoring sections such as environmental monitoring, industrial sensing, habitat modeling, healthcare and enemy movement detection systems. Researchers were found that 16 bytes packet size (payload) requires Media Access Control (MAC) and globally unique network addresses overheads as more as the payload itself which is not reasonable in most situations. The approach of using a unique address isn't preferable for most Wireless Sensor Networks (WSNs) applications as well. Based on the mentioned drawbacks, the current work aims to fill the existing gap in the field area by providing two strategies. First, name/address solutions that assign unique addresses locally to clustered topology-based sensor devices, reutilized in a spatial manner, and reduce name/address size by a noticeable amount of 2.9 based on conducted simulation test. Second, name/address solutions that assign reutilizing of names/addresses to location-unaware spanning-tree topology in an event-driven WSNs case (that is providing minimal low latencies and delivering addressing packet in an efficient manner). Also, to decline the approach of needing both addresses (MAC and network) separately, it discloses how in a spatial manner to reutilize locally unique sensor device name approach and could be utilized in both contexts and providing an energy-efficient protocol for location unawareness clustered based WSNs. In comparison, an experimental simulation test performed and given the addresses solution with less overhead in the header and 62 percent fair payload efficiency that outperforms 34 percent less effective globally unique addresses. Furthermore, the proposed work provides addresses uniqueness for network-level without using network-wide Duplicate Address Detection (DAD) algorithm. Consequently, the current study provides a roadmap for addressing/naming scheme to help researchers in this field of study. In general, some assumptions were taken during the work phases of this study such as number of Cluster Head (CH) nodes is 6% of entire sensor nodes, location unawareness for entire sensor network and 4 bits per node address space which considered as the limitation of the study.

Keywords: Addressing\Naming; MAC address; global address; locally unique address; tree spanning; clustering; duplicate address detection (DAD)

1 Introduction

To design reliable and efficient information and communication system, Sensor Devices play a great role as an information gathering technique WSNs. The new studies in wireless communication field, have made the sensing devices with Signal Processing (SP) in one low cost integrated chip [1–5]. Sensor devices composed of small memory, multi-functional sensing hardware, small power battery, limited processor capabilities, and short radio communications range [6]. WSNs get applications in various fields such as environmental monitoring, industrial sensing, habitat modeling, emergency (first) response situations, and battlefield control awareness and diagnosis of machinery [7,8].

The environmental implementation for both WSNs and Internet is completely different. The WSN environment adds some extra unique challenges to researches in this field. The topology deployment of WSN in linear\grid application isn't common. In ad hoc deployment, sensor devices must handle with the process of distribution and then finding he next hopes for routing the underlying packet to BS sensor device within entire WSN. After the sensor devices are deployed, they worked in an unattended manner Moreover, the nature of deployment environments for sensor devices are dynamic and hostile [9].

The energy constrained aspect in WSNs is well known and very common in the field of WSN. Thus, sensor device is considered as dead node when the power of battery power is no longer enough to achieve specific tasks of WSN [10]. Therefore, to elongate the lifetime of entire WSN, the need arises to implement the optimized algorithm for energy conservation purpose. The energy efficiency factor was regarded as one of the most significant challenge in designing of WSNs [11]. The WSNs differ than the distributed systems, as the packet size and collected data rate are tiny, almost 16 bytes for each packet [12]. Due to limited energy and small rates of collected data in WSNs, the overheads of implementing global unique name\address approach are not preferable for most applications.

Address\Name means to identify a sensor device in any case of MAC\network level address. The required size of globally unique address is between 16 to 32 bits, this size is depending on the entire network size. After deployment of WSN, sensor devices in various clusters may hold similar name/address simultaneously without any interrupt in the functionality of the algorithm. The spatially reutilized locally unique names in spatial manner achieve the function with lower addresses size than global addresses size. In WSNs, every transmitted bit limits and consumes energy that leads to reduce the entire network lifecycle, thus reducing the size of name/address elongates the entire network lifetime.

In general, the current study concentrates on the both Cluster based topology [11,13] and Spanning Tree topologies [14,15].

1.1 Clustering Based Algorithms

This study will introduce and focus on clustering based topology in Section 4. In local clustered based WSNs, one sensor node is assigned as the Cluster Head (CH) device. This type outperforms multi hop scenarios, because of making efficient local coordination within entire sensor devices in WSNs [16]. In clustering based approach, the sensor device participates within its cluster members and the rest of communications with the entire network would be done through the CH sensor node. The current study exploits this idea in the spatial reutilize of the locally unique addresses. The current study suggests address\name solution would assign unique addresses locally to sensor devices, reutilized in a spatial manner and reduce name/address size by noticeable amount. So this work will provide serving this approach for the both (MAC and network level) name/address scheme.

1.2 Spanning Tree Topology Based Algorithms

This study will introduce and focus on Multi-hop Spanning Tree based algorithm in Section 5. In general, there are two types of WSN applications; data centric and node centric applications:

- **Data Centric Applications:** Data generation sensor device is no longer need to be uniquely identified. For instance, as it is required to use application for temperature monitoring, huge amount of sensor devices deploy to cover the area of interest. The monitored temperature in this applications relates to the group of sensor devices within geographic area, and it is useless to identity each sensor device.
- **Node Centric Applications:** In this type, it is necessary to identity data generation sensor device. As the data sending sensor device is uniquely identified, the collected data is significantly becomes useful and vice versa. This application is used in emergency response scenario [17,18].

In general, there are two levels of information collected by WSNs; events and data. In Section 5, the current work focuses around event driven based applications. In this type of WSNs, only events packets are communicated to the destination or Base Station (BS). This application is used in healthcare and enemy movement detection systems [15].

The current study proposes Multi-hop (Spanning Tree) Based Algorithms which cops also an event driven based application for WSNs. Furthermore, the suggested approach provides network level addressing, reutilizes addresses efficiently, and energy efficient as it avoids using of DAD system.

The current work is organized as follows. Previous related approaches are introduced in Section 2. The role of addresses in WSNs is debated in Section 3. Section 4 introduces clustered based node address naming solution in details. In Section 5, the novel spanning tree based naming solutions is presented. Section 6 discusses an experimental simulation results and finally, Section 7 concludes and provides possible future works in details.

2 Previous Related Works

Many recent approach in WSNs is focusing either in specific network topology or needing to use MAC and global address. These approaches add extra overhead bits, reduce the efficiency factor, exhaust the network resources and limit the entire life cycle. Contrarily, the proposed approach in this work relaxes the complexity, reduces overhead bits, increases the efficiency factor, and prolongs the lifetime of entire WSNs.

