LAUTECH Journal of Engineering and Technology 2021 15 (2) 2021: 108-112

INTELLIGENT WIRELESS SENSOR BASED BOMB DETECTION: AN INTEGRATION QUALITY OF SERVICE MODEL FOR INTERNET OF THINGS PLATFORM

Akinde O.K.
Department of Electrical and Electronic Engineering, First Technical University, Ibadan, Nigeria
olusola.akinde@tech-u.edu.ng

Abstract

Owing to the global security concerns, intelligent Wireless Sensor Networks (iWSN) have been a major outcome of technological breakthrough. It thus becomes a practical platform where the information about the real world could be obtained via data fusion and computational embedded hardware systems. This paper presents a new perspective to Bomb Detection Technology (BDT) using an integration model that is based on the Internet of Things (IoT)ideology. QoS performance evaluation of selected algorithms, that is, the LEACH, Direct, as well as, a proposed cluster head (CH) algorithm for event based sensing and communication within an IoT deployment context was undertaken. Detection of suicide bombers and their related security frontiers is addressed in the IoT integration processed at the network level. The obtained results validate the need to integrate WSN devices into the IoT stack. In this regard, the IoT based CH algorithm is proposed for efficient communication system and energy utilization in bomb detonation hardware designs.

Keywords: IoT Platform, BDT, Bomb Detection, Integration Process, Quality of Service (QoS).

1. Introduction

The IoT ideology was developed in parallel with WSNs. Ashton, 2009 defined Internet of Things (IoT) as a way of uniquely identifying objects and their virtual depiction in an "internet-like" structure. Basically, these objects can be anything from security modules, large buildings, industrial plants, cars, machines, any kind of goods and services, specific machine to human (beings) systems, animals and plants, etc. According to Broring, et al, 2011, a Wireless Sensors Network (WSN) is broadly described as a "network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the environment". The sensing, processing, and communicating activities with a limited supply of energy, calls for a cross-layer design approach that requires the joint consideration of distributed signal/data processing, medium access control, and communication protocols (Presser, 2009).

Through synthesizing existing WSN applications in an IoT infrastructure system, potential new applications for mitigations such as the Nigerian Boko Haram attack vector model as well as Islamic group and other human attack vectors can be identified and mitigated. In this regard, there is need for the development of intelligent bomb detonation model that will meet future technologies and market trends.

The IoT paradigm could contribute to solving various security challenges in Nigeria. This is because the advents of Software Defined Network (SDN), IPv6, Distributed Storage, Data Fusion, Routing and Control Protocols, as well as, Identity Management and Object Recognition, have greatly extended the frontiers of IoT utilities and services. Notable areas could be found in cognitive reasoning about Things and Smart Objects, crowd-sensing, or human centric sensing, smart city management, as well as, context or situation awareness and intelligence. Identifying suicide bombers and other criminally minded entities require cognitive intelligence. Several security challenges must be addressed including QoS, security integration mechanisms and user acceptance to ensurea secured WSN integration in the IoT (Meyer, 2009).

The work presented is focused on communication inter-connection at the network level of the IoT stack. There are other security challenges that though not addressed in this paper, must be considered in future research works. QoS and other security issues are tightly related to WSN technologies and still affects IoT integration models generally.

The rest of the paper is organized as follows: Section 2 discussed IoT integration approaches; Section 3 gives the performance evaluation; while the conclusion reached is outline in Section 4.

2. IoT Integration Approaches

Considering the intelligent wireless bomb detection framework, there are various approaches identified from literature for its implementation. These are briefly discussed in the subsections below. WSN in relation to IoT integration can be achieved with two basic approaches as shown in Figure 1, that is the stack-based integration as elucidated in Roman and Lopez, (2009), as well as in topology-based integration Christin, 2009.

i. **WSN Stack Based Integration Technique (WSBIT):** According to Alcaraz et al. 2010, in the stack-based classification by Roman and Lopez, (2009), amidst the Internet and a WSN, the extent of integration often relies on the comparison between the built-in network stacks as shown in figure 1. In SBIT, the WSN is completely abstracted from the internet using the Front-End interface. The Gateway is then used to facilitate the information exchange using Internet hosts or through a shared layer of network TCP/IP protocol.

