ISSN No. 0976-5697

Volume 5, No. 1, Jan-Feb 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Wireless Sensor Networks – Sensor Node Architecture and Design Challenges

Roxanne Hawi
Student Masters in Computer Systems
Department ICS
JKUAT-Westlands Campus Nairobi, Kenya
roxannehawi@gmail.com

Abstract: Advancements in microelectronics and semi-conductor technologies have been a major contributor in the embracement of wireless sensor networks (WSN). They have enabled the development of more flexible, smaller and cheaper sensing devices that still have sufficient processing power, storage capabilities, memory and communication capabilities to carry out their dedicated purpose effectively. However, the characteristics of WSNs such as: resource-constrained small form factor of the sensor nodes, wireless communication and unattended harsh operating environments; makes designing a reliable and efficient WSN quite formidable. This paper presents an overview of the WSN architecture and a comprehensive discussion on some of the major design challenges WSNs designers encounter during implementation.

Keywords: Wireless sensor network; sensor architecture; radio frequency; WSN design challenges; wireless security

I. INTRODUCTION

The constant advancement in technology has greatly influenced adoption of wireless communication in not only the IT world but also social, business, government, health care sectors and many more. In particular, advancements in very large scale integration (VLSI) and semiconductor technologies have been a major contributor in the embracement of distributed sensor systems; for example, they have enabled the development of microprocessors with increased processing capabilities while at the same time shrinking the size of the processors. This miniaturization of computing and sensing technologies enables the development of tiny, low power, and inexpensive sensors, actuators, and controllers [1].

A *sensor* is a device that gathers information from the environment in which it is placed (e.g. entrance door of a building) into digital signals which can be processed and analyzed. An example could be a CCTV camera at the entrance of a building door that captures images and enables monitoring of people entering and leaving the building. A *sensor network* is a heterogeneous system combining tiny sensor nodes placed at different points geographically in order to monitor and collect/gather data; often than not sensor data e.g. when a door is opened or closed and transmit the data to the centralized processing station; (It is heterogeneous since it consists of sensor nodes with different functionalities and capabilities depending on the environment they operate in).

Most sensor networks comprise of hundreds or even thousands of sensor nodes, often deployed in inaccessible and or remote areas. For this reason wireless sensor networks (WSN) come in handy in such situations, seeing that it is difficult and near impossible to wire all the distributed sensors. When many sensors cooperatively monitor large physical environments, they form a *wireless sensor network* [1]. Due to the fact that wireless sensors not only communicate with the base station but also with each other; in addition to the sensing component, they also possess their own processing, communication and storage capabilities.

However just like with other distributed systems, implementation of WSN comes with its fair share of challenges and constraints which impact the design of a wireless sensor network, which will be discussed in section III of this article. Firstly, we look at the basic architecture of a sensor node in a WSN.

II. ARCHITECTURE OF A SENSOR NODE

The crown of any WSN is the wireless sensor node. Sensing, processing, and communication take place through the node. The quality, size and frequency of the sensed data that can be extracted from the network are influenced by the physical resources available to the node [1].

The main design objectives of a sensor node focus on economic viability, increased flexibility (to ease process of deployment and blending into its environment) and conserve energy (limited processing, communication, memory and storage capabilities).

The sensor node consists of four subsystems namely; sensing, processing, communication and power supply. The *processor subsystem* is the cerebral part of the node, responsible for processing and storing collected data. The *sensing subsystem* gathers data from the environment (using sensors) and converts the data from analog to digital signals (using analog to digital converter (ADC)). *Communication subsystem* is responsible for providing a communication channel from one node to another node in the network (using a transceiver). Lastly, the *power supply subsystem* is responsible for providing energy to the nodes (using a battery). Figure 1 below shows the basic interaction between the four subsystems

A. Power supply subsystem:

This unit provides energy to the sensor nodes. Typically the battery is the core element used to power the sensors.

a. Batteries: They can either be replaced or recharged. For the non-rechargeable batteries they are disposed once their energy is depleted. For this reason, to manage cost of replacing them, they are built to have a high energy density meaning they can store more energy – so as to last longer. The rechargeable batteries can be reenergized using for instance, solar power.

