International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2018/49501 Volume 5, Issue 4, July – August (2018)

RESEARCH ARTICLE

Wireless Sensor Network Surveillance on Forest Illegal Mining using 'Planned Behaviour Abortion Tower': Analytical Modelling

Eric Opoku Osei
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana.
eoosei@ug.edu.gh

James B. Hayfron-Acquah
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana.
jbha@yahoo.com

Michael Asante
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana.
masante@yahoo.com

Published online: 11 October 2018

Abstract – The USAID report on climate change vulnerability and adaptation in Ghana confirmed the impact of recent explosion of illegal gold mining in forest reserves and in river body. Government of Ghana responded to such wake-up call in deploying military combatants against perpetrators operating at day and midnight hours when drones are ineffective to monitor. We aimed at wireless sensor network (WSN) deployment to compliment military efforts for real time remote sensing. A conceptual framework on WSN technology is proposed based on expert view gathered from Delphi technique data analysis. A close textual reading of illegal mining editorial and the primary evidence of climate change impact from water shortage due to river body pollution with cyanide chemical in Ghana are key input factors for this technology-based conceptual exploration. Positive analytical feedback from the 'Delphi' suggests that we can apply this conceptual framework to all environmental case studies in which technology-based security protocols are good compliments to abort human intention towards certain behavior. The comparative discussion on the use of Drones, Satellite and WSN showed that the latter is: economical to deploy, energy efficient for continuous operational availability and reliable data sensing at midnight mining compared to drones' image processing power at night to track manual mining excavations. This study gives a starting point for uptake investigation in WSN deployment for surveillance on illegal mining; hence the findings may have limitations such as subjectivity of expert view. This conceptual framework is a recommendation to urgent national issue and thus it is relevant having real-world implementation for testing the human behavioral assumptions.

Index Terms – Wireless Sensor Network, Surveillance, Illegal Gold Mining.

1. INTRODUCTION

Relations between the science and arts of climate change which demands an interdisciplinary knowledge convergence to fight the global impart is well established [1]. Wireless sensor networks in ad-hoc deployment for monitoring diverse phenomena in the environment is receiving an attention [2].

However, evidence that WSN deployment can scare or abort human intention in committing illegal gold mining has not been confirmed in any studies; especially in the tropics. Several ailments such as nervous system effects and vitamin B_{12} deficiency in human and animals have been linked to the doping of cyanide chemical applied in washing of gold and channeled back to river body for human consumption [3][4].

Satellite and Drones for remote surveillance are known in the tropics and subtropics, however the use of wireless sensor network technologies such the Mobile Ad-hoc Networks (MANET), Wireless Mesh Network (WMN) and 'Smart Dust' are underutilized for environmental monitoring [5]. Ghana is a country in the tropical area of Africa facing the negative impact of illegal gold mining in the forest and water body by aggressive perpetrators. The government of Ghana deployed 400 security personnel task force to carry out what became known as 'operation vanguard' in 2017 to protect the environment most in affected areas [6]. Empirical evidence gathered for this study showed that the illegal miners work at midnight when the military force had returned to camp. Some work under tree-masked forest pits where the deployment of drones may even have difficulty with image processing of their location at midnight (21GMT-3GMT).

RESEARCH ARTICLE

We aimed at performing analytical modelling of using wireless sensor network deployment to compliment the manual surveillance efforts by the illegal mining task force in Ghana as shown in Figure 1.

The objective was to determine how WSN architecture for surveillance can be applied in deep forest reserves to deter or abort human behaviour. This will make WSN technology relevant to sustainable development.

2. BACKGROUND ON WSN APPLICATIONS

2.1. Wireless Networks

Wireless Networks support communication in a mobility mode. A typical example is the GSM communication architecture and Wi-Fi modem operations for data services. We can divide wireless networks based on application environment: Wireless Personal Area Network (WPAN); Wireless Metropolitan Area Network (WMAN); Wireless Local Area Network (WLAN); Wireless Wider Area Network (WWAN) and Wireless Ad-hoc Networks [7]. In addition, we have the global/satellite communication network, Space network for space crafts and cellular distributed network.