Many researchers have been suggested to utilize aspects/attributes from outside of the underlying topology and based on specific application to implement low level addressing/naming [19]. Authors of [16,20] have been conducted their efficient routing algorithms based on designed strategy followed in [19]. However, the address algorithms based on aspects/attribute design philosophy are recognized the need of a global network address per sensor device. This approach is still applicable to conduct diverse administrative tasks [21]. To minimize overheads of utilizing large length address size of global network names/addresses, the authors of [22] have proposed the usage of Random Ephemeral TRansaction Identifiers (RETRI). After implementing of RETRI, yields in small address size comparing to statically given globally unique names/addresses. However, they have doubts about the avoidance of collisions phenomena. The current study guarantees the avoiding of occurring of collisions and minimizing the name/address size to some extent. Recent Huge energy efficient schemes based MAC layer algorithms have also suggested over WSNs [23]. This approach requires unique MAC names/addresses leading to MAC header overheads. Reference [24] proposed a distributed name/address assignment algorithm which aims to minimize MAC names/addresses size. The allocated names are reutilized spatially and leading to reduce the name size is conducted through using encode technique over name/address. In their study the entire network wide unique MAC name/address per sensor device was changed into a locally unique MAC name/address. Furthermore, locally unique MAC name/address was exploited with the aspect/attribute based address/name specifying the final sink of packets. For instance in Fig. 1, network wide unique MAC name/address of 100 transfers to locally unique MAC name/address of aspect/attribute 1 and 110 transfers to 2. The locally unique names/addresses need smaller bits for representation and lead to energy conservation [19].

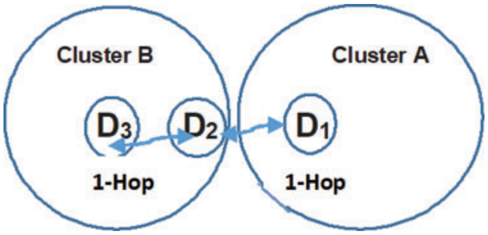

Figure 1: Two hop sensor neighbors (D1 and D3) as hidden terminals from each other

References [21,25–30] have suggested spatial IP based sensor device name/address scheme, which is derived from the location information per sensor device. In this scheme, the sensor device builds its spatial IP name/address from the location coordinates of the sensor of interest. The spatial IP name is represented lowest 2 significant octets in internet address IP. However, the length of name/address size of spatial IP stills considerably very large and adds extra communication overhead to entire WSNs.

The payload length of packet in Internet is large enough; this is reasonable for large IP style overhead. Unlike, the payload of WSN sensor devices which is almost lower than 16 bytes for each packet which considers high naming/addressing overheads are not preferable in WSNs applications. Various naming/addressing approaches in literature have considered the necessity of building efficient naming algorithms which is done well in [15,31,32].

Reference [33] categorizes naming/addressing approaches for WSNs into two types, stateful approaches which exploit the use of allocation table, and stateless approaches which not exploit the use of an address allocation table. In stateless approaches, the idea of using DAD is considered to guarantee the uniqueness of names/addresses in WSNs. Stateless naming/addressing scheme in Tree Cast Chaudhuri et al. [15] is suggested for efficient addressing, and needs the building of multiple disjoint trees which are intertwined and rooted at BS node.

Reference [31] suggested an energy efficient sensor node naming/addressing approach which exploits spatial reutilize of locally unique names/addresses. In this approach, sensor devices are arranged in a hierarchy of layers with layering numbers to suit the uniqueness condition. The authors of [24] suggested a distributed on-demand naming/addressing approach to provide assignment of link layer (MAC) names/addresses. This approach gets benefits of spatial reutilize of names/addresses and minimizes the header name/address overhead by the help of implementing Huffman coding scheme.

In [14], the approach of event-driven naming/addressing was suggested. Local uniqueness among neighbor sensor devices is considered for MAC naming/addressing, and an on-demand mechanism for network level naming/addressing is suggested as well. This approach is coupled with routing algorithm and uses DAD scheme to guarantee network layer uniqueness. Data aggregation and using the act of diluting by modulus naming is suggested in [34].

It was proved by all of the above naming/addressing scenarios in literature that the complexity of the naming/addressing process is placed on WSNs by persisting on strict arrangement or by implementing DAD scheme through broadcasting. The current study tries to dilute the complexity from the sensor devices to BS/sink node.

3 Conventional Role of Names/Addresses for WSNs

The classical role of names/addresses in WSNs states that member sensor device is given a wide unique global address for the purpose of administrative tasks such as, monitoring, configuration, data aggregation and downloading binary code within WSNs [21]. However, it was proved by recent researches that this global network names/address is no longer need to be applied upon routing work phases or identifying the BS/sink sensor device. Since, the inquiries in WSNs are broadcast towards entire networks [16]. Thus, aspects/attributes like location of sensor device location and/or data reading of sensor are utilized to identify BS/sink sensor device. These aspects/attributes are participating to construct routing algorithm as described in [20].

MAC name/address packet format shown in Tab. 1 is utilized by current research to find the next hop sensor device. Every sensor device processes the received packet to find the next hop link level MAC name/address. Based on available information in local routing table, each sensor device updates its next hop name/address of the sending packet. All sensor devices continue with this process till the desired packet is reached to the BS/sink sensor device based on destination name/address of the packet.

Table 1: Packet format in WSNs

Network address	MAC Address of next hop, Unique node ID say (100 . . . 110)	Attribute of next hop say (A1 . . . A2)	Payload data

4 Methodology of Naming/Addressing Solutions for Clustered Based WSNs

This section provides the naming solution methodology for cluster topology in the following subsections.

4.1 Problem Solution and Present Design Objectives

The clustered based WSNs algorithms provide dividing of sensor devices into clusters. To minimize communication and name/address overheads of entire network, the assigned sensor devices names/addresses could be utilized amongst cluster member sensors of other different clusters. Such approach provides the dual purpose of MAC and network level name/address.

Communication algorithm like CSN [35] requires unique sensor device names/addresses for its functionality phases. This algorithm assigns bounded times for lookup data and guides to data storage distribution based research for WSNs. The TCP/IP protocol stack memory minimization motivates the research into connecting WSNs with TCP/IP networks of Internet [36,37]. Using of TCP/IP algorithm needs unique name/address names for its functionality in WSNs. Due to inherited energy constraints of WSNs, global unique names/addresses are considered not preferable. Thus, the suggested solution in current study addresses such issues by providing energy efficient reusable locally unique names/addresses strategies.