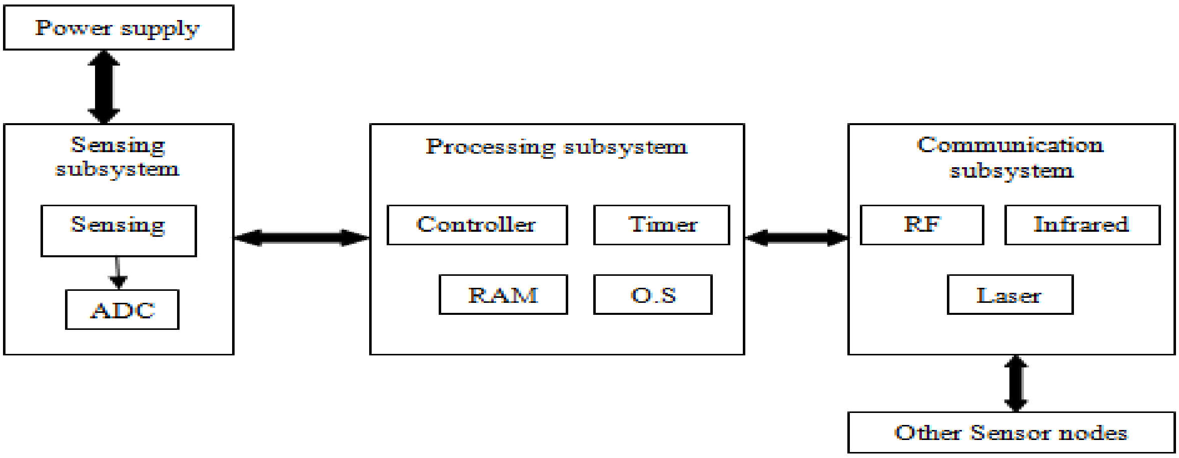

Figure: 1 Sensor Node Architecture

B. *Processing Subsystem:*

According to Figure 1 above, this unit comprises of RAM, controller, operating system (O.S) and timer, responsible for storing, processing and executing events respectively. The processor subsystem is the central element of the node and the choice of a processor determines the trade-off between flexibility and efficiency – in terms of both energy and performance [1]. In other words it is the unit that determines energy consumption as well as the computational capabilities of a node.

There is a variety of processor options (each having its own set of benefits and drawbacks): microcontrollers, digital signal processor, application-specific integrated circuits and field programmable gate arrays (FPGAs). Most commonly used processor in sensor nodes is the microcontroller.

a. ***Microcontroller***: It is a general purpose processor. As a result, design and implementation process is not as costly and complex as the other processor options, it is able to support dynamic code installations and updates of software running on wireless sensor nodes which occasionally require modifications or remote debugging. Such tasks require a considerable amount of computation and processing space at runtime, in which case, special-purpose, energy-efficient processors are not suitable [1].

b. ***Timer/Clock***: Microcontrollers need clocks so that our programs can be executed in rhythm with the clock [3]. Instructions are executed in sync with the ticks of the clock/timer. For instance timers come in handy when sensors receive pulse width modulation (PWM) signals. A Pulse Width Modulation (PWM) Signal is one way to represent an analog signal in the digital domain [4]. They can be used to control mechanical objects such as valves, pumps, hydraulics among others.

c. ***Operating System (O.S)***: Its main task is to enable applications to interact with hardware resources, to schedule and prioritize tasks, and to arbitrate between contending applications and services that try to seize resources [1]. In WSN, a multitasking O.S would be the ideal choice. For example, in a wireless sensor node, the processor subsystem may interact with the communication subsystem while aggregating data that arrive from the sensing subsystem [1]. However, this multitasking function would require a lot of memory to manage concurrent processing of tasks – which most existing sensors cannot handle due to limited resources. TinyOS is the most familiar operating system in sensor network which is event driven and calls the appropriate event handler for execution [2].

d. ***RAM***: this is a volatile internal memory used for data storage. (Flash memory (ROM) can also be used for storing basic program codes). Choosing the appropriate memory size is crucial in that it can affect overall cost of node as well as power consumption.