2.1.1. Wireless Personal Area Network (WPAN)

Connectivity between a person's earpiece and mobile phone using Bluetooth (10meters) or infrared light (IrDA) or ZigBee link is known to be WPAN. This connects devices within relatively smaller area within the reach of a person. It has the capacity to synchronize and/or transfer files within a limited radio range at home or the workplace at an approximate bandwidth of 1Mbps [8].

2.1.2. Wireless Local Area Network (WLAN)

Standard LANS, wires such as the Ethernet cable are used for data transmission in the form of electrical signals. Wireless LAN also make use of the air interface as medium of transmission to propagate the same electrical signal in a crafted name as radio signal [9]. The latter achievement is credited to the significant research made by Heinrich Hertz (1857-1894); Andre-Marie ampere (1775-1836); Michael Faraday (1791-1867); James Maxwell (1831-1879) and William Herschel (1738-1822) who first opined from his astronomical insight that infrared light existed and were beyond human eye visibility.

Bandwidth is crucial in network transmission and it is realized from the radio frequency. Bandwidth is a term to represent the volume of data per second that any signal transmission medium (wired or wireless) can carry form source to destination. Like a large or wide bus vehicle having many seats is able to carry more passengers and still run a faster speed; the same way a large data bandwidth is able to move volume of information/data at a faster speed (bits per second/Mbps/Mb/s) from source to destination. For example, internet service connectivity having larger bandwidth support faster browsing because many data set can be moved speedily at a time. If the bandwidth is small, the internet browsing will be comparatively slow because in real world situation, you would be using a small Toyota vehicle to carry more passengers.

Modulation in wireless networks is the process of superimposing the modulating signal on the carrier signal for data transmission within the air interface. The modulated signal consists of three factors: the Frequency, Phase and the Amplitude which are used for the modulation. The three modulation techniques are DSSS, MIMO and OFDM in wireless networks. The 802.11b devices uses the DSSS modulation technique. The 802.11n devices in the market uses MIMO modulation technique and OFDM is also use to achieve highest data rates at low resistance; although it is not considered a spectrum technology.

The Institute of Electrical/Electronic Engineering (IEEE) developed the 802.11 protocol specification for transceiver (duplex) operations on a WLAN. The use of 802.11 specification requires no operating license, but an implementer must adhere to the standard rules that governs power levels and frequency spectrum range. Bandwidth can be referred to the RF channel width and it can also mean the data rate.

IEEE 802.11 came up as wireless communication system standards for anyone implementing wireless networks. The IEEE 802.11a followed to set rules or standards for implementing wireless sensor networks with OFDW modulation. IEEE 802.11b also came for DSSS modulation and IEEE 802.11g considers both OFDW and DSSS modulations, however for different indoor and outdoor transmission ranges.

2.1.3. Wireless Metropolitan Area Network (WMAN)

This type of network integrates several local area networks acting as clusters and connected to a centralized hub or server. The Worldwide Interoperability for Microwave Access (WiMAX) is an example of the WMAN using the IEEE 802.16 set of standards to guide service providers and implementers. One advantage is that it offers Media Access control (MAC) and multiple physical layers to speed up transmission at less congestion [10].

2.1.4. Wireless Wider Area Network (WWAN)

This is intercity networking connecting corporate branches. Microwave is adapted to the point-to-point connectivity at 2.4GHz band. It supports both voice and data file transfers using the GSM telephony infrastructure. WWAN using 3G signaling links to connect cities are reliable more than the earlier 2G which has low data transfer. Some operators of WWAN has adopted fiber cable transmission [10].

RESEARCH ARTICLE

2.1.5. Wireless Ad-hoc Network (W-ad N)

There are related WAN including: Wireless sensor network (WSN); including Smart Dust Sensor Networks, the Mobile Ad-hoc Networks (MANET), and Wireless Mesh Network (WMN) have their respective names based on the design and application environment. The key knowledge here is that all these related distributed wireless sensor networks are built on the fundamentals of distributed computing [11]. Ad-hoc means: "for this specific purpose". If wireless sensing devices are distributed "for a specific purpose" the implementers may like to name it to reflect that specific purpose. However the generic name is always referred to as wireless sensor network [12].

