IMPLEMENTATION OF WSN PROTOCOL ON A HETEROGENEOUS HARDWARE

JAGADEESHA, R.B. 1,*, OMAR ALFANDI 2

1 National Institute of Technology, Karnataka, India
2 Georg-August-Universitat Gottingen, Germany
*Corresponding Author: jagadeesha_rb@yahoo.com

Abstract

Wireless sensor network has become the ubiquitous communication system due to its low power consumption, durability, ease of deployment, and simplicity of the protocol stack. It is most suitable for applications involving limited, infrequent data transfers. But to make it suitable for applications involving high data rate and bulk amount of data transfers like video surveillance or monitoring, certain modifications are necessary. As the WSN stack is based on IEEE 802.15.4 standard regulations, when it is implemented on a IEEE 802.15.4 compliant hardware it may not be possible to serve the above purpose. Thus in this proposal, to achieve high data rate, the WSN stack is imported on to the IEEE 802.11 enabled hardware by making suitable modifications into the protocol stack. Even though the IEEE 802.11 based hardware consumes higher power, the WSN stack is suitably tailored to mitigate the excess power requirement for the data transfer by using some power conservative techniques. To make the system more power conservative new node deployment scheme, range selection method, power conservative microcontroller sleep states, block acknowledgement methods are also introduced. The features like higher bandwidth and buffer capability of the transceiver are explored in this proposal to achieve the objectives efficiently. Thus by making the stack simple and power efficient based on IEEE 802.15.4 standard and importing on to IEEE 802.11 compliant hardware the application requirements are suitably handled.

Keywords: IEEE 802.15.4, IEEE 802.11, Block acknowledgement method.

1. Introduction

The wireless sensor network consists of a network of sensors to exchange the gathered information by wireless means. Such networks will have the features
like low power consumption, high durability, easier network formation, self-organization, which makes them most suitable for applications involving monitoring, automation; namely, temperature, pressure monitoring in industry, monitoring chemical activity in the oil fields, video monitoring in public areas, etc. In most of such applications it is enough that some amount of data that is being monitored by the sensors be communicated to the remote station. In such applications the amount of data to be transferred will be limited and little amount of delay can be tolerated. But for applications like border area monitoring using video surveillance, the amount of data has to be transferred to the remote controlling station without much delay; which requires large data rate, bandwidth, memory capacity. The WSN is based on IEEE 802.15.4 std consisting of physical and MAC layers [1]. The recent developments and involvement of many researchers in the field of WSN has given rise to think about the applications which demands more resources like memory, power, bandwidth and computational capabilities [2-4].

Inspired by such innovations, here proposed a concept to implement a low powered WSN stack onto the IEEE 802.11b/g/n enabled transceiver [5]. This requires suitable modification into the protocol stack, and to exploits the benefits provided by the hardware [6]. The IEEE 802.11 transceiver has higher and adaptable data rates of 1, 2, 11, 54 Mbps, offers higher bandwidth of 20 MHz as against the IEEE 802.15.4 std’s data rate of 250 kbps and 2 MHz bandwidth. The power consumption by the IEEE 802.11 transceiver for various data transmission activities will be several times greater than that of IEEE 802.15.4 std. Thus there is an immediate need to perform the modifications on to the WSN protocol stack targeted for low power applications to achieve higher data rate and better range.

The organization of this paper is as follows: In section 2 the literature review of the previous various projects which relate to the proposed work are considered. In section 3 the protocol stacks on which the proposed ideas to be implemented are discussed in detail. The subsections deals with the power conservative schemes for microcontroller operation, a power efficient trans-reception method for wireless sensor network, node deployment and addressing method, implantation of WSN protocol on heterogeneous hardware using block acknowledgment and variable data rate features of the hardware. In Section 4 paper is concluded highlighting the main outcomes of the proposed work.

2. Literature Review

In this section we reviewed the previous works done in the similar area related to the proposed topic. There are five protocol stacks which are considered in this literature that are compatible with 802.11 to provide higher data rate for WSN applications. The ultra-low power SensiFi stack [7], a proprietary protocol stack by the Redpine Inc. is compatible with 802.11a/b/g/n and has an on board microcontroller. It supports variable dates using DSSS and OFDM. Panoptes [2] is another project for WSN based video monitoring applications that demand higher bandwidth and data rates. It uses Intel StrongARM processor and 802.11 enabled transceivers. It supports variable data rates using DSSS and OFDM. SensEye [8] a stack for heterogeneous video surveillance project using 802.11 std operates at 900 MHz, uses multi-tier architecture for sensor deployment.
The ultra-low power Wi-Fi G2C543 [9] uses TCP/IP features with two operating modes: active and sleep to reduce the power consumption. In addition to that, it has sensor interface to access the environmental monitored data. The ZG2100M [10] of microchip corporation is a low power 802.11 based embedded Wi-Fi module operating at 2.4 GHz ISM band.