C. *Sensing subsystem:*

This comprises of the physical sensors and analog-to-digital converters (ADC). It acts as the interface between the physical environment and virtual world, i.e. collecting data from the environment and converting this data from analog to digital signals for smooth processing.

a. ***Sensor***: Basically a sensor is device that senses physical phenomenon such as pressure, motion, speed etc and transform it into analog signal [2] using a transducer. A WSN integrates a large number of sensor nodes with each node containing one or more sensors depending on the application area. There is a variety of sensor types that can be employed in WSNs. An example of sensor classification is active and passive sensors. *Active sensors* supply, or send out, their own electromagnetic energy and then record what comes back to them [5]. That is, they must emit some kind of energy (e.g., microwaves, light, sound) to trigger a response or to detect a change in the energy of the transmitted signal [1]. Radar is an example of such a sensor. Alternatively, *passive sensors* detect naturally radiated or reflected energy from its surroundings and draw out their power from this energy input. Thermometers are a good illustration of a passive sensor.

b. ***Analog-to-Digital Converter (ADC):*** The output of a sensor is an analog signal. This means there needs to be an interface between the sensor and the digital processor (microcontroller). The analog-to-digital converter (ADC) converts the output of a sensor –

which is a continuous, analog signal into a digital signal [1].

D. Communication or Transceiver subsystem:

This unit is responsible for handling data transfer between the subsystems of a wireless sensor node. It facilitates conversations between all the subcomponents of the sensor node and the processor as well as node to node interactions.

a. ***Transceiver*****:** this is a device that operates as both a transmitter and a receiver. It receives instructions/commands from the processor and transmits internally to other subsystems within the node or to other nodes in the network. The communication subsystem is the most energy intensive subsystem and its power consumption should be regulated [1]. As a result most transceivers provide a functionality to interchange between operation states (i.e. active, idle and sleep states) in an attempt to regulate usage of resources.

As seen in Fig. 1 above; WSNs can use a variety of wireless transmission media for communication, such as:

a. ***Radio Frequency (RF)*****:** This entails transmission of data using specific radio frequencies. RF is a term that refers to alternating current (AC) having characteristics such that, if the current is input to an antenna, an electromagnetic field is generated suitable for wireless broad casting and/or communications[7]. It is the most common transmission media that is used by WSN applications. Communication in WSN nodes mostly uses IEEE 802.11 standards. Where IEEE802.11 is a set of standard used for WLAN computer and communication is carried out at 2.4, 3.6 and 5GHZ frequency bands [2].

b. ***Infrared*****:** It is bi-directional, however, for communication to take place the sensor nodes have to be aligned within a plane. Needs no antenna but it is limited in its broadcasting capacity [6], short range of about 1 metre distance. A practical analogy to describe how sensors that use infrared technology for communication operate is television remote control units.

c. **Laser (optical communication):** telecommunication system in which transmitter converts signal into optical form at sender side and then converts optical signal into original signal at receiver side [2]. Require less energy, but need line-of-sight for communication and are sensitive to atmospheric conditions [6].

III. DESIGN CONSTRAINTS OF A WSN

The primary objective of wireless sensor network is to implement, smaller, cheaper as well as more efficient devices. Driven by the need to execute dedicated applications with little energy consumption, typical sensor nodes have the processing speeds and storage capacities of computer systems from several decades ago [1]. These constraints impact the overall design of a WSN. Working with these limited resources while at the same time ensuring efficiency comes with its fair share of challenges to WSN designers. Some (but not all) of the most common design challenges include:

A. Energy efficiency:

Sensors are microelectronic devices; this means that they operate on a limited energy budget hence the need to regulate their energy consumption. They are typically powered through batteries as mentioned in section II above. Ideally the battery life should match up to the mission time (i.e. duration of the task the sensor is meant to operate on), however there are some tasks that use up more energy than expected especially the communication subsystem. Mentioned below are just but a few of the challenges that designers face when trying to regulate energy consumption:

a. ***Switching states*****:** To control the power usage during communication, transceivers are designed to have states: active, idle and sleep states. Where active is when the nodes are receiving and transmitting, idle is when the sensor is on but not transmitting or receiving any data and sleep state is when the sensor is off. Designers thus have the task of deciding how and when it is appropriate to implement each state in order to conserve energy and still maintain network efficiency For instance if node 1 wants to send data to node 2, but node 2 is in sleep state this might cause some communication/network disruptions. Also [6] most transceivers operating in idle mode have power consumption almost equal to the power consumed in receive mode. Thus, it is better to completely shut down the transceiver rather than leave it in the idle mode when it is not transmitting or receiving. A significant amount of power is consumed when switching from sleep mode to transmit mode in order to transmit a packet.

b. ***Rechargeable vs Non-rechargeable batteries*****:** Whether the battery can be recharged or not significantly affects the strategy applied to energy consumption [1]. If the sensors operate in harsh environmental conditions which makes it difficult and or impossible to change the battery or replace the sensor, then it would be advisable to use rechargeable batteries such as solar panels – which recharge themselves. However, rechargeable batteries are more expensive than disposable ones; this means the WSN designers will have to make the difficult decision of a trade-off between cost and energy consumption (and overall network reliability – in the event that energy in disposable batteries is likely to get depleted before task completion hence disrupting sensor operations in the network).

B. Real time:

WSN interact with real world environments and more often than not sensor data must be delivered within specific time constraints for the information to remain relevant (i.e. appropriate observations can be derived from the data). An example of a sensor application based on time is the fire detection systems.

However, achieving real-time in WSN is quite difficult due to some common network issues, such as; congestion and noise (seeing that most WSN use free licence radio frequencies that are shared by many other networks) which could lead to lost and or distorted messages as well us disrupted communication. Another issue is the transient behaviour of the sensor networks (where system lifetime and robustness keep being extended overtime – no fixed topology), and this makes it taxing to constantly keep up with these changes in real-time.

While there are a few results that exist for ensuring real time in WSNs, [8] most protocols either ignore real-time or simply attempt to process as fast as possible and hope that this speed is sufficient to meet deadlines. Thus, it is important for the designers to develop real time protocols; [8] that deal with the realities of WSN such as lost messages, noise and congestion. This poses a challenge since very few results exist to date regarding meeting real time requirements in WSN.

To date the limited results that have appeared for WSN regarding real time issues have been in routing [8]. There are a few routing protocols proposed to address this issue:

- ***a.*** ***RAP protocol***: proposes a new policy called velocity monotonic scheduling. Here the packet has a deadline and a distance to travel. Using these parameters a packet’s average velocity requirement is computed and at each hop packets are scheduled for transmission based on the highest velocity requirement of any packets at this node. While this protocol addresses real-time, no guarantees are given. [8]
- ***b.*** ***SPEED***: This protocol uses feedback control to guarantee that each node maintains an average delay for packets transiting a node. Given this delay and the distance to travel (in hops), it can be determined if a packet meets its deadline (in steady state). [8]

It is not enough to just develop real time protocols, designers of WSN need to also come up with the corresponding analysis techniques. For instance; [8] dealing with real-time usually identifies the need for differentiated services, e.g., routing solutions need to support different classes of traffic; guarantees for the important traffic and less support for unimportant traffic. (Hence there is a need to analyse the traffic in a WSN).