For example, if a developer insert tiny sensors in Biro/Pen or pencil to monitor cheating behaviour in the extermination hall by measuring pressure on holding the sensor-based pen at a certain time interval to trigger alert to the surveillance monitoring room, then the implementers may choose a name such as "Wireless Sensor Pen Network" (WSPN) or simply called it as "Ad-hoc Intelligence Pen" (AIP) [working paper]. It is evident that the name is given for this specific purpose; hence it is an ad-hoc network. Ad-hoc may refer to a system permanently implemented for a "specific purpose only" or a system temporary implemented to die off after the purpose. A research unit provides attractive names to the same wireless sensor network to attract readership and citations; making it seems as a new brank of study. This can sometimes create serious alignment in souring and retrieval of relevant papers for cohesive literature review on WSN.

2.1.6. Wireless Mesh Network (WMN)

Mesh is a robust self-configuring ad-hoc network with high throughput efficiency. The mesh network has good scalability as it can cover estimated 1000 square feet. Mesh network is costly but it is one of the robust network topology for wireless sensor network. It is mostly in-built in cloud-based backend systems or in a firmware on each router. The topology in mesh is static as a constant movement will take more time updating routes than data delivery assignment. For energy optimization factor, the mesh network reduces retransmission of all data passing to the base station. There are limitations that are general to all other wireless sensor networks types. Sensors are prone to short energy dissipation due to low battery capacity; as most of the sensors power are non-rechargeable and/or replaceable. The sensor nodes are largely designed for data collection; hence sometimes it is unpredictable to classify the type of network topology in use. This also means that whiles some sensors would be underutilize, others would overwork due to unpredictable differentials in the measurement of distance of peer-to-peer connectivity. The longer the distance of peer-to-peer connectivity, the shorter the energy lifespan of the sensor node as it has to utilize more energy for data transmission to the next hub. This challenge has resulted to several proposals on energy efficient routing protocols or algorithm for connecting nodes in peer-to-peer and for transmission unto the sink or the base station for processing data [13]. The sensor nodes are also self-governing; once they are deployed, it requires no human engineering intervention or maintenance until the network dies off with respect to time limit for entire energy depletion in the sensor devices.

2.1.7. Mobile Ad-hoc Network (MANET)

TinyOS and TinyDB are not application in MANET deployment as this make use the traditional networking infrastructure protocols. MANET is a revolution in terms of network implementation in an ad-hoc situation; especially in an environment with poor infrastructure deployment. There are specific routing protocol standards develop to enhance these Ad-hoc network called MANET. The MANET performs self-configuring routing and it may not require any infrastructure as the mobile devices works in a peer-to-peer connectivity. As autonomous topology, each device has freedom to independently move and will establish and de-establish links with other peer mobiles. MANET can be classified based on application environment as: vehicular Ad-hoc network (VANET); Smart phone Ad-hoc networks (SPAN); Internet-based Mobile Ad-hoc Network (iMANET), Hub-spoke MANET, Military MANET, flying Ad-hoc Network (FANET) [10].

2.2. Wireless Sensor Network (WSN)

Tiny sensory devices are distributed at random or nonrandom approach to spy, track, monitor, trace, alert environmental factors such as temperature, pressure, humidity, sound and then transmit the data using routing protocol or algorithm from source to destination. This is considered as one of the ad-hoc network as it spontaneously forms and connects sensors in an autonomous approach. WSN formation can contain several hundreds to thousands at dispersed environment of interest [12].