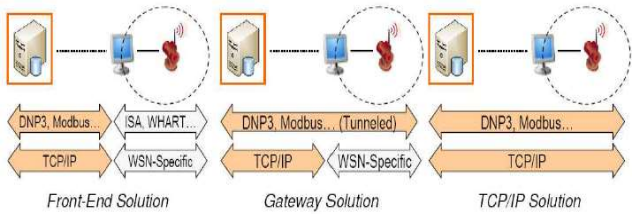

Fig. 1: WSN Stack based Integration framework (Roman and Lopez, 2009).

WSBITemployed a Front-End solution approach; in it there is no direct communicate between the sensor nodes and the external Internet hosts. There is distinct separation of the WSN from the Internet; with this it can execute its inbuilt protocols (for example, the Wireless as shown in figure 2 (HART, 2010). The central based device, like the base station, manages the communication between the wider world and the sensor network. The incorporated base station could store data streams from the WSN; the generated data streams could further be sent to external entities via recognized interfaces, for instance, the Web Services (Kansal, Nath, Liu, and Zhao, 2007). Besides, the base station or the sink could allow the navigation of other queries from the Internet hosts.

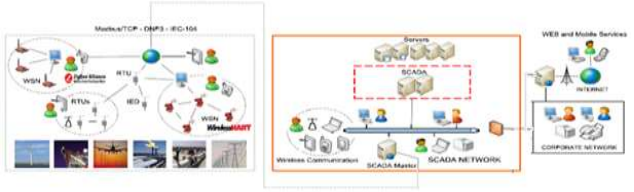

Fig. 2: WSN SCADA Environment (HART, 2010).

ii. WSN Topology Based Integration Technique (WTBIT): In this technique, the topology based classification has levels of integration. The precise location of the node that provide Internet connection often influences the typical level of integration. The nodes could primarily be a base station (e.g., few dual sensors) that could be at the core of the WSN (Hybrid); otherwise, it could be a complete backbone of devices which enables a sensing node connects the Internet in one hop (Alkaraz, 2010). Figure 3 depicts the levels of integration classification in WTBT.

Fig. 3: WSN Topology Based Integration Technique (WTBIT)/framework (Christin, 2009).

As in figure 2, the approach uses a gateway solution in which a device acting as a base station is used as an application medium access to decipher the lower stratum protocol from TCP/IP and proprietary networks. It also ensures passing of the information from an end to another. Consequently, direct connection in this topology does not exist between Internet hosts and sensor nodes for communication and information transfer. The WSN array is distinctly separate from the internet while queries are routed through a device for access as in figure 3. Sensor nodes, however, could interface directly with web service to other entities while their controlling codes are kept intact.

Besides, regarding WTBIT shown in figure 3, the adopted approach is Hybrid solution based; and in it a set of nodes within the WSN is placed at the network borderline. The node sets could connect Internet directly via communication algorithm. More so, easy mapping of inbuilt nodes to base stations could be done; much more that each sensor in the WSN collection needs to route their data through them to the centralized device, and vice versa. Redundancy and network intelligence thus constitute the main attributes of this approach. More than one base station could be connected to the internet network functionality in the WTBIT scheme. The network intelligence (i.e., the implemented protocols for dissimilar sub-station) is transferred to the subnet of the WSN since the base stations in WTBIT is equipped with capacity for Internet connectivity.

The Access Point solution approach as in WTBIT has its potentials benefits. Among these includes, WSNs been akin to an unbalanced trees with multiple roots, where leaves depict sensor nodes and other elements of the tree are Internet-enabled nodes [5]. This allows all the sensor nodes to access the Internet easily. The additive capacity of the network backbone nodes constitutes a major attribute of this integration approach.

In this context, a synergy of the Stack based Integration (SBI) and Topology Based Integration (TBI) techniques are leveraged for the IoT platform. In the proposed IoT structure, the sensors for event sensing are Internet-enabled nodes representing the front-end. A cluster head efficiently isolates the WSNs from the Internet gateways while data transfer is allowed directly between the sensors and the central control devices. Essentially, integration of the hybrid solutions (that is, the TCP/IP and backbone) becomes inevitable, to ensure effectual Internet connection of incorporated nodes. The node that connects the local network to Internet functions as translators for the sensed events.

iii. IoT TCP/IP Stack.