All these protocol stacks which are designed for low power high data rate applications are either proprietary or SoC, whose further details are hidden. In addition to this, in all of the stacks the IEEE 802.11 protocol features are implemented on the compliant hardware. The other issues as discussed in this paper like address and node deployment scheme used in [11, 12] concentrates on the network growth by considering the current network elements.

However, in our proposal an attempt is made to implement the IEEE 802.15.4 based protocol stack onto the IEEE 802.11 compliant transceiver with suitable modifications into the stack to meet the low power and high data rate requirements of the application. The proposed architecture consists of several layers through which the functionalities required for WSN applications are extracted and are supported by the proposed protocols to make the system power efficient.

3. Research Methodology

The objective of the research is to attain high data rate to meet the requirement of the applications in the field of wireless sensor networks. The usual WSN protocol stacks offers low data rate when developed on the hardware which are 802.15.4 compliant. But here the WSN stack is imported on the 802.11 based hardware to explore the feature of its higher data rate even though it consumes excess power comparatively. Thus there is a need to make suitable changes into the protocol stack to make the system power efficient.

There are several protocol stacks available like zigbee [11], atmel stack [13], etc. based on IEEE 802.15.4 MAC and PHY guidelines; and are developed on the 802.15.4 enabled hardware by considering the OSI model as a reference. Zigbee is considered as a benchmark in most of the literatures and it has application objects to cater the need of different sensors deployed for variety of applications. In recent years there are protocol stacks based on IPV6 connectivity, popularly known as 6LoWPAN stacks like nanostack [14], uIP6 stack [15], Jennic stack [16], etc. to carry the WSN data through IPV6 network. But while IP enabling a WSN stack which is designed on hardware of limited resources, and limited address space, there is a need to have an adaptation layer to perform the conversion activities suitably [17] for efficient communication.

The coordinator in a WSN can assign the nodes with a 64 bit address, but the IPv6 needs address space of 128 bits. Also the maximum size of MPDU in a 802.15.4 based stack is 127 octets, whereas in IPv6 the minimum size of the data gram is 1280 octets; thus there is a need to fragment the IP datagram by the adaptation layer to meet the requirements of the WSN MAC layer before imposing on the hardware.

By considering all these, in this paper two protocol stacks are proposed: one to carry the data generated by general WSN applications like video surveillance, environmental monitoring, which requires data to be transferred at higher rate by the IEEE 802.11 enabled transceiver having higher bandwidth; other stack to
carry the WSN data through the internet, i.e., IP infrastructure based on TCP/IP model. This requires an adaptation layer to perform the conversion process to meet the data size requirements of 802.15.4 MAC layer and to be carried by the 802.11 based transceiver.

The protocol stack, shown in Fig. 1, consists of application layer, application support layer, network layer, device management layer, link management layer, medium access control layer, physical layer and hardware layer. There are sub blocks like resource unit, power management unit to enhance the performance of the stack. The functionalities of the different layers are discussed here in brief.

The application layer has functions to initialize the lower layers as soon as the device is turned ON, and to provide the user interface. There are initialization functions defined by each layer to initiate the operations of the layer below it. There are also the tasks associated with each layer which enables the particular operation of a layer by providing the appropriate parameters in the form of primitives. These primitives between any layers are based on the guidelines of IEEE 802.15.4 std as defined between the MAC and PHY layers [1]. The application layer can be configured with different application object in association with the application support layer to present the data from various sensors deployed for monitoring the different kind of events.

The application support layer has functions to initialize the network layer and also it holds the data base of different application profiles which are invoked by the application layer, when data from different sensors dedicated for various applications have to be accessed. This helps in directing the data to the particular sensor from the application.

Network layer has the function of node deployment, address allocation, routing and initiation of the device management layer. The device management layer has functions to enable the security module, interference avoidance unit.

![Fig. 1. WSN Protocol Stack on 802.11 Hardware.](image)
Link interface layer has the responsibility of making the stack accessible by different link technologies like Ethernet, 802.15.4, 802.11, Bluetooth, etc.

The functions of the MAC layer includes beacon generation, providing support for channel access using CSMA-CA, initialization of data and management activities and initialization of the PHY layer functionalities. PHY layer deals with transceiver mode selection and activities connected with transmission and reception. The hardware layer has functionalities and modules for interrupt to govern the trans-reception activities, timing module to track the various events, SPI module, and power conservation functions. The hardware is 802.11b/g transceiver enabled module which has adaptable data rate to meet the demand of applications requiring higher data rate; also the hardware supports higher buffer space to enable faster data transfer.