2.2.1. Smart Dust Sensor Network

Smart dust is a type or class of wireless sensor network and an Ad-hoc sensor-based network for specific purposes that are distributed in the interest environment as tiny like the dust particles. They are made of MEMS technology at cubic millimeter in size and very low power computing capacity. It is referred to as Motes as in their distributed mode, they are able to automatically organize themselves using Self-Organizing Maps (SOM) in a network; given them autonomous features to decide which cluster to join in the network. It uses message passing to communicate; harvest their own solar energy form the environment to power the circuit and creates connections to other motes within the network with no human intervention [14]. Smart Dust sensor network is applicable in chemical industry, business settings,

RESEARCH ARTICLE

biological elements control, real time events tracking, quality control, military battlefield intelligence and large scale forest reserve supervision from remote location. For example this dust particle size can be thrown in the enemy's camp to collect sound or intelligence signal without significant notice of its deployment due to its dust particle size in nature. In the near future, this smart dust sensor device will power the smart city or internet-of-things deployment in our society, due to its cubic millimeter size and low visibility for a passer-by. Quiet interesting applications; these sensors can monitor your body temperature and automatically adjust the air conditioner degree to suit your body without human interventions for regulating the output air with the tab. Smart dust has wider scope of application; including the pre-detection of possible fire in the forest.

This type of wireless sensor node deployment has strong processing power and can network huge volume of sensors at a reliable performance measurement. The sensors has a mechanism to vibrate in identifying precise electro-mechanical defects in oil refinery systems. For every wireless sensing network, data (voice, queries etc.) broadcasting and data throughputs are key. The Smart Dust produces efficient performance on these factors. Mobile internet gadgets like the iPad helps in the integration of sensory inputs quickly; thereby driving adoption of sensory technologies in the 3G and 4G infrastructure era. Wireless sensor network made of the smart dust technology is greatly raising real time connectivity to navigation in the transport (sea, land, air space) environments. Using smart dust sensory network, the HP Company (WSN service provider) in collaboration with the Royal Dutch Shell (Corporate client) aim at deploying over a trillion volume of the smart dust sensors crosswise the planet poles to generate on the earth, a central nervous system, to aid in oil exploration [15].

Smart dust is applied in wireless networks and it is produced as an integrated system bringing tiny micro electro mechanical systems (MEMS) including sensors, robots and other devices having computational capability to sense, track or detect light, temperature, vibration, chemical leakage, magnetism and other pressure. Smart dust are tiny like dust particles operated without an antenna of significant size and it is a product made from a prolonged research work of the Defense Advanced Research Projects Agency in the USA and Research and Development corporation. The transmission range of smart dust is in few millimeters [15]. During setup, the smart dusts are spread within the interest environment for data collection.

2.3. Sensor Devices

The fundamental experiments pursued by designers of portable wireless sensor nodes are the need for reducing sensor energy consumption, increasing ad-hoc network lifespan under scalable deployment in a wider area of interest to monitor. The wireless sensor nodes operates on small battery pack, hence the energy depletes at a faster rate due to peer-peer sensors communication and data processing transactions and hop to hop transmission to forward packet to the base station of the network. In accordance, routing protocols aimed at minimizing the energy consumption to ensure long lifespan for these portable sensors under any scalable topology are desirable to improve the application of wireless sensor networks [16]. In this chapter, we are reviewing the performance of existing routing protocols to analyze some of the inherent challenges so that we can propose an enhanced routing protocol. Each node consists of a radio transceiver, antenna, and microcontroller, embedded battery that may non-rechargeable or rechargeable using solar.

2.3.1. Chipcon CC1010

The Chipcon is built on a single-chip embedded with a UHF transceiver that provides an integrated high performance. The overall architecture of the Chipcon has a dedicated protocol processor and is able to keep a partition between application processing and protocol. The frequency spectrum allows operation within the 300-1000MHZ range to make it applicable in low power wireless transceivers. This Chipcon has become commercially viable built on Intel 8051 microprocessor [17].