The objectives for the addressing/naming solutions of the present design are:

- To minimize the data overhead per packet and provide all packets without collision for the entire WSNs.
- To avoid the centralized based approach and transfer to distributed based approach, also to consider scale well with large WSNs size.
- To exploit the use of dual purposes for both (MAC and the network) level names/addresses over entire WSNs.

4.2 Suggested Naming Solutions Assumptions and Basic Concepts

Naming is used to recognize things, while address is used to provide the required information that lead to get things [38]. The current study assumes sensor devices are static and distributed within an ad hoc topology configuration. BS sensor node must be placed far away from all sensor devices within entire WSN. The model used for data delivery is observer initiated model as in [6]. In the current study, the assumption used by [35,39] for clustering routing is considered as the process of cluster formation is finished at boot time phase of algorithm work. All formed clusters are kept with changes based on sensor node connect and disconnects within entire WSN lifecycle. Also the topological sensor device members are geographically closest to each others. In Hierarchical clustered approach, layer i CH sensor cooperates as layer i + 1 member. In all layers, CHs number is assumed as 6% and cluster member devices are limited to 16.

From basic concept view, cluster member sensor devices per any cluster are tending to exclude (incompatible) from other clusters, and names/addresses given to the cluster member sensors per one cluster could be spatially reutilized for others. Author of this work consider the optimum number of CHs in the WSNs as 6%. Also makes use of optimum number of cluster member sensors per cluster as 16 sensor devices, these 16 sensor devices could be given locally unique names/addresses implementing 4 bits per address space.

4.3 Suggested Collision Analysis Approach

Collision phenomena takes place within the coverage range of more than one sensor devices say D_i, hold same given locally unique name/address. To provide all packets without collision for the entire WSNs, collisions of communications packets could be overcome per cluster after disregarding rest of existing clusters at hierarchical level 0. In layer 1, communicated packets to/from clusters are considered as communication among sensors device members. But, space of 4 bits is no longer enough as there should be means to differentiate between layer 0 and layer 1 address. In Tab. 2, the author of this work suggests the addition of extra 2 bits to the existing 4 bits address space to make address space for higher layer.

Table 2: Global unique address format in WSNs

Layer n (locally unique address)	Layer 1 (locally unique address)	Layer 0 (locally unique address)
6-bit address	6-bit Address	4-bit address

The collisions are overcome while assignments of name/address fulfill the two cases below:

- **Case 1:** Cluster member sensor devices of cluster say C hold different names/addresses with a locally unique address say A_i given per one member sensor of cluster C say member sensor device M_i.

- **Case 2:** One hop and two hops non member neighbors of member sensors in cluster say A hold distinct names/addresses. Based on hidden terminal issue in WSNs, the need arises to place two hop sensor neighbors in case 2 too. Suppose D_1 is cluster member sensor device of a cluster say A, D_2 and D_3 are cluster member sensor devices of another cluster say B. Then, D_2 is one hop neighbor of D_1 and D_3 is one hop neighbor of $D_{2'}$ hence both of D_1 and D_3 are considered as hidden terminals from each other due to their short radios communication range. So in case of considering only one hop neighbors, and sensors D_1 and D_3 hold the same locally unique name/address, the collision phenomena occurs while there is communication between sensors D_2 and D_3. Based on avoiding collisions issues, this work includes two hop sensor neighbors as hidden terminals from each other in case 2 as shown in Fig. 1.

Suggested approach in this work considers each new sensor device say D_N would enter any clusters must fulfill both cases 1 and 2 above, then sensor device D_N is assigned with new name/address. This approach leads to provide avoid collision free in the functionality of name/address assignment set up work.

4.4 *Suggested MAC and Network Address/Name Approach*

Suggested approach in this work is to make use of 4 bits address space in link level as MAC names/address in layer 0 (locally unique for next hop destination). Addition of extra 2 bits to the existing 4 bits address space is used to make address space for higher layer level. These 6 bits address space are implemented as locally unique which must be utilized for finding next hop sensor device within routing the packet. The right most significant two bits of the 6 bits sensor device name/address of higher layer refers to find next hop sensor device. If the next hop MAC name/address is reduced to 4 bits, this refers that packet is passing down layer 1 to layer 0 and vice versa. Based on both cases 1 and 2 of previous subsection, avoiding collisions issues is achieved in the clustered based WSNs.

In general, the network level name/address is identifying the BS/sink sensor device of a sent packet. Within cluster, the 4 bits network names/addresses per cluster are implemented for communication. While 6 bits names/addresses per layer are implemented in communication within a layer. This work suggests a dynamic globally unique name/address approach for packet routing among multiple layers. The idea here, every layer within hierarchy removes 6 bits of sending down packet from global name, and every layer adds 6 bits to the name/address for sending packet up. Dynamically, the suggested auto-configuration addressing always implements small size bits while constructing name/address for network level.

4.5 *Suggested Global Name/Address/Name Approach*

The term wide unique network names refer to auto-configuration strategy that is sufficiently flexible to meet, implement and back global names/addresses. This approach adds extra bits to the existing address as leads to extra header overhead. Global names are commonly utilized for the purposes of administration like follow up the WSNs maintenance. The current approach creates dynamically an auto-configuration wide unique global name when there is application level demand. To create a global name on-demand, all addresses of all CH sensor devices within hierarchy are placed together per sending packets. Based on this approach, the least significant 4 bits of the globally unique name/address become the 4 bits name/address for layer 0, then appending the 6 bits name/address of the CH at layer level 1 to the left more significant side of the already existing 4 bits. Tab. 2 above shows the building process of the global address for underlying WSN. To the best of our knowledge, the name length of the suggested auto-configuration globally unique address scheme varies dynamically with the size of WSN.

4.6 Suggested Necessary Software Tools

All the necessary software tools are driven from CSN protocol [35]. This CSN protocol has two modes of operation; the Energy Efficient mode (EE_{mode}) and the Robust mode (R_{mode}) and goes through many steps as presented in the following subsections:

4.6.1 Initial Setup Phase

In order to maximize energy savings, every node in the network must interact through its closest neighbor. The term "The Ring Problem" arises as a result of this sensor environment restriction. This phase aims to create a logical ring of sensors network in which each node's clockwise successor is spatially nearest to it. Two approximate solutions to the entire ring issue have been proposed in this phase: the Chain Method (CM) and the Set Average Method (SAM).