In case of applications like industry automation, smart home, border security the sensors are deployed and are to be monitored remotely using IP infrastructure. To facilitate the sensor monitored data accessible by the IP infrastructure, suitable modification is necessary to the proposed stack shown in Fig. 1. The MAC layer allows the maximum size of the data packet to be of 127 octets, whereas IPv6 packets will be at minimum 1280 octets. So an adaptation layer is introduced in the Fig. 2 as per [17], between the network layer and the link layer to perform the fragmentation of the datagram from the network (IP) layer. The TCP/UDP layers are introduced to make the stack accessible by the existing IP infrastructure. TCP has the task of establishing and maintaining the connections between the peer nodes, and UDP provides the unreliable connectivity without concern of overcoming the errors.

During the process, the TCP adds the 20 octets of header; UDP adds 8 octets of header to the upper layer data [18]. To make the stack simple and light weight UDP is considered in the context. The network (IPv6) layer has the responsibility of node address allocation and routing. The IPv6 header added by the network
layer will be 40 octets with 128 bits of source/destination address. By using the header compression techniques the IP header can be reduced considerably, as the eliminated data can be retrieved by the subsequent layers [17]. Thus the amount of data added by the MAC layer will be limited by the addition of these overheads as well as the overheads to be added by the MAC layer. Thus there is a need to introduce an adaptation layer in to the stack which makes the IPv6 based datagram into a format suitable to be carried by the lower layers. Adaptation layer does the data fragmentation during the transmission of ipv6 datagram into smaller sized chunks, and reassembly during the reception of WSN datagram. The address translation from the 128 bit to 64 bit extended address or 16 bit short address as per 802.15.4std are done via stateless auto address configuration, with the assumption that the lower layers and intermediate routers have the capacity to recover the address as proposed in IETF [19].

The link management layer has the responsibility of making the stack accessible by different physical link technologies like Bluetooth, Wi-Fi, Ethernet enabled hardware as an option. The application layer can receive the interrupts from the sensor module directly during critical events. The resource module provides the buffers and queues to be dynamically accessible by each of the layers for their data transmission. The power management layer governs the optimization of power consumption in the stack by controlling the transceiver and microcontroller’s operating states. The transceiver’s additional features like auto CSMA-CA, auto ack transfer, etc., are initialized by the additional features module.

3.1. Power conservative methods

As the main objective here is to implement the WSN stack on to the 802.11 enabled transceiver involving higher power requirements for its operation, measures has to be taken to optimize the power consumption in the stack by suitable modifications. Thus in the following sections few power conservative schemes are discussed.

The protocol stack consisting of different layers will be implemented in a microcontroller and is used in conjunction with a transceiver for trans-reception activities. In order to make the stack more power efficient during data transmission and reception, in this paper a special power conservative method for microcontroller is introduced. Usually it is a common practice to operate the transceiver via few minimum power consuming modes as defined by the manufacturer [20] to save power. But during such operations the microcontroller consumes enough power to drain the battery at the earliest if left untouched. During the time of normal transmission and reception of the data packet, the transmission process between the microcontroller and transceiver is done via SPI, where a set of interrupts between them governs the trans-reception. In this proposal, during this period a sleep state is introduced to the microcontroller between commencement and completion of data transmission and reception process [21, 22]. It is done by designing a separate interrupt module to handle the transmission and reception activities. By this the microcontroller and its different functional units like core, associated clocks, etc., can be shut down (sleep mode) to reduce power consumption.
During the start of frame transmission, the frame from the microcontroller is downloaded into the transceiver by asserting TX_START interrupt as a result the transceiver starts the transmission process with the preamble. When the transceiver is being transmitting the data frames, the core of the microcontroller can be put under sleep mode. As the transceiver (802.11b/g/n compliant) buffer is large enough to hold multiple 802.15.4 based PDUs, data transfer can be fastened. At the end of data transmission the transceiver invokes the microcontroller using TX_END interrupt as shown in Fig. 3.

Similarly during the reception of data from the transceiver into the microcontroller upward into the protocol stack, the packets are received by the transceiver registers and then uploaded into the microcontroller by using an interrupt RX_START; till the occurrence of this event the microcontroller can be under sleep mode. The SPI which is responsible for the communication between the transceiver and microcontroller has to be active during the process. By this the amount of power consumption by the microcontroller and associated peripherals can be reduced.