C. Wireless Networking:

The reliance on wireless networks and communication poses a number of challenges to a sensor network designer [1]. The wireless medium is considerably vulnerable to noisy environments. For instance it is easier for an attacker to interfere with a wireless network than a wired one and cause noise that consequently affects communication; the fact that WSNs are infrastructure-less means that nodes can communicate directly with base station hence if the attacker gets access to a specific node then this provides direct access to data centre. Sharing of unlicensed frequencies with other networks also contributes to a noisy environment. Another factor that affects wireless medium is attenuation of signals, whereby, the radio signal strength weakens as it propagates through the network. Attenuation of an RF signal can be expressed using the *inverse square law*; which states that, [1] the received power P_r is proportional to the inverse of the square of the distance d from the source of the signal. In other words the further an object is from the source (e.g. sensor node it is communicating with) the weaker the signal it receives. The equation can be summarised as:

$$P_r \propto \frac{1}{d^2}$$

Such that,[9] if the separation distance is doubled (increased by a factor of 2), then the signal is decreased by a factor of four (2 raised to the second power). And if the separation distance is tripled (increased by a factor of 3), then the signal is decreased by a factor of nine (3 raised to the second power).

Thus as described above, it is evident that an increase in the distance between a node and a base station will trigger the need to use more transmission power. Thus, in the design of WSN, short range transmission should be considered, in order to reduce eavesdropping, attenuation as well as minimize power consumption during transmission.

However, in an attempt to make the network more energy efficient by splitting up large distances between nodes into several shorter distances, WSN designers are faced by yet another challenge. Supporting of *multi-hop* communications and routing [1].

In multi-hop communication the sensor nodes serve as relays for other sensor nodes, and must cooperate with each other to find the most efficient route to transmit sensor data towards the base station. This *routing* problem, that is, the task of finding a multi-hop path from a sensor node to the base station, is one of the most important challenges and has received immense attention from the research community [1]. This challenge is especially experienced in networks that use switching techniques (i.e. switching between idle, active and sleep states) to conserve power. In such networks, the sensor nodes are switched off when not in operation. As a consequence, during these down-times, the sensor node cannot receive messages from its neighbours nor can it serve as a relay for other sensors [1]. Some strategies have been developed which the WSN designers can use to resolve this issue:

- ***a.*** ***Wakeup on demand strategy*** [1], which requires the sensor nodes to switch to active state when need arises.
- ***b.*** ***Adaptive duty cycling strategy,*** when not all nodes are allowed to sleep at the same time. Instead, a subset of the nodes in a network remains active to form a network backbone. [1]

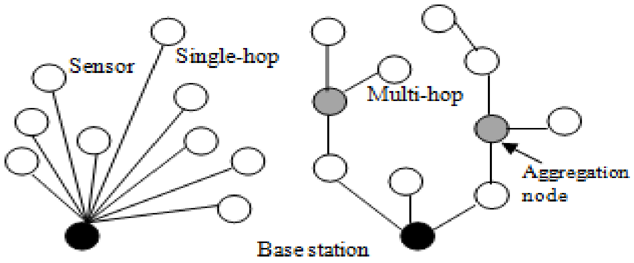

Figure 2: Single-hop and Multi-hop communication

D. Self management:

Most sensor networks operate in harsh and remote areas where human permeability is very difficult, dangerous or impossible. So that, the nodes are deployed in an ad hoc manner, for example, sensors serving disaster areas could be deployed from aeroplanes to cover the areas of interest for monitoring. This means that maintenance and repair, as well as infrastructure support will be unlikely. For this reason, sensor nodes should be *autonomous*, [1] in that they configure themselves, operate and collaborate with other nodes, and adapt to failures, changes in the environment, and changes in the environmental stimuli without human intervention.

Therefore, for the WSN designer the challenge is ensuring that the network is self organizing, self optimizing, self protecting and has the ability to self heal without incurring energy consumption overheads.

- ***a.*** ***Self-organizing*****:** this is the ability of the sensor to configure and setup itself in the new environment it is deployed in, establish connections with its neighbouring nodes so as to initiate its sensing responsibilities. For instance, a node should be able to adapt to addition of new nodes or be able to reconfigure itself in case a node it was communicating with in the network fails.
- ***b.*** ***Self-optimizing*****:** ability of the node to manage and monitor the usage of its resources to maintain highest level of efficiency possible. For instance know when to switch from active state and to sleep state in order to conserve energy.
- ***c.*** ***Self-protecting*****:** ability of the sensor node to shield itself from attacks (both environmental e.g. Harsh weather conditions or system attacks e.g. unauthorized access to its data).
- ***d.*** *Self-healing*: ability to diagnose and recover from its own failures or network disruptions.