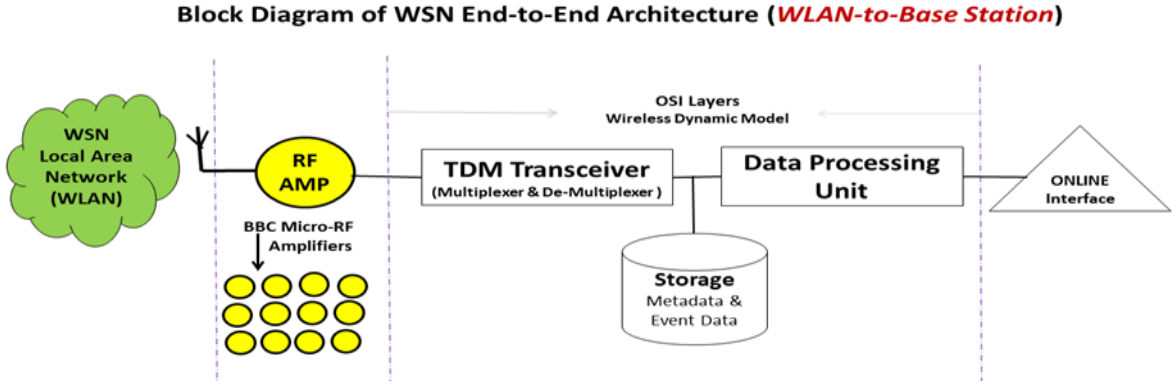

Figure 1: Block diagram of Wireless Sensor Network using BBC-LEACH Routing Protocol

RESEARCH ARTICLE

3. RELATED WORKS

WSN Ad-hoc deployment for environmental monitoring is not new. Some routing protocols exist such as the Low Energy Adaptive Hierarchical routing protocol (LEACH). However, one limitation is about scalability. Any attempt to position the base station far away for sensors lead to shot lifetime of the sensors; whether the sensor type is produced as energy-harvesting or non-energy harvesting. The illegal miners are like often aggressive to commit behaviour. Deploying WSN on grounds may be insufficient to deter them from secretive illegal mining. Due to this we proposed: (i) new routing protocol name BBC-LEACH [25] which can meet scalability factor to help position the base station afar from the WLAN deployed for surveillance in the suspicious illegal forest mining areas. (ii) *fit-for-purpose* base station mounted on surveillance tower for illegal mining planned behaviour abortion in line with the theory of panopticism [20]

Figure 1. End-to-End wireless sensor network architecture. The dotted vertical lines divides the entire architecture into four (4) units. The WLAN on left indicates the sensors deployed as local area network for surveillance. The rest are integrated circuit called the base station (BS). The RF AMP is the first unit functioning as power amplifier propagation via antenna. WLAN uses a routing protocol called "Backbone-LEACH to communicate with the base station. This BBC-LEACH is a routing protocol redesign for scalability and is based on the Low Energy Adaptive clustering Hierarchy (LEACH) [18]. The BBC is a large-cluster backbone made of micro-RF amplifiers. The micro-sensors are deployed within the BBC cluster; hence the name backbone. There is division of labor: The sensor uses single hop path to transmit packet to micro-amplifiers. The micro-amplifiers functions as backbone to suing multi-hoping to forward packets from cluster-heads to bases station. Now, TDM Transceiver transmit and receive packets at time slots on the OSI data and physical layers. Data processing unit manages the rest of the OSI layers in data communication. The Storage unit handles both system metadata and captured activity data from sensors. The Online interface can be a satellite or GSM link for remote monitoring between Forest and the military camp. The micro-sensor device is made of four (4) units: Microcontroller, Transceiver, Sensing unit and the battery source as shown in Figure 2.

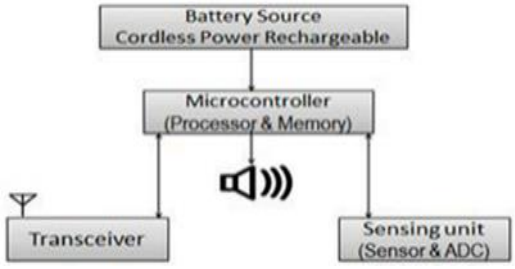

Figure 2. Wireless Micro-Sensor Device

Wireless sensor network are made of small energy dependent nodes dispersed in spatial mode for monitoring and recording conditions of interest in an environment such as sound, pressure, temperature, pollution level in river body, humidity, wind and other phenomena using sensors for data capturing.