In CM mode, it assigns each sensor node a_i in a cluster C the available sensor that is geographically nearest to it as its successor. Consequently, this indicates that the least amount of energy is expended when a_i connects with its successor node. The initial configuration must be performed by the SAM if the intended mode of operation is R_{mode}. While if EE_{mode} is the intended mode of operation, a CM should indeed be chosen.

4.6.2 Cluster Head Rotation Phase

In contrast to LEACH [13], the algorithm of the current work rotates cluster heads in a round-robin way. In addition, this algorithm like CSN protocol has no idea of rounds, thus when a cluster is established during the initial setup, the cluster creation algorithms shouldn't need to be run again. When each CH sensor node of cluster C at level (i) has used one energy quantum E_q, it makes its clockwise successor in the ring the next head. The value of E_q is given by:

$$E_q = E_m/\mu \tag{1}$$

where E_m is the sensor's maximum energy and μ is a constant number. One may make CH rotations more regular by raising the value of μ and conversely. In this work, the cluster head rotation technique has the advantage of avoiding head rotation while the sensor node is inactive (that is when there are no\few requests out from service. Furthermore, the rotation mechanism assures that a sensor node is reassigned as CH only after every other cluster member has served as CH precisely once.

4.6.3 Hierarchical Clustering Phase

This work's CM and SAM may simply be utilized to create higher levels of clusters. As a super sensor Si, each cluster head from the lower layer participates in the upper layer, and thus reducing the total number of nodes participating in the higher levels. Those nodes involved in the higher levels will need to save more information, and it would be preferable to spread this data among a greater number of nodes per cluster due to storage constraints.

Furthermore, given the geographical gap between higher layer cluster members grows as we move up to a higher level. Having more nodes per cluster is desirable in order to reduce the geographical distance between neighbor nodes in higher layer clusters. For instance, let λ_i be the maximum number of sensors in a cluster C at level i and N_i be the total number of nodes participating in level i of the cluster hierarchy, then at level i the number of clusters S_i is given by:

$$S_i = N_i/\lambda_i \tag{2}$$

4.6.4 Energy-Efficient Mode vs. Robust Mode Phase

The proposed tool like CSN functions may perform lookups with a limitation of O (log N) packets while running in R_{mode}. However, because each node is directly communicating to a node that may be farther away, this efficiency in data lookup comes at the cost of increased energy consumption. The R_{mode} has only been utilized if the EE_{mode} is unable to meet the application delay requirements. The logical function of communicating to a node is isolated from its real routing in the EE_{mode}, and packets are routed by each node only interacting with its nearest neighbor.

As EE_{mode} is the normal mode of operation, the suggested protocol changes to R_{mode} only if EE_{mode} cannot meet the user latency requirements. The application's allowable delay, say d, is compared to a delay threshold level, Γd, and if ($d \leq \Gamma d$) R_{mode} is used; otherwise, EE_{mode} is used. All logical communications to a node are transmitted straight to it in pure R_{mode}. Unlike in pure EE_{mode}, where all logical messages to a node are routed indirect means by each node forwarding the message to its nearest neighbor.

4.6.5 Incremental Setup (ISA) vs. Parallel Setup (PSA) Phase

In a parallel setup, the CH selection is identical to LEACH [13]. Each sensor node ai selects a random value between 0 and 1 and decides to become the CH if ($y > \Gamma h$), where Γh is a threshold. At the current level i, Γh is set to the required number of CHs ($\Gamma h = 0.06$ gives 6% of the total sensors) as CHs. Therefore, in this case, $\forall \alpha i$ probability of 0.06 is chance of becoming a CH. After determining on the CH, the logical ring clusters can be formed using either the chain technique or the set-average method.

However unlike ISA algorithm, which has one cluster formation prompts the formation of the next, the PSA method has all cluster formations happen at the same time. The ISA method takes longer, but ensures that the most energy-efficient cluster formation occurs. PSA algorithm on the other hand, creates clusters fast, however the optimal cluster formation may not occur because CHs are not distributed evenly across the network.

4.6.6 Lookup Operation Phase

Each sensor, say ai in the topmost level m, has the ability to listen to user requests. The user submits his inquiry to the $\alpha i \in$ level m nearest to him geographically. Upon receiving the query, the sensor ai examines if the requested key is present in its own local store, according to R_{mode}. If indeed the key isn't discovered, sensor ai looks through its local finger table. Each node ai has a finger table that includes data about O (log λi) other nodes. If such finger table doesn't quite contain the needed key, the query is forwarded to the node in the finger table that is closest to the target. Let's say ak is the node in question. At any such sensor ai the identical method is followed. When a node, say af, finds a key mapping at level $I \neq 0$ in hierarchical clustering, af executes the lookup operation in its member cluster at level i-1. So the method is continued until we reach level 0, at which point the lookup operation's result will point to the sensor node that properly stores the data related with the requested key.

5 Methodology of Spanning Tree Based Naming Solutions Approach

This section provides the naming solution methodology for spanning tree topology in the following subsections.

5.1 Suggested Naming Solutions Basic Concept and Assumptions

Suggested solutions are built according to an on-demand approach which exploits a lease-based idea during the name assignment process. It exploits the advantages of random nature based event-driven sensor network. This aspect helps to allocate and leave names/addresses per sensor device dynamically within entire WSN. Consequently, it is exploiting the approach of reuse names/addresses per sensor devices within entire WSN. Suggested approach aims to minimize the header overhead of underlying naming/addressing scheme. The idea in [34] is that main requirement of almost applications of WSN needs unique sensor device identification. For applications such as, battlefield, Intrusion Detection Applications (IDA) and emergency response, useful events are tying down to a specific sensor device in real time.

This work considers location unawareness for entire sensor network, Consequently, the reduction of overheads which come from the location related process is achieved. The scheme provided by [14] is adopted for sensor device link level name/address assignment as well. Finally, the idea of relatively stationary is assumed for entire WSN sensor devices.

5.2 Suggested Naming Solution Approach Work Phases

Suggested approach goes through 3 work phases as in the following subsections:

5.2.1 Setup Work Phase

In the current study, assignment of network level layer name/address scheme is introduced for spanning tree based WSNs. In setup work phase, it assigns permanently locally unique link level name to each sensor node similar to approach used in algorithm of [14]. In this type of name/address scheme, providing reassigns process when original sensor device is dying and/or new sensor devices join WSN. The work process here, the Sink/BS sensor device broadcasts a configuration message packet. The sent message packet must be forwarded by the nearest sensor device member to the next hop sensor node neighbor. Consequently, this process continues till spanning tree will be created, started from Sink/BS and ended in last sensor device within tree. This approach helps sensors to find next hop on their ways to reach BS sensor device as shown in Fig. 2. Every sensor device is considered joined the WSN (booted) in successful manner only after holding the configuration packet.