E. Decentralised management:

While centralized management results in more optimal algorithms for network management such as routing solutions or topology control; the dynamic nature, large scale deployment and limited energy resources of WSN make it impractical to use centralized algorithms – this is because [1] the overhead can be significant, particularly if the topology changes frequently, as is the case in WSNs. For instance, in this centralised approach, the base station (act as the network controller) will have to keep reconfiguring the location coordinates for each node and relaying the information to the other sensors each time the topology changes.

Sensor nodes in WSN are normally deployed in an ad hoc manner meaning they have no global knowledge of the network pre-deployment. For this reason they have to collaborate with neighbouring nodes in order to configure themselves and adapt to the environment accordingly. This is *localization*, whereby sensors cooperate with each other to determine their physical coordinates as well as their spatial relationship with its environment without global knowledge of the network (i.e. a node only has a list of its immediate neighbours and their distances to the base station). This decentralized approach minimises the management overheads especially in the dynamic environment of WSN, the base stations are relinquished of the overburdening and resource straining task of determining the location of all the nodes in the network.

However, when it comes to routing based tasks, decentralized algorithms do not always provide (accurate and) optimal routing solutions; the sensors typically make decisions based on distance, i.e. which node is closest node to forward my packet? Rarely do they consider resource efficiency. On the other hand in centralized approach, since the base station has global knowledge, it is able to analyse entire network and compute most efficient route in terms of distance and or energy (or resource) consumption.

As a result, decentralised management leaves the designers with the challenge of ensuring optimality in terms of routing efficiency as well as manage the limited resource budget without the need to make a trade off between the two.

F. Hardware constraints:

Due to the small physical form of sensors and the lack of advanced hardware features. Designers of WSNs are faced with the challenge of implementing an efficient network (that is capable of operating with high volumetric densities [10]) on resource constrained hardware. Consequently these limitations affect a number of design elements, such as:

- ***a.*** ***Routing*****:** the operating system architecture of sensor nodes has a small memory allocation, for this reason only small amounts of data can be stored in them at a time. This affects the structure of the routing tables in sensors in that, the routing tables mostly have only a list of its neighbours – a list of all possible destinations in the network may take up too much memory to fit in the small memory of sensor nodes. Consequently this could result in sensors using non optimal routes during packet forwarding. This could lead to packet delays or even lost messages possibly because the route chosen was too long (hence the delays) and as a result render the message irrelevant; also attenuation of the signal as it travels could distort message by the time it reaches its destination.
- ***b.*** ***Data gathering*****:** sensors in WSNs not only forward their own packets to the base station but also receive and transmit packets from other nodes (a consequence of using multi-hop communication). For this reason, sensors employ certain algorithms/techniques (e.g. aggregation techniques which is described in [11]) to collect sensory data from multiple nodes and eventually forward them to the sink node (base station) where the data is processed. However, these [1] sensor fusion and aggregation algorithms may require more computational power and storage capacities than can be provided by low-cost sensor nodes.

Therefore designers of WSNs face the daunting task of trying to minimise redundancy (by fusing data), at the same time ensure there is no loss of critical information during this aggregation process as well as ensure successful packet forwarding to the sink node – all the while operating under the hardware related resource constraints of sensor nodes.