Most of these phenomena could be agitated by human behavior or activities. For example the pressure sensor can effectively monitor excavation works in mining pits at all times (sec); compared to drones which is battery dependent. It is hypothesized in this study that WSN for surveillance can cause planned behavior abortion extracted from. Ajazen, 1985 modeled the "Theory of Planned Behavior-PBT" as shown in Figure 3 in understanding complexities of human behavior [19]. The PBT is modified in Figure 5 for this study with details.

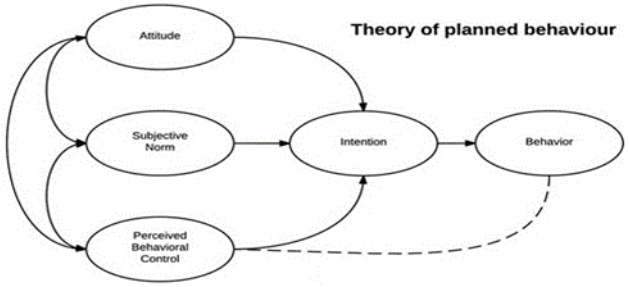

Figure 3: Theory of Planned Behavior

Foucault, (1977) experimented a non-electronic physical surveillance tower to control prisoners behaviour at the Bentham's panoptic on [20]. The theory known as panopticism or the gaze has a centralized tower structure for observing activities of the prisoners. The presence of the surveillance tower created an impression that changes intention to perform behaviour at every point in time. The prisoners could imagine the consequence of their behaviour at any gaze of the tower. Because they were unable to predict whether the wardens were inside the tower or not kept the prisoners from performing their aggressive behaviour [20].

Analytically, Behavioral Intention (BI) is given as:

*BI =(W_1)AB[Σ(b)(e)] + (W_2)SN[Σ(n)(m)] + (W_3)PBC[Σ(c)(p)]

We can as well perceived behavior and control (BC) execution as:

**BC = (W_1) BI + (W_2) PBC [Σ(c) (p)]

AB: Represents Attitude to behavior:

(*b*): shows strength of each belief concerning an outcome

(*e*): Is the evaluation of the outcome or attribute

SN: Subjective norms

(*n*): Indicates strength of each normative belief

RESEARCH ARTICLE

(*m*): Indicates motivation to comply

PBC: Perceived Behavioral Control

(*c*): Strength of each control belief

(*p*): Perceived power of the control factor

W: empirically derived weight/coefficient [21]

In summary, we used the existing mathematical modelling *(* and **)* of PBT for modification in our proposed PBAT.

4. METHOD OF ANALYSIS AND DESIGN

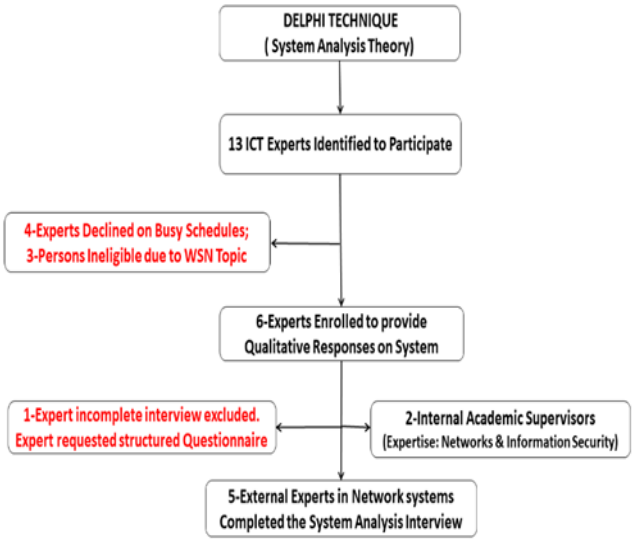

Figure 4. System Analysis and Design

This flowchart summarizes methods for data collection, data sampling and enrollment of experts in the field of WSN for system design and analysis known as the Delphi technique [22]. It is a one type of method for data collection and analyses under qualitative research for confirmatory testing responses. Only the expert views are used for system design reworks, where required, in health, engineering and the sciences. The proposed network application is based on mathematical or analytical modelling and we used the expert view for confirmatory testing on the system design and analysis.