### 3.2. Power efficient range selection

As per this scheme the transmitting node uses few predefined dummy data frames as soon as the formation of the network to know the receiver response. These dummy bits are transmitted in bursts with the varying power levels as shown in Fig. 4, in an order by the initiating node. The receiver on receiving each of these bit streams notices the LQI value and also calculates the BER. Based on the best values of LQI and BER, receiver sends the acknowledgement along with this report. On receiving this, the transmitter configures its network database with the receiving node id and corresponding transmission power for future transmissions.

The Network information base (NIB) of the network layer which contains the mapping table of LQI values and transmission power based on the distance is used to derive the optimized power levels. This eliminates the need for transmission of data with high power for closer immobile nodes and with less power for distant nodes by optimizing the transmission power.
When the node moves to a new location from the current configuration, it performs the similar procedure to inform the coordinator about its transmission power, thus the distance. On receiving the ACK, it configures its network table for its future communications with in the network.

The performance of this scheme is also enhanced due to the reason that the ACK frame is received by all the nodes which are already associated under the same coordinator to extract this information to update their respective network data bases. This helps all the surrounding nodes to adjust their transmission power to avoid interference. This is done on a separate time slot of the beacon duration which is reserved for the purpose of network information update.

As soon as the network formation with a node or configurable number of nodes, the coordinator selects a time slot for the exchange of this network data base. The selection of this time slots can be invoked by the application as per the requirement at configurable intervals by considering the network growth.

### 3.3. Addressing scheme

In this section, a new node addressing and deployment scheme is discussed to overcome the excess power consumption during data routing in the network. During the design of a protocol stack, to make the overall system power conservative it is essential to optimize the power consumption at each layer of the stack. At the network layer as the addressing of the nodes and information routing are the main objectives, the protocols designed for this purpose has to be made efficient in terms of power consumption, timing requirement, and resource consumption.

In IEEE 802.15.4 based network, the coordinator provides a 16 bit address to each of its associated child nodes during the formation of the network [1] which are called as short address, also it can assign 64 bit address to the nodes (un associated) for their communication with the coordinator as the extended address to facilitate data transfer in the network.

In the existing addressing protocols as used in zigbee [11], which is for tree (cluster) based network topology, the network can grow only up to certain depth and it doesn’t support the addition of router nodes in future in an adhoc manner. Here the addresses are assigned during the initial phase of network formation by
considering the current existing nodes in a pre defined manner but not by considering the physical area coverage. Even though the scheme promises the reservation of addresses at different depths for additional nodes, there is no guarantee of utilizing them in future. So most of the time addresses will remain unused in the network at the closer depths from the coordinator, thus limits the network growth as the addresses have already exhausted. In stateful address algorithms [23] there will be huge overhead on the coordinator as it has to keep track of all other node’s address table. In case of stateless address algorithms [12] the addresses are allocated dynamically without considering these overheads. Also in some of the schemes as in [12], the network growth is made directional, by allowing the parent to have two child nodes at each layer next to them. In all these algorithms there is a need of compromise between the network growth and ease of address allocation. Thus the routing of information may not be efficient and may take un-optimized paths during its travel towards the destination node.

By considering all these issues of the existing algorithm here proposed a new addressing scheme. This precedes assigning of required number of nodes at any location from the coordinator. Once the nodes are assigned at suitable locations from the coordinator to cover a geographical region based on their physical coverage range, the addresses are allocated based on the derived formulae.

The coordinator estimates the number of routers required at any level to cover a region based on the physical coverage range of the nodes and thus optimizes their number in that particular level. Thus by assigning the required number of routers at every layer from the PAN coordinator to cover all the directions efficiently; eliminates the need for the addition of further routers at the region where the address has already allocated. This also enables the possibility of having an adhoc network in terms of direction of network growth by allowing the addition of the nodes based on the area to be covered.

The core of the proposed algorithm is, it covers the entire region around the coordinator at the first layer and then hops to the higher layers to deploy the nodes. During this, the nodes are deployed at the maximum distance from the coordinator to cover a region fully by the minimum number of routers, thus optimizes the process of node deployment. This also makes the address assignment procedure for the deployed nodes easier and flawless.

The proposed addressing scheme consists of two main divisions namely deployment of nodes and addressing the nodes.

### 3.3.1. Node deployment

As per the proposed node deployment scheme, the PAN coordinator deploys the router nodes at the point of its maximum coverage area (range) to cover the highest possible physical distance along the direction of network growth. Once a router node is placed, based on its maximum range, peer router nodes are placed at the same layer from the PAN coordinator. Thus the number of router nodes required around the PAN coordinator to form an omni directional network at any depth is given in the following relation, which allows the user to select the number of routers based on the required depth of the network growth.
During the time of network association itself the PAN coordinator or router node decides the number of nodes required around it in the next layer to allow the network growth in any direction in future to cover the entire physical region. This eliminates the need for inclusion of additional nodes at any time in any layer even in an adhoc network as the existing nodes can cover the entire region. This feature promises the easier and efficient address allocation without wasting many addresses.