For scalable WSN, a new node to enter the network it must broadcast join-request packet, then this sent packet is captured by the nearest neighbor sensor devices within its transmission range. Sensor node within one hop distances answer to received join-request message using the same configuration packet they have already received from the BS/Sink sensor. To this end, a new sensor device received the configuration packet and the setup phase is over. The source of the configuration packet is considered as next hop sensor by a new sensor device entered the WSN.

5.2.2 Suggested Name/Address Request Phase Work

To deliver the event of interest to the BS/Sink device, a need arises to hold network level name/address. This is helpful for identifying the source sensor device of the generated event at the Sink sensor device. Address/Name request packet generated by the source of event is shown in Fig. 3.

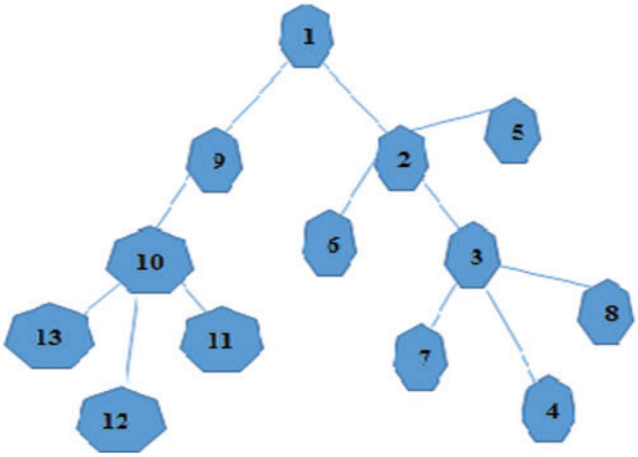

Figure 2: Multi-hop (spanning tree) structure

Source Device ID	Type	Event Identifier (ID)	ST path (to reach the sink node)

Figure 3: Address request packet format

Where Source Device ID refers as the link level name of the source sensor device, the term Type refers as the type of packet and also used as an ID for the name/address request packet destination sensor device. While the term Event Identifier ID is used for identifying the particular generated event request. It is also helpful for mapping name allocation to the specific name request. Finally, the ST path to reach BS/sink node denotes rout path of the name/address to the BS/sink sensor device.

5.2.3 Suggested Name/Address Assignment Phase Work

The task of BS/Sink sensor device to maintain names/addresses allocation table, this table includes a list of names/addresses associated with related (free/in use) status flag per each name/address. After receiving an address request, the sink node assigns available free name to specific sensor device or to discards the request. To this end, the sink node broadcasts name allocation message as shown in Fig. 4.

Source Device ID	Type	Event Identifier (ID)	Name / Address	ST path (in reversed direction)

Figure 4: Name/Address allocation packet format

Where Source Device ID refers to link level name associated to BS/Sink device, Source ID refers to link level name related to requested sensor device, the Type term refers as the type of the packet and can be used as an ID for the name/address for BS/Sink sensor device. While the term Event Identifier ID is copied to the name/address allocation packet from specific name/address request packet and is also used for mapping name/address allocation to the specific name/address request. Name/address field refers as the allocated name/address. Finally, the ST path (in reversed direction) refers to in reverse path of (ST path to reach the sink) within name/address request packet. The Bs/Sink sensor device keeps both ST path of the requested sensor device and the event identifier ID and then ties them in network layer level name/address.

While BS sensor device responds the name/address allocation, the lease_timer is started with setting value to T_{max}, where T_{max} is maximum amount of time per sensor device can hold name. For the current study, the T_{max} is denoted as a lease timer with a fixed value between (180secs-200secs). This lease timer after being expired, will be assigned to another sensor device will request name/address in future. Name/Address request and an allocation name/address are illustrated clearly in Fig. 5.

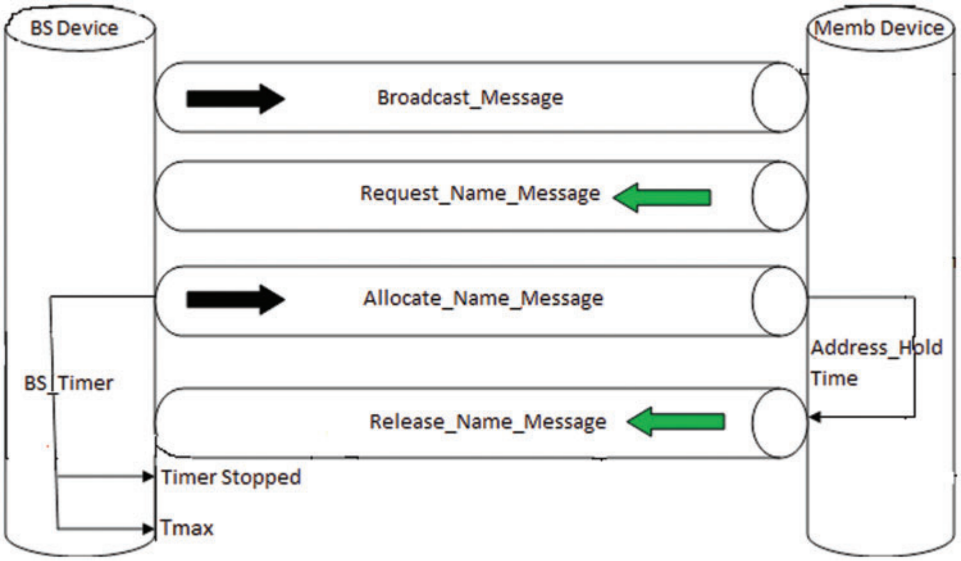

Figure 5: A typical name/address request and allocation process

6 Methodology of Experimental Environment and Simulation Test

In this work, the simulator developed for [35] is conducted. The approach of wireless communications based on first order radio model used in LEACH [13] is adopted for efficiency (E) evaluation. The energy dissipated by the transmitter-receiver and the transmit amplifier is denoted by $E_{electric}$ and $E_{amplifier}$ respectively.

$$E_{Transmit}(k,d) = E_{electric} \times k + E_{amplifier} \times k \times d^2 \tag{3}$$

$$E_{Receive}(k) = E_{electric} \times k \tag{4}$$

where $E_{electric} = 50$ nJ/bit, $E_{amplifier} = 100$ pJ/bit/m^2, k is rate of data (bits per packet) and d is the distance to transmit. The communication with the Base Station (BS) is considered as high energy operation in this test bed. Random deployment of sensor devices on used test bed of (L × L) m is adopted. All sensors are placed at random on a (200x200) meter test bed. Fig. 6 depicts a 120-sensor node network that was randomly deployed. At the lowest level of hierarchical clustering, the little dots represent regular nodes and the circles represent CHs. The distribution of CHs according to the Incremental Setup (ISA) algorithm is seen in Fig. 6. CHs number is set to 6% of the entire sensor devices within the layer, this is reasonable value as it is used in LEACH [13] as well. The Incremental Setup (ISA) based cluster head distribution was shown to be superior than the Parallel Setup (PSA), which had a random CH distribution with so many heads concentrated in tiny regions.