As illustrated in figure 1, the TCP/IP represents the third level in SBIT. The WSNs in IoT framework executes the TCP/IP stack (or compatible protocols set like 6LoWPAN (Montenegro, Kushalnagar, Hui, and Culler, 2007) in 802.15.4 networks. Hence, combination remains full-fledged elements of the Internet. Direct linkage to Internet is made possible with the TCP/IP stack, when any of the host is opened. Basically, the stack based solutions implement the WSNs on IoT platform. An accepted corollary of the scheme is the use of sensor nodes devoid of definite WSN protocols (Alcaraz, Najera, Lopez, and Roman. 2010).
There are limitations with TCP/IP leverage for IoT integration despite the fact that it offers the most efficient solution for

successful integration of WSN and the Internet. The merits are herein stated and briefly discussed below.

i. External system interfaces such as sinks can retrieve information from the nodes directly. This is because the nodes via IPv6 remains the link to the Internet and has the capacity to cross check any of its services.
ii. Using the TCP/IP stack, the in-built nodes can only connect the services that are implemented in the central devices for Front-End solutions.
iii. A reasonable level of congestion control could be achieved with TCP/IP.

Nevertheless, careful selection in choosing a particular integration method is ideal, some necessary feature that must be consider while leveraging TCP/IP are apt for consideration. The purpose of this research is to provide a QoS analysis, as well as, discussing the factors that impacts WSN whose nodes are wholly deployed on IoT platform. Some identified TCP/IP factors include:

- Resilience. TCP/IP driven WSN that are serviceable to external sinks; such are liable to some attacks like DoS. This arises from the throughput of the broadcasting channel and the ability of the sensor nodes. Security systems which safeguard the Gateways and sensor nodes against such attacks must be included.
- User's verification and permission. Applications that enable Internet sensor nodes linkage execute security devices that regulate access to traffic services.
- Security of the communication channel might be too heavy for constrained WSN.
- Traffic Audit and liability. It is ideal for an Internet based WSN to build a spread system which could record system users with their operations. With the records of day to day operations, recreation of security incidents and abnormal situations could be achieved.
- Traffic Utility. Is taking into account where some sensor nodes application does not implement Internet connection.
- Embedded Hardware Leverage. Due to large memory demands of the diverse security mechanisms (for example AES-128, Elliptic Curve Cryptography primitives, key negotiation protocols) aninhibited sensor node may be disable from connection to the Internet directly.
- WSN In-built limitations. Some of the attacks Internet operated sensor nodes are prone to consist of DoS, exploit and so on. This factor uniquely determines if some sensor nodes applications should be detached from the Internet connection, and thus filter arriving packet at the network end.
- Network redundancy. For redundant purposes, a set of sensor nodes could reproduce same utility; although in TCP/IP scenery, IP addresses are needed by definite nodes for external host permitted services. The implication is that for specific circumstances it is required to grow some TCP/IP milieu to relate with special nodes, usually those out-of-reach.
- Protocol optimizations. Networks that provide self-healing ads-on and optimized internal activities are incorporated in certain WSN protocols. Such features are not yet obtainable in 6LoWPAN based networks and IPV6 for intelligent detection algorithms.

3. Performance Evaluation

1) A WSN algorithm for smart event sensing and reporting was studied via an empirical test bed using Riverbed Modeler version 17.10. Riverbed Modeler is a discrete event-simulation engine. Often, it is employed for the purpose of analyzing and designing of communication networks. It has a set of protocols and technologies with a refined development environment deployed towards modeling of all network types and technologies (this may include, VoIP, TCP, OSPFv3, MPLS, IPv6, and a lot more). Riverbed Modeler analyzes networks with the aim of comparing the influence of different technology designs on end-to-end behavior; It enables a user to test and demonstrate technological designs before they are produced.In the work, three scenarios were used for the sensor nodes evaluation (the source and sink nodes inclusive) in a linearly spread pattern within an area of of 100m×100m for site_1 and site_2. The radius of nodes broadcast is 30m. The proposed clusterhead algorithm was evaluated with three scenarios for the triangular linear topology performance. The procedure for each test run include: (1) All sensor nodes were deployed at each site; (2) In the simulation test-bed, the configuration parameters were set. The scenarios (#1, #2, and #3) precisely target the proposed Clusterhead (CH), Leach and Direct schemes. Each node with its Zigbee parameters specifies its configuration. The preset values available for this attribute was used in configuring explicit traffic. For simplicity, each subnet site has nodes initially communicating with a sink. In the setup, the sensed events are communicated to the CH via the basic sensor nodes. The CHs then transmits to the logic control console, which is the multiplexer engine. The sink logic control center then transmits to the action initiation console. Within the communication structure, the routing algorithms ensure that the sensed events are used to activate the automated control functionality of the system. Thus, the QoS of the Intelligent Wireless Bomb Detection System (IWBDS) was measured to establish its performance in relation to LEACH, Direct algorithms. Table 1 shows the simulation parameters used in this study.