Figure 5 shows the scenario of node deployment, where region around the PAN coordinator is placed with router nodes at a uniform distance of ‘r’ and each router maintains a distance of ‘x’ among themselves, which is being their physical coverage range to encircle the PAN coordinator at the first layer of the network.

Here the number of router nodes can be varied according to the required network density as required by the application by using Eq. (1)

The number of routers at a particular layer is

\[ R_n = \frac{2\pi \times \text{range}(r) \times \text{depth}(d)}{\text{range of Router}(x)} \]

(1)

where \( r \), \( x \) and \( d \) respectively represent the vertical range of a node, the horizontal coverage range or distance, and the layer from PAN coordinator.

![Fig. 5. Nodes Deployment Scenario (Spider Web Geometry).](image)

While placing the router nodes at the second layer from the PAN coordinator similar approach is followed. The second layer router nodes will be the child router nodes of the router nodes present in the first layer, which are place at the maximum coverage range ‘r’ from the first layer. To place the end device child nodes of the router nodes in the previous layer, ‘some percentage’ of its coverage range (%) is considered. This means the end devices are placed at a distance ‘p’ from the parent router node; where ‘p’ will be the fraction of its maximum coverage range ‘r’. Thus by varying the value of ‘p’ the child nodes (end device) can be placed at different distances from the parent. This is done with the reason to make the transfer of information from the parent node to its child node at optimum power of transmission and eliminates unnecessary excess power consumption. In this way network can grow by different layers in which the...
routers are placed by the PAN coordinator at the first layer and by the
corresponding layer parent node at the subsequent layers. In this scenario uniform
distribution of the nodes is considered; based on the required network density the
distance of the peer router nodes within the layer from the PAN coordinator can be
assigned. In Fig. 5, 8 router nodes can be placed at a uniform distance ‘r’
(AB) from the PAN coordinator. The distance between the nodes in the router
nodes will be their horizontal range ‘x’ (BD). The second layer router nodes are
placed at a distance of ‘r’ from the first layer nodes, thus the distance (FC) will be
of length ‘2x’ where double the number of nodes in the first layer can be placed
[24, 25]. The child nodes are placed at a distance ‘p’ (DE), which is the fraction
of range(r) of the routers, in the previous layer. The number of child nodes under
a router is assigned based on the required network density. So this scheme of node
deployment will follow spider web pattern.

During the network growth along the subsequent layers, the router/coordinator
nodes in the previous layer will also prefer to place them at the maximum
coverage range(r). Thus it is possible to place router nodes which will be
increasing as the multiples of the number of router nodes in the first layer.

Any node wishing to join as a reduced function device (RFD) or as an end
device must indicate this during the time of association. These nodes are placed as
child nodes at that particular layer under a router node using the child node
deployment procedure to conserve power.

The maximum number of child nodes/end devices under as a router node is

\[ C_m(d) = \frac{2\pi([d-1]+\text{fraction } \times \text{range(r)})}{\text{range(x)}} \text{ for } d \geq 2 \]  

This scheme limits the maximum number of child nodes under a router at any
layer during the time of association itself. The reason for imposing such a
restriction is to make the addressing scheme effective and easier else the addition
of child devices at any time under a router necessitates reserving of some
addresses which may leave unfilled space in future; or to eliminate need of re-
assignment of addresses from the beginning.

Even though the child nodes can be placed at a distance of maximum coverage
range of the router node, by considering end devices role as they have limited
capability and responsibility in a network structure they are made to reach at
minimum power of transmission. So they are placed at a fraction of router node’s
coverage range, \( p \) (preferably 50%) between the current and the next layer. The
term fraction of range (\( p \)) can be set according to the requirement to save power
and expected child nodes.

Thus the total number of nodes at any particular level is the sum of router
nodes and the child nodes in that particular layer.