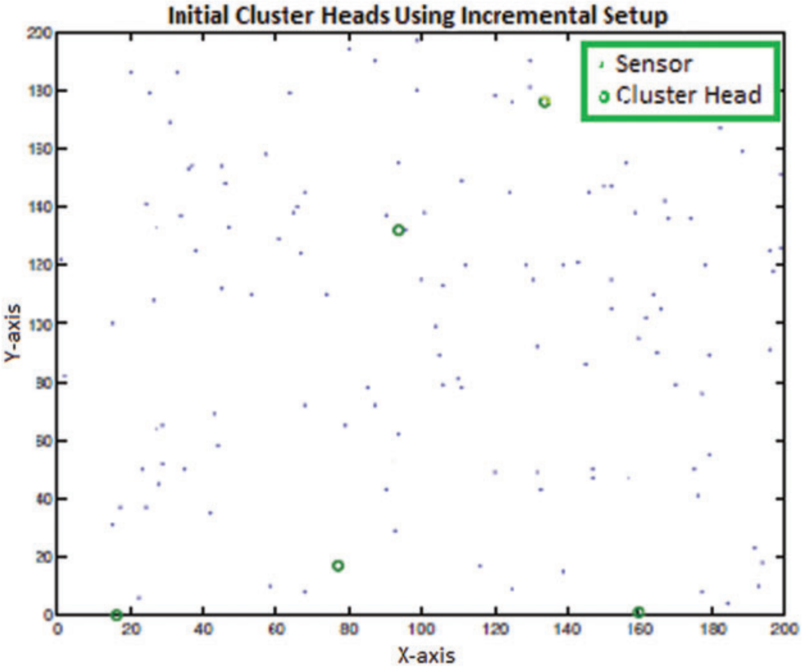

Figure 6: A random deployment of a 120 sensor node network using ISA algorithm

The effective Efficiency parameter (E) is defined as:

$$E = \frac{D}{D + H} \tag{5}$$

where D is the data payload in bits and H is bits header.

From simulation findings, Fig. 7 shows that display of efficiency E factor is affected by network and MAC addresses; while Fig. 8 presents only the network address effect on E factor. From both Figs. 7 and 8, increasing of efficiency E upon increasing in data rate is justified as more useful bits are sent for each packet with keeping the overhead of bits header H constant as in Eq. (5) above. Finally, based on simulation test, the E factor of locally unique name/address outperforms the global name/address by twice time.

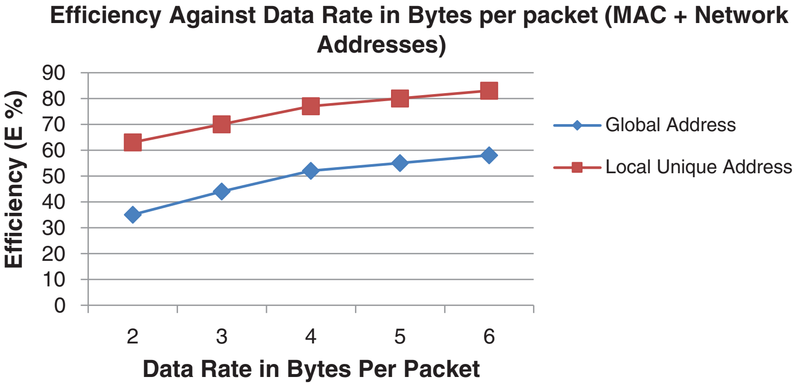

Figure 7: Efficiency of global and locally unique (MAC + Network) addressing

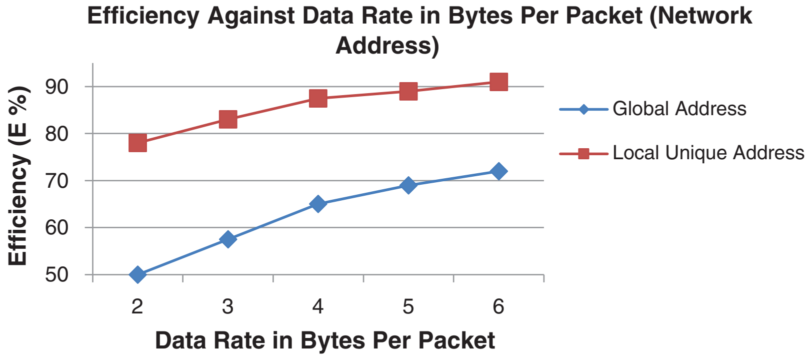

Figure 8: Efficiency of global and locally unique (Network) addressing

To conduct the scalability test, the global address of 16-bits is used, and then the network size is gradually increased. The scalability of global and locally unique addresses is evaluated as in Fig. 9. The E curve of global name stays constant and scales well till the end point of name space exhaustion. In this point and onward, it can no longer support the entire sensor devices within network. To this end, a new 32 bits of global name is assigned after the 16 bits address exhausted. Fig. 9 shows that E factor of locally unique name declines slowly and gracefully with increasing in size of sensor network. Contrarily, there is a rapid breakdown for a system as in the global name/address case.