Table1: Parameter Specifications of Intelligent Wireless Bomb Detection Communication System

	Simulation Parameters	Values
1	Sensor Type	Zigbee Station Adv
2	Sensing rate	Auto Calculate
3	Packet Reception Power Threshold	-85
4	Transient Power	0.005W
5	Device Types	End Device (BSN), and Coordinators (CHs)
6	Beacon Order	6
7	Maximum Children	>7
8	Route Discovery Timeout	10Secs
9	Application Traffic	Random
10	Access Control	TDMA
11	Packet Size	1024
12	Channel Sensing Duration	0.1Secs
13	No of Nodes	12
14	No of Cluster heads	3
15	Buffer Sizes	256000

The obtained result from the evaluation of three algorithms based on vital QoS metrics for event based communication and sensing are summarized as follows.

i. Average Energy Dissipation

In an IoT based bomb detection system, an implemented cluster head helps to shorten communication path to the sink, thereby lowering the average energy dissipated per rounds. In the design, it desirable that energy needed for data propagation is balanced, that is, data propagation to the sink is done in such a way that the average dissipation in each sensor is at each time the same.

The average energy dissipation per sensor as shown in figure 4 is taken to be the fraction of the total energy spent per sensor in the triangular design. The plot of energy dissipation shows that the proposed CH algorithm has a lower dissipation rate of 500J/Bit compared with the consumption of 900J/Bit (LEACH) and 1000J/Bit (Direct) algorithms. The lower dissipation rate is as a result of the CH in the deployment. The implication is that the IWBDCS can last for a longer time in its event sensing considering the proposed cluster head algorithm.

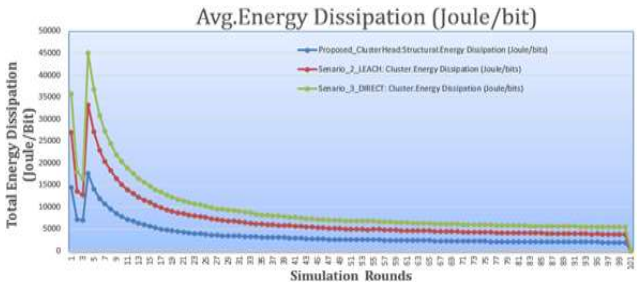

Figure 4: A Plot of Packet Reception Rate

ii. Latency Behaviour

Specifically, latency measure the average time a packet takes to reach the sink from the instant it is generated. Long delays will result in packets reaching the sink when the information is no longer useful (Kozierok, 2005). Figures 5 and 6 show the comparative relationship of the latency response of the three independent algorithms in view of sensed event. This work evaluated the latency from the packet broadcast time on the source node to the reception time at the sink node. The work directly measures the latency of packets received at the sink, thus the metric should be considered as reliable. The latency in the WSN is dependent on the queuing delay pattern and the responsering which reduces the packets rate a node can send. The load carried by a channel affects its latency.

The impacts of resource reservation (RR) and the control's algorithm deployed in this work resulted in the latency response of the proposed CH scheme to be as low as 18.42%. The Leach and Direct schemes yield the network latency of 36.84% and 44.74% for the Leach and Direct algorithms respectively. The lower latency response of the proposed clustered head (CH) scheme is optimized compared with the Leach and Direct schemes.