Total nodes at any layer is

\[ \text{Total Nodes} = R_N + C_m \Rightarrow \frac{2\pi d}{\text{range of router (x)}} + C_m \times R_N(d) \text{ for } d \geq 1 \]  

The maximum number of child nodes under a router node can also be
configured to a pre fixed value (Cm) based on the required density to cover a
region, thus total number of nodes at any layer will be as shown in Eq. (4) and in the proposed addressing scheme this method is followed.

\[ C_{mT(d)} = R_{N(d)} \times C_m \quad \text{for } d \geq 1 \]  

(4)

3.3.2. Address assignment

Once the nodes are placed as per the proposed node deployment scheme, the nodes are assigned with addresses starting from the PAN coordinator level. During the address assignment along the layers, the router nodes at a layer are given with the minimum address within the range allocated for that particular layer along clockwise/anti clockwise direction based on the requirement. Its child end device nodes are addressed after the address assignment of the router nodes in the next layer. The range of addresses for any layer from the PAN coordinator can be calculated based on the formula (5); i.e., once all the nodes in the first layer \(d_1\) are assigned with the addresses, then the next layer \(d_2\) router nodes are assigned with addresses, the child nodes (end device) of the router nodes in the first layer \(d_1\) are provided with the highest range of addresses (remaining) which are reserved for the second layer \(d_2\). The same procedure is carried out in the subsequent layers from the PAN coordinator. In this scheme the PAN coordinator is not allowed to have any child node acting as end devices to enhance the performance by allowing more routers to associate to expand the network.

The range of address at any layer \(d\) is;

\[
\begin{align*}
A_{\text{start}}(d_k) & = \sum_{n=1}^{k-1} R_N \times n + 1; \\
A_{\text{End}}(d_k) & = \sum_{n=1}^{k} R_N \times n + \sum_{n=1}^{k-1} C_m \times R_N \times n; \quad \text{for } K = 2 \\
A_{\text{start}}(d_k) & = \sum_{n=1}^{k-1} R_N \times n + \sum_{n=1}^{k-2} C_m \times R_N \times n + 1; \\
A_{\text{End}}(d_k) & = \sum_{n=1}^{k} R_N \times n + \sum_{n=1}^{k-1} C_m \times R_N \times n; \quad \text{for } K \geq 3
\end{align*}
\]  

(5)

The PAN coordinator is given with the starting address of ‘0’ followed by the routers at each upcoming layer. As all the address gets exhausted, address assignment can be repeated starting from a pre-defined address range.

3.4. Block acknowledge transfer

In case of IEEE 802.15.4 based networks, the transmission of each data packet will be acknowledged by the receiver separately. This leads to excess power consumption due to separate transmissions and addition of physical layer overhead even though the acknowledgment packets are of smaller size. The IEEE 802.11 standard offers a feature of continuous transmission of data packets without being interrupted by the acknowledgement from the receiver, in turn the acknowledgement packets are received as a single block of data; thus avoiding the addition of physical overhead separately for each acknowledgment packets. This feature is the block acknowledgment transmission as defined in [6]. This feature
of the dot 11 physical layer is exploited here to transmit the WSN packets. As per the beacon interval of IEEE 802.15.4 standard, the nodes contend for the channel using cama-ca during the contention access period (CAP) of the beacon frame and occupy the free slot for transmission; the occupied slot will be sufficiently large for the transmission of multiple frames. During the contention free period of the beacon (CFP) nodes can get reserved slots for the communication. This has to be acquired by the nodes on prior request during the start of beacon frame by the method of guaranteed slots, i.e., (GTS) [1].

In the proposed method these GTS slots are utilized for the reception of block of acknowledgements from the receiver. In this way nodes can receive the block acknowledgment for all the transmissions done during the contention access period.

The acknowledgement frame as per IEEE 802.15.4 standard is 5 octets in length consisting of frame control field (FCF) of 2 octet, Sequence number of 1 octet, frame check sequence field (FCS) of 1 octet when added by the MAC layer. The Physical layer adds PHY overhead as Preamble field of 4 octets, start frame delimiter of 1 octet, physical packet length of 1 octet. Thus the acknowledgement frame will be of total 11 octets when transmitted by the hardware [1]. In a wireless environment reliable data transfer between the nodes depends on several factors like transmission power, receiver sensitivity, bit error rate, signal to noise rate, surrounding interference, channel access method, etc. So it is essential to include the acknowledgement to confirm about the data delivery. But in case of data streams which require to be transmitted as multiple fragments, acknowledging each of these individual frames will be a heavy task; because in such case each transmission involves the addition of overhead by the PHY layer separately and consumes excess power

So in the proposed method by using the 802.11 enabled transceiver, the block acknowledgement feature is introduced to conserve power. This special feature is initialized by the MAC layer of the proposed stack, which invokes the hardware to perform the above stated activity. This feature is useful while transferring large amount of data belonging to a single event. These blocks are transmitted during the guaranteed time slots (GTS) of contention free period.

For some of the applications where large amount of data has to be transferred like in IP enabled WSN stack, the data frame has to be converted into smaller fragments by the adaptation layer [17]. In this scenario all the fragments are acknowledged by the receiver in the form of a block consisting of sequence numbers for all the successfully transmitted fragments.