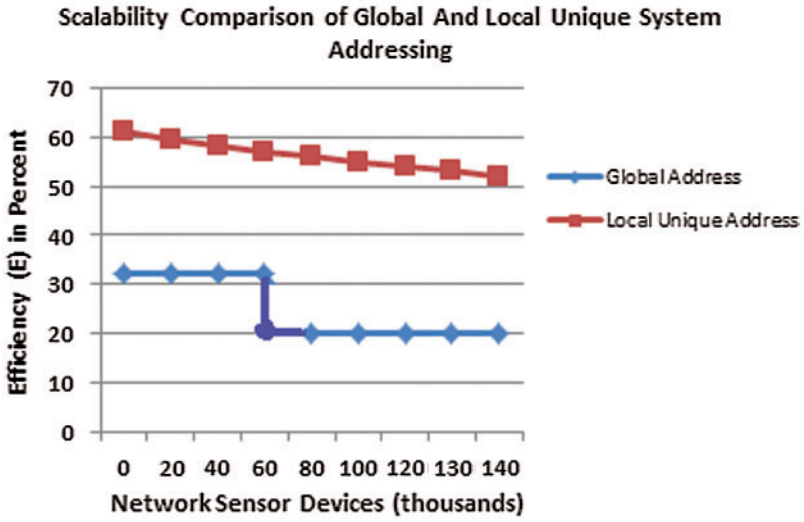

Figure 9: Scalability test of global and locally unique (MAC + Network) addressing

7 Conclusions and Future Works

In WSNs, Addressing/Naming is considered as hot research topic nowadays. This topic is helpful to provide essential levels associated to functionality of network communication for instance like unicast process. Naming/Addressing idea provides flexible auto-configuration based names/addresses scheme in the field of WSNs. This work suggested names/addresses auto-configuration solutions for 2 topologies cluster and novel spanning tree based WSNs. To meet requirements in cluster based WSNs topology, the current study has supplied naming/addressing mechanism based on locally unique spatially reutilizing names, and has shown by an experimental simulation test how such approach outperforms globally unique name/address approach in efficiency by twice, this comes from reduction of header overhead bits and more payload efficiency E factor. Consequently, leads to energy efficient system and to extend the lifespan of entire sensor network, has also achieved that the separate function of names/addresses approach for MAC and network level layers are not required.

To handle the requirements for novel spanning tree based topology, the suggested solution is very plausible in event-driven based applications and is capable of gaining probabilistic reutilize of network layer level addresses as well. Suggested scheme achieves rational reusability factors that minimize the names/addresses number for deployment of specific WSN. This approach has considerable significance as WSNs are distinguished for using the range of hundreds of thousands of sensor devices. To the best of my knowledge, suggested addressing mechanism for the above mentioned topologies provides the followings: First, to handle high degree of scalability to include very large WSN and are satisfied by network layer algorithms in literature as in [35,39,40]. Second, cost terms descriptions of addressing like exchanging of extra packets and maintaining address/names scheme are satisfied by recent algorithms in literature as in [41–44].

The author of current study provides a guideline to mitigate assumptions that push addressing/naming algorithms to more flexibility for network layer level algorithm based on clustered WSNs like [45–49].

Despite the fact that the current study suggested solutions are favorable for energy efficiency, there is need for further study to handle other key issues: First, the term Quality of Service (QoS) aware naming algorithm in WSNs can reduce the time delay of duration of communication connection as recent applications requires real time information. Yet, a few researches have handled with aspect of QoS for limited energy tiny WSNs. Second, consideration of secure WSNs is significant issue in auto-configuration algorithms. Recent protocols have no longer considered it in their works. Because of broadcasting environment view WSNs, naming/addressing algorithms are vulnerable to many types of threads. Third, integration of WSN with wired network is another future research for handling naming/addressing algorithms.

Acknowledgement: Author thanks those who contributed to the article.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declares that he has no conflicts of interest to report regarding the present study.

References

[1] Q. I. Sarhan, “Systematic survey on smart home safety and security systems using the arduino platform,” *IEEE Access Journal*, vol. 8, pp. 128362–128384, 2020.

[2] J. A. Fadhil, O. A. Omar and Q. I. Sarhan, “A survey on the applications of smart home systems, “in *Proceeding of CSASE*, Duhok, Kurdistan Region, Iraq, pp. 168–173, 2020.

[3] I. S. Kocher, “Software engineering methods to improve the design of software reliability systems: Roadmap, “*Journal of Southwest Jiaotong University*, vol. 55, no. 3, pp. 1–9, 2020.

[4] V. Raghunathan, C. Schurgers, S. Park and M. B. Srivastava, “Energy aware wireless microsensor networks,” *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40–50, 2002.

[5] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler *et al.*, “System architecture directions for networked sensors,” in *Proceeding of ASPLOS IX: The Ninth International Conference on Architectural Support for Programming Languages and Operating Systems*, pp. 93–104, November 2000.

[6] S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, "A taxonomy of wireless micro-sensor network models, "*Mobile Computing and Communication Review*, vol. 6, no. 2, pp. 28–36, 2002.

[7] A. Schmidt and K. V. Laerhoven, "How to build smart appliances?," *IEEE Personal Communications*, vol. 8, no. 4, pp. 66–71, 2001.

[8] D. Estrin, L. Girod, G. Pottie and M. Srivastava, "Instrumenting the world with wireless sensor networks," in *Processing of ICASSP*, Salt Lake City, Utah, 2001.

[9] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–116, 2002.

[10] G. Pottie and W. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, no, no. 5, pp. 51–58, 2000.

[11] W. R. Heinzelman, J. W. Kulik and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceedings of the ACM MOBICOM*, Seattle, Washington, USA, pp. 174–185, 1999.

[12] K. Sohrabi, J. Gao, V. A. Wadhi and G. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Personal Communications Mag.*, vol. 7, no. 5, pp. 16–27, 2000.

[13] W. Heinzelman, "*Application-specific protocol architectures for wireless networks*, " *Ph.D. thesis*, Massachusetts Institute of Technology, 2000.

[14] S. Motegi, K. Yoshihara and H. Horiuchi, "Implementation and evaluation of on-demand address allocation for event-driven sensor network," in *Proc. of the 2005 Symposium on Applications and the Internet*, Trento, Italy, pp. 352–360, 2005.

[15] S. P. Chaudhuri, S. Du, A. K. Saha and D. B. Johnson, "Treecast: A stateless addressing and routing architecture for sensor networks," in *Proc. of the 18th Int. Parallel and Distributed Processing Symposium*, Santa Fe, NM, USA, pp. 221–231, 2004.

[16] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proceeding of MOBICOM*, Seattle, Washington, USA, pp. 263–270, 1999.

[17] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel *et al.*, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.

[18] V. Kumar, D. Rus and S. Singh, "Robot and sensor networks for first responder," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 24–33, 2004.

[19] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin *et al.*, "Building efficient wireless sensor networks with low level naming," in *Proc. of the Symposium on Operating Systems Principles, Chateau Lake Louise*, Banff, Alberta, Canada, pp. 146–159, 2001.

[20] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. of the Sixth MOBICOM*, Boston, pp. 56–67, 2000.