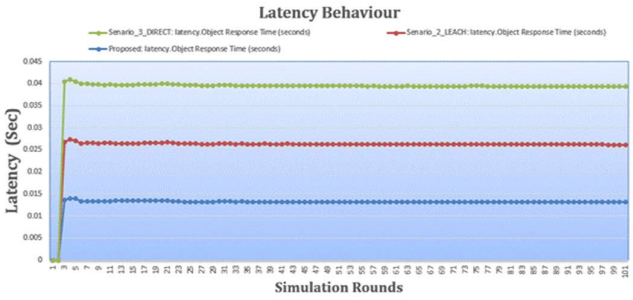

Figure 5: A Plot of Latency Behaviour

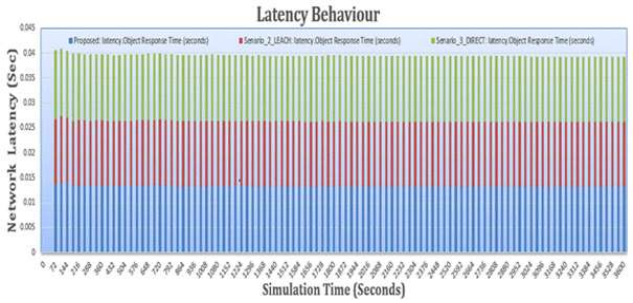

Figure 6: A Plot of Latency Behaviour

iii. Throughput Behaviour

Throughput is a unique measuring index of WSN deployment. It is the number of packets reaching the gateway per unit time. It is important because if large number of packets is dropped, the gateway cannot form the correct vision for the activities in the covered area (Kozierok, 2005). In the periodic workload arrangement, a sensor network is monitored where the incorporated sensor nodes communicating to the sink produce readings at different time gap. In the set-up, each node transmits at specific rate and forwards packet to the sink. Figure 7 illustrates normalized throughput behaviour. The Leach and Direct yielded 33.00% and 30.09% correspondingly, while the proposed CH algorithm yielded 36.90% cumulative throughput at the sink. As shown in the plot of figure 12, the response of throughput with time follows a transition from the initial low values to higher ones for all the algorithms (Leach, Direct and the proposed CH). From the obtained result, it was observed that the throughput is a WSN prime measurement index because; a lower throughput indicates a poor sensing capability and so WSN overall impacts is reduced.

Figure 7: A Plot of Throughput Behaviour.

4. Conclusion

The paper discussed the basic QoS performance for a vibrant WSN leveraging the TCP/IP communication stack. Selected algorithms for event based communication were compared for adoption in the bomb detection proposal in an on-going research. It is clear that the potential of the iWSN paradigm has fully unleashed remote tracking and monitoring of events via the Internet. The deployment of TCP/IP stack in WSN management in the platform (IoT) is thus recommended for smart intelligence and application services. After discussing the QoS metrics based on selected parameters using TCP/IP directly, it should be noted that certain related issues about security must not be neglected in the implementation of WSN ON IoT premise. Issues like security method and services, interest of users and data privacy organization must be investigated in future works to make iWSN a widely acceptable platform for IoT integration. Nigeria could benefit from this concept if it is adopted for use.

REFERENCES

Alcaraz C. Najera P., Lopez J., and Roman R., Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?", 1st International Workshop on the Security of the Internet of Things (SecIoT10), 2010. NICS Lab. Publications: https://www.nics.uma.es/publications

Ashton, K. *That 'Internet of Things' Thing. In the real world, things matter more than ideas*. RFID Journal, 22 June 2009. Available from: http://www.rfidjournal.com/articles/view?4986

Broring, A. et al. *New generation sensor web enablement*. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652.

Christin D., Reinhardt A., Mogre P.S., Steinmetz. Wireless Sensor Networks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVSFachgesprch "Draht lose Senso rnetze", 2009.

HART Communication Foundation, http://www.hartcomm.org/, Accessed on October 2010.

Kansal A., Nath S., Liu J., Zhao F. Sense Web: An Infrastructure for Shared Sensing. IEEE Multimedia,Vol. 14, No.4, pp. 8-13, 2007.

Kozierok C. M., The TCP/IP Guide(http://www.TCPIPGuide.com)Networking Fundamentals Version 3.0 : September 20, 2005 http://www.tcpipguide.com/free/t_PerformanceMeasurementsSpeedBandwidthThroughputand.htm

Mayer C.P. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, 2009.

Montenegro G., Kushalnagar N., Hui J., Culler D. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. 2007.

Presser M., SENSEI. Integrating the physical with the digital world of the network of the future. IEEE Explore, 2009. Available from: http://www.sensei-project.eu/

Roman R., J. Lopez. Integrating Wireless Sensor Networks and the Internet: A Security Analysis. Internet Research, Vol. 19, No. 2, Pp. 246- 259, 2009.