In a general scenario if the acknowledgement has to be transmitted separately for ‘n’ packets the physical layer adds the overhead ‘n’ times. If block acknowledgement is used then the physical layer adds the overhead once as it involves single block transfer of comparatively higher duration. The following relation shows the time duration for the acknowledgement transmission separately and in the form of block acknowledgement data transfers.

Time duration of a data transmission and reception of the Ack frame:

\[ T_{Tx} = Data\_Tx\_Time + Turnaround + Phy\_overhead + Ack\_duration + SIFS\_Duration \]

For “n” data transmission it will be

\[ n \times T_{Tx} \]  \hspace{1cm} (6) \]
by using Block ack transfer, duration for “n” data transmission and ack reception:

\[
\text{Duration} = (\text{Data_Tx_Time} + \text{Unit_gap}) \times n + \text{SIFS} + \text{Phy_overhead} + (n\times \text{Unit_Ack.duration})
\]

Figure 6 shows the arrangement of data frames during block ack transfer scenario. For different fragments of a single protocol data unit (PDU) a common block acknowledgement is transmitted by the receiver. The sequence number field of all the fragments remains the same and the fragment number field is incremented at every transmission. In the acknowledgement block the fragment numbers are indicated for the correctly received ones. During the reception of the fragments by the receiver, the Link quality (LQI) value is noted and if it is below the threshold value for a particular fragment, then the ack frame corresponding to it is sent immediately inferring retransmission. Based on the buffer size of the transceiver, the maximum size of the fragment can be decided; all the fragments must be of same size except the last one, which may be lesser than the maximum size. Between each fragments a minimum time gap (unit gap) is maintained to prevent the overlap. All these transmission takes place during the contention access period of a beacon frame. The reception of the ack frame takes place in the GTS slots; if the provided slot is insufficient due to excess long transmissions, then the reception can be resumed in the next available GTS slot for the node. After the transmission of all the fragments and before the start of reception of the Ack blocks an Inter frame spacing duration is provided (SIFS) as per the 802.11 standard regulations.

![Fig. 6. Block Acknowledgement Transmission Scenario.](image)

**Algorithm for implementation of BlockAck scheme**

1. **Begin**
2. Perform scan – cx and also obtain slot for fragment (data) transmission
3. Obtain CTS for the reception of BlockAck frame by CTS _Be got Transmitter
4. Transmit data fragments with Unit_gap in between the fragments
5. Measure LQI of each received packet
6. If LQI < Threshold:
   - Accept ACK during CTS
7. **End**

**Journal of Engineering Science and Technology**
October 2013, Vol. 8(5)
3.5. Enhanced data rate

In video surveillance applications of WSN stack, the amount of data to be transmitted will be large; which has to be transmitted at a higher data rate to complete the data transfer within the specified time. So in this paper the IEEE 802.11 enabled transceiver is used to offer higher data rate than the usual 802.15.4 based transceivers for WSN applications. As per 802.11 standards the physical layer adds the overhead as PLCP preamble and PLCP header to every frame during transmission, consisting of Synchronization field of 8 octets, SFD field of 2 octets in the preamble; PLW field of 12 bits representing the data size in octets as transmitted by the MAC layer, PSF field of 4 bits enabling the variable data rate selection, HEC field of 16 bits representing the error checking bits in the header field of PLCP frame format [6]. The subfield as PSF, allows the configuration of data rate as per the requirement varying from 1.0 Mbps to 4.5 Mbps in increments of 0.5 Mbps in a general scenario. This feature of the 802.11 based hardware makes it suitable to carry the WSN data.

The proposed hardware here for the implementation is microchip MRF24WB0MB as transceiver along with the microchip PIC24FJ128GA010 family 16 bit flash microcontroller, which communicates to each other via SPI. In most of the low power 802.11 based modules [7-9] which are SoC, the specifications of microcontroller or transceiver hardware are not separately mentioned from the point of development or modification of the existing solutions as they are proprietary. So in order to explore the features of the hardware and to utilize the features of the proposed stack the microcontroller and transceiver are separately chosen even though SoC are readily available.

The Microchip MRF24WB0MB [5] is a 2.4 GHz, 802.11b/g/n compatible transceiver consists of few power saving modes like hibernate (0.1μA), sleep (250 μA), rx_mode (85 mA), tx_mode (154 mA), and standby to optimize the power consumption during various transmission and reception activities. It offers a data rate of 1-2 Mbps, DSSS modulation, RSSI measurement capability, and a physical range of 400 mts. It is compatible with 16 bit microchip PIC24FJ128GA010 microcontroller [22] via 4 wires SPI for efficient stack and transceiver communication. The microcontroller consists of 16-bit modified Harvard architecture, SPI, UART, Interrupts, timers, 128KB flash memory.