[21] A. Dunkels, J. Alonso and T. Voigt, "Making TCP/IP viable for wireless sensor networks," in *Proceeding of First European Workshop on Wireless Sensor Networks EWSN, Work-in Progress Session*, Berlin, Germany, 2004.

[22] J. Elson and D. E. Random, "Ephemeral transaction identifiers in dynamic sensor networks," in *Proceeding of ICDCS'01*, Phoenix, AZ, 2001.

[23] W. Ye, J. Heidemann and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proc. of Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies*, New York, NY, USA, vol. 3, pp. 1567–1576, 2002.

[24] C. Schurgers, G. Kulkarni and M. B. Srivastava, "Distributed assignment of encoded mac addresses in sensor networks," in *Proceeding of the 2nd ACM Int. Symp. on Mobile Ad Hoc Networking & Computing*, Long Beach, CA, pp. 295–298, 2001.

[25] A. Savvides, C. Han and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, pp. 166–179, 2001.

[26] J. Chen, L. Yip, J. Elson, H. Wang, D. Maniezzo *et al.*, "Coherent acoustic array processing and localization on wireless sensor network," *IEEE*, vol. 91, no. 8, pp. 1154–1162, 2003.

[27] N. Bulusu, J. Heidemann and D. Estrin, "GPS-Less low cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28–34, 2000.

[28] H. Wang, J. Elson, L. Girod, D. Estrin and K. Yao, "Target classification and localization in habitat monitoring," in *Proc. of IEEE ICASSP2003*, Hong Kong, China, pp. 4–844, 2003.

[29] N. Bulusu, V. Bychkovskiy, D. Estrin and J. Heidemann, "Scalable, ad hoc deployable, rf-based localization," in *Proc. of the Grace Hopper Conf. on Celebration of Women in Computing, Vancouver*, Vancouver, British Columbia, Canada, pp. 1–5, 2002.

[30] N. Bulusu, J. Heidemann, D. Estrin and T. Tran, "Self-configuring localization systems: Design and experimental evaluation," *ACM Transactions on Embedded Computing Systems (ACM TECS)*, vol. 3, no. 1, pp. 24–60, 2003.

[31] M. Ali and Z. A. Uzmi,"An energy-efficient node address naming scheme for wireless sensor networks," in *Proceeding of IEEE International Networking and Communications Conference (INCC)*, Lahore, Pakistan, pp. 25–30, 2004.

[32] T. Huynh and C. Hong, "A novel addressing architecture for wireless sensor network," in *Proc. of the 24th IEEE Int. Conf. on Performance, Computing, and Communications*, Phoenix, AZ, USA, pp. 529–533, 2005.

[33] K. Weniger and M. Zitterbart, "Address autoconfiguration in mobile adhoc networks: Current approaches and future directions," *IEEE Network*, vol. 18, no. 4, pp. 6–14, 2004.

[34] E. Cayrici," "Data aggregation and dilution by modulus addressing in wireless sensor networks," *IEEE Communication Letters*, vol. 7, no. 4, pp. 355–357, 2003.

[35] M. Ali and Z. A. Uzmi, "A network protocol for serving dynamic queries in large-scale wireless sensor networks," in *Proc. of 2nd Annual Conf. on Communication Networks and Services Research (CNSR2004)*, Fredericton, N.B., Canada, 2004.

[36] A. Dunkels, "Full TCP/IP for 8-bit architectures," in *Proc. of MobiSys'03*, San Francisco, California, pp. 85–98, 2003.

[37] A. Dunkels, T. Voigt, J. Alonso, H. Ritter and J. Schiller, "Connecting wireless sensornets with tcp/ip networks," in *Proc. of the Second Int. Conf. on Wired/Wireless Internet Communications (WWIC2004)*, Frankfurt (Oder), Germany, pp. 143–152, 2004.

[38] H. Karl and A. Willig, "Protocols and archtectures for wireless sensor networks," www.wilew.com, *2007*, accessed at 19- 09-2017.

[39] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proc. of IEEE Aerospace Conf.*, Big Sky, MT, USA, pp. 33–39, 2002.

[40] F. Ye and R. Pan, "A survey of addressing algorithms for wireless sensor networks," in *Proceeding of 5th Int. Conf. on Wireless Communications, Networking and Mobile Computing*, Beijing, China, pp. 24–26, 2009.

[41] Z. Yao and F. Dressler, "Dynamic address allocation for management and control in wireless sensor networks," in *Proc. of the 40th Annual Hawaii Int. Conf. on System Sciences (HICSS'07)*, Waikoloa, HI, USA, pp. 292b, 2007.

[42] Y. Li-Hsing and T. Wei-Ting, "Flexible address configurations for tree-based zigbee/ieee 802.15.4 wireless networks," in *Proceeding of 22nd Int. Conf. on Advanced Information Networking and Applications AINA*, Gino-wan, Japan, pp. 395–402, 2008.

[43] J. I. Bangash, A. Abdullah, M. H. Anisi and A. Khan, "A survey of routing protocols in wireless body sensor networks," *Sensor*, vol. 14, pp. 1322–1357, 2014.

[44] M. M. Warrier and A. Kumar, "Energy efficient routing in wireless sensor networks: A survey," in *Proc. of Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 1987–1992, 2016.

[45] I. Gawdan and Q. I. Sarhan, "Performance evaluation of novel secure key management scheme over ban wireless sensor networks," *Journal of University of Duhok*, vol. 19, no. 1, pp. 179–188, 2016.

[46] I. S. Kocher and Q. I. Sarhan, "Classifying routing algorithms upon clustered based wireless sensor networks: A survey," *ZANCO Journal of Pure and Applied Science (ZJPAS)*, vol. 29, no. 2, pp. 25–36, 2017.

[47] I. S. Gawdan, C. -O. Chow, T. A. Zia and Q. I. Gawdan, "Cross-layer based security solutions for wireless sensor networks," *International Journal of the Physical Sciences (IJPS)*, vol. 6, no. 17, pp. 4245–4254, 2011a.

[48] I. S. Gawdan, C. -O. Chow, T. A. Zia and Q. I. Sarhan, "A novel secure key management module for hierarchical clustering wireless sensor networks," in *Proceeding of 3rd Int. Conf. on Computational Intelligence, Modeling and Simulation (CIMSim 2011)*, Langkawi, Malaysia, pp. 312–316, 2011b.

[49] I. S. Kocher, "A systematical roadmap on various security vulnerabilities and countermeasures in routing algorithms upon wsns," *Academic Journal of Nawroz University (AJNU)*, vol. 10, no. 3, pp. 1–17, 2021.