G. Security:

The application purposes of sensor networks (e.g. military battlefield surveillance) results in collection of critical information – hence the need to secure these networks from intrusions and attacks. The first line of defence against security attacks is to provide only controlled physical access to a sensor node [1]. However, WSN are typically used in unattended, remote, harsh and public environments, which leave them vulnerable to: [1] physical attacks, unauthorized access, and tampering. Furthermore, wireless communication is more susceptible to attacks compared to wired communication. This is because RF (radio frequency) is essentially an open medium [12]. Below are a few of the most common security attacks associated with the wireless sensor network (WSN):

- ***a.*** ***Eavesdropping:*** whereby an adversary listens (to capture crucial information) into conversations between sensor nodes, without authorization.

b. ***Man-in-the-middle:*** this is when the attacker intercepts and modifies all messages from the sender before retransmitting it to the original message recipient in a manner such that the receiver will not have any knowledge of the modification – assumes the message is from original sender.

c. ***Denial of service (Jamming attack):*** works by disrupting network services to authorized users. The [12] legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless networks can no longer function. For instance, [1] the adversary can overload the sender with requests and tasks such that the sender is not able to transmit its message (in a timely fashion) to the receiver.

However, the complexity with WSN attacks is that some of them [12] may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well (free RF spectrum licence used by most wireless networks).

Thus a common challenge designers face, is deciding how the network will distinguish security breaches from common node failures – which normally arise as a result of the nodes being [1] very resource constrained and operating in harsh environments.

There are three main dimensions considered when designing effective security mechanisms: *Confidentiality*, *Integrity* and *Availability*.

a. ***Confidentiality*****:** ensure no unauthorized access to information by any other party other than the original sender and the recipient of the message. Security mechanisms (e.g. encryption) here can be used to prevent the eavesdropping attack.

b. ***Integrity*****:** ensure that unauthorized persons do not tamper and alter original contents of message as it's transmitted from sender to recipient. Security mechanisms (e.g. digital signatures or hashing functions) here can be used to prevent the man-in-the-middle attack.

c. ***Availability*****:** ensure that the up time percentage of the network is higher than its down-time percentage i.e. the network should perform its operations any time (when needed) without disruptions. Security mechanisms here can be used to prevent the denial of service (and or jamming) attacks.

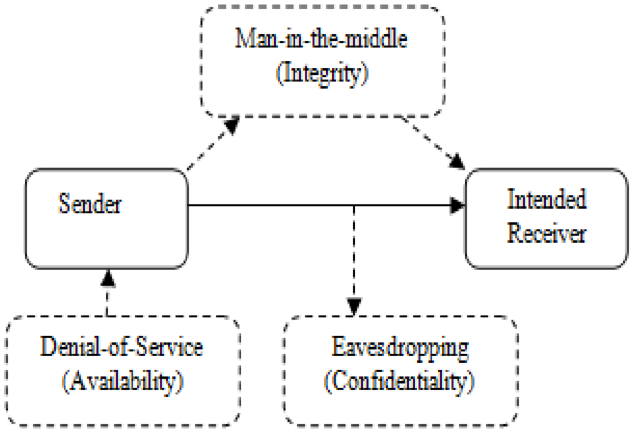

Figure 3: Illustration of common WSN security attacks

While there are numerous techniques and solutions for distributed systems that prevent attacks or contain the extent and damage of such attacks, many of these incur significant computational, communication, and storage requirements, which often cannot be satisfied by resource-constrained sensor nodes [1]. Designers are faced with the daunting task of implementing security mechanisms using the limited resources available in sensors.

Moreover, implementing *authentication* (this is proving that the message came from the node it claims to have come from) and *non repudiation* ([1] proving that a person or device has performed a transaction or transmission) procedures is quite difficult since [2] sensor networks are data centric so there is no particular ID associated with sensor nodes – an attacker can easily insert itself into the network and steal important data by becoming part of the network without the other sensor nodes detecting the changes. As a consequence, sensor networks require new solutions for node authentication [1] and *digital signature* schemes.

H. Proprietary technology approach of WSNs:

Unlike the traditional networks which are based on well established standards, sensor networks in particular WSN employ the proprietary approach. Whereby, there is no universal [2] networking and system architecture to build different applications. This poses a few challenges for the designers especially when it comes to implementing interoperability of WSN applications, this is because, most proprietary technology require that interaction can only take place between applications that use that same technology or share same system architecture. However, WSNs are mostly *heterogeneous* – consists of devices with varying hardware capabilities [1], performance, quality requirements, functionalities and architectures etc which eventually need to co-ordinate and effectively interoperate with each other despite their architectural differences.