While implementing the stack on this hardware by considering its capabilities, it is essential to determine the performance of the same. Thus in the following sections, few scenarios are described to evaluate the hardware performance. By considering the different operating states of the transceiver, their power consumption, transition times among the states; csma ca scheme for the transmission of a data frame and reception of the acknowledgement is performed for the proposed microchip MRF24WB0MB transceiver. This is done based on the CSMA-CA protocol guidelines specified in [1, 26]. The different states of the protocol are effectively implemented by utilizing the various operating modes of the transceiver. The various states in the CSMA-CA protocol are sketched in Fig. 7.

While implementing the protocol using the transceiver, it is essential to monitor the power requirement of the different operating modes of the transceiver and effective switching between the modes. This scheme is also compared with an 802.15.4 enabled transceiver, i.e., Atmel RF230 [20], by considering its power consumption and various operating modes. The different operating modes
supported by RF230 transceiver and respective current consumptions are trx_off (1.5 mA), PLL_on (7.8 mA), Rx_on (15.5 mA), Busy_tx (16.5 mA), busy_rx (15.2 mA), and sleep (0.02 µA).

Fig. 7. CSMA-CA Scheme in IEEE 802.15.4.

Here the CSMA-CA protocol is used for the transmission of data packets and reception of the ack frame. This activity is done by both the transceivers separately to measure their parameters. The scenario is simulated for ‘n’ number of nodes for multiple times and power efficiency of the transceiver is plotted. The power efficiency is little higher for the 802.11 based microchip transceiver than the 802.15.4 based RF 230 due to the availability of higher buffer and as a result lesser number of transmission for the same amount of data. As the number of nodes increases the power efficiency of the transceiver reduces due to collisions. The performance of both the transceivers is shown in Figs. 8 (a) and (b).

Fig. 8(a) CSMA-CA using 802.11 Transceiver.

Fig. 8(b) CSMA-CA using 802.15.4 Transceiver.
As the 802.11 hardware is configured for higher data rate of 2 Mbps as compared to the 802.15.4 enabled transceiver of 250 kbps, the data from the MAC layer can be pre downloaded and made ready to be transmitted in a 802.11 transceiver at 4µs/octet; against 32µs/octet in the later. This enables the faster data transmission as shown in Fig. 9, for different packet length.

The buffer size available in the transceivers is 4095 octets for 802.11, and 127 octets for 802.15.4. Thus the large amount of data emerging in the applications like video surveillance applications will be of size 2-4KB can be easily transmitted at minimum number of transmissions in an IEEE 802.11 based transceiver as shown in Fig. 10. Up to data size of 4KB an 802.11 transceiver needs a single transmission whereas 802.15.4 hardware needs around 26 transmissions. By considering the overhead added by the hardware and the transmission power consumption details, the plot is generated. In this plot the power consumption of both the transceivers during the direct transmission, i.e., without performing CSMA-CA is considered.

![Data transmission time](image1)

**Fig. 9. Data Transmission Time for the Transceivers.**

![Power consumption](image2)

**Fig. 10. Power Consumption by the Transceivers.**
4. Conclusions

The proposed scheme of implementation of the WSN communication protocol on 802.11 compliant transceiver is effective as the hardware offers higher data rate, higher bandwidth. Thus it also enables faster data transfer, even though the transceiver consumes excess power than the usual 802.15.4 based hardware. So the natural need of power conservation is satisfied in this proposal by some of the power conservative schemes like node deployment and addressing, which eliminates the redundancy in node deployment by prefixing the nodes at the maximum distances of coverage. Thus makes the addressing process much simpler as the locations of the nodes are already available; and effective in terms of not wasting the addresses. This also enables the routing process without much energy consumption for end device child nodes.

The power conservative range selection method enables the nodes to transmit the data with the optimum power by pre knowing the receiver distances using the trail data sequences and exchanging the information between the peers. To conserve the power by the microcontroller, the sleep states are introduced for the microcontroller during the time between the transmission and reception where microcontroller is not being used.

The block acknowledgement feature of the 802.11 standard has been utilized in the WSN protocol stack to reduce the power consumption for multiple acknowledgement transfers, and combining the acknowledgements within a single transmission. This reduces the amount of overhead added by the hardware in terms of preamble. Thus by these modifications into the IEEE 802.15.4 based WSN protocol stack, when implemented on 802.11 hardware makes it suitable for effective and power efficient communication.

References

15. Contiki 2.2.1. (2010). 6LoWPAN implementation data sheet, SICS.