Most of the applications and research prototypes are integrated in order to maximise performance [2] within the network while interoperability runs in the background. The heterogeneous nature of WSN is thus forcing designers to consider interoperability in the design plans. As result a key challenge remains on how to implement open standardization into the design of WSN. Standards are important for interoperability of WSN applications [1].

IV. CONCLUSION

Wireless sensor networks have very useful practical applications – health care, supply chain management, environment monitoring, and transportation/traffic control just to mention a few. However, designing of WSNs come with its unique share of challenges with the resource constrained and small form factor of the sensor nodes and the nature of the environments in which they operate in being the some of the main contributors.

This paper first presented an overview of the sensor node architecture and functionalities of each component in an attempt to justify the reasons behind some of the design constraints of WSN. The paper then went on to elaborate on some of the most common design challenges that WSN designers face during its implementation as well as describe possible solutions to some of the mentioned challenges. Although it has not covered the challenges experienced from the architectural point of view of the nodes (i.e. physical layer, media access layer, network layer, transport layer and application layer), it is possible to highlight from the discussion some of the architectural challenges a WSN might face. For instance at the physical layer we can refer to the issues of wireless media being prone to attenuation or noise, at the media access layer we can refer to the switching-state challenges, at the network layer we can refer to the issue of routing and data aggregation, at the transport layer we can refer to the multi-hop communication issues and at the application layer we can refer to the authentication security challenges.

While a great deal of advancement (work and research) has been done on WSN; as the wireless communication and in general information technologies continue to evolve so will the design needs of WSN as well as challenges. Therefore there is still a need to discover new (promising) solutions to these emerging design challenges and constraints wireless sensor networks face.

V. REFERENCES

[1]. Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks Theory and Practice, ISBN 978-0-470-99765-9, 2010

[2]. A Jangra, Swati, Richa, and Priyanka, “Wireless Sensor Network (WSN): Architectural Design issues and challenges”, International Journal on Computer Science and Engineering, Vol.02, No.09, 2010, 3089-3094

[3]. Newbie Hack: Microcontroller - A Beginners Guide - Basic and Default Usage of a Timer and Counter and The Microcontroller Clock. [Online]. Available: http://www.newbiehack.com/TimersandCountersDefaultandBasicUsage.aspx

[4]. National Instruments: What is a Pulse Width Modulation (PWM) Signal and What is it Used For? [Online]. Available: http://digital.ni.com/public.nsf/allkb/294E67623752656686256DB800508989

[5]. Earth & Planetary Sciences (eps): Passive vs. Active Sensors. [Online]. Available: http://www.es.ucsc.edu/~hyperwww/chevron/pas_act.html

[6]. Sensor Node. [Online]. Available: http://en.wikipedia.org/wiki/Sensor_node,

[7]. Search Networking Tech Target: Definition Radio Frequency. [Online]. Available: http://searchnetworking.techtarget.com/definition/radio-frequency

[8]. B. Singh Kaler and M. Kaur Kaler, “Challenges in Wireless Sensor Networks”. unpublished. [Online]. Available: http://www.rimtengg.com/iscet/proceedings/pdfs/misc/176.pdf

[9]. The physics Classroom: Inverse Square law. [Online]. Available: http://www.physicsclassroom.com/class/estatics/u8l3c.cfm

[10]. G.Singh and H.Arora, “Design and Architectural Issues in Wireless Sensor Networks”, International journal of Advanced Research in Computer Science and Software Engineering, Vol.03, No.01, January 2013, 28-32

[11]. R. Rajagopalan and P.K.Varshneys, “Data aggregation techniques in sensor networks: A survey”, unpublished. [Online]. Available: http://surface.syr.edu/cgi/viewcontent.cgi?article=1021&context=eecs

[12]. Spam Laws: Types of Wireless Network Attacks: Jamming. [Online]. Available: http://www.spamlaws.com/jamming-attacks.html