In all, seven (7) experts were selected for the Delphi analysis [22]. Each expert view is anonymous to one another. We had an oral interview on the design based on technical feasibility. The major questions centered on "Perceived usefulness" of the framework and "Perceived ease of use" guided for the questioning as guided in the Technology Acceptance Model (TAM) model by [23]. Interviews were recorded and transcribed. A minimum professional experience of ten (10) years in the field of computer network application was a selection criteria of respondents.

5. PROPOSED MODELLING

5.1. The Theoretical Model (PBAT)

Figure 5 represents the theoretical model setting up the Planned Behavior Abortion Tower modified from both theories in controlling human behavior. Significant introduction is the while loop on intention using WSN.

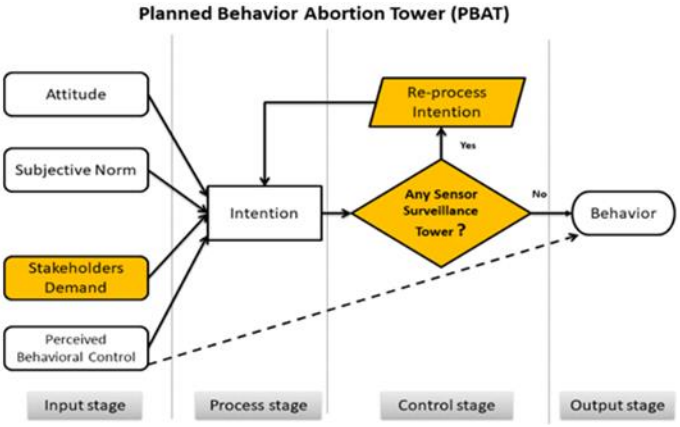

Figure 5. A model for Planned Behaviour Abortion Tower

Y_1 is the modification of PBT given as:

$$BC = (W\_1)\ BI - (W\_1)\ SCT + (W\_2)\ PBC\ [\Sigma(c)\ (p)]$$

Where SCT is the Surveillance Control Tower that creates a looping negation value of zero:"0" to nullify intensive. The loop is active until a condition of arrest or abortion once intention. We also suggest additional input labeled in the PBAT model as "*stakeholders' external demand*"; which implies that external demand for gold by local and international dealers influences attitudinal strength to commit illegal mining behavior by the perpetrators. When motivation is full, then intention is developed. However the introduction of a "while Loop" on intention factor can result to planned behaviour abortion.

The Pseudocode algorithm with the precondition variable declarations as A, B, C and D were setup. Unlike the original PBT having three (3) inputs to influence human intention to commit behaviour; we have rather four (4) inputs that influences intention to commit illegal mining behaviour by the aggressive miners. These four (4) inputs creates intention to commit behaviour. However, we have declared an intermediary variable "R", which is a while loop control structure between the time for nursing intention and committing behaviour.

As the whiles loop is active for surveillance, then time interval to move from intention to behavior will still widen. It is hypothetically confirmed from the Delphi technique responses that there is high probability of behaviour abortion by the activeness of the while loop.

RESEARCH ARTICLE

5.1.1. Precondition Variables

LET A = Attitude towards the behaviour

LET B= subjective norms

LET C= Perceived behavioural control

LET D = stakeholder demands.

LET R = revise intention after surveillance alert

For every behaviour (F) output performance {

LET T = intentions

Move A, B, C to T

Process T

WHILE F is awaiting T {

Add R into T

}

If T=A + B + C –R {

Then F=0

}

}

The theory of panoptic tower control was once used to control behavior of hard core criminals in a prison (panopticon). The independent works of Bentham and Michel Foucault regarded the panopticon as a symbol of the disciplinary society of surveillance. The panoptic style of architecture is usable in areas of Ad-hoc surveillance needs, such as schools, factories, or hospitals. However, such surveillance are not based on technology. In this work, we are testing it in forest environment based on WSN supported by BBC-LEACH routing protocol for the surveillance. The unique feature of our proposed model in Figure 5 has to do with combination of two theories: (i) Theory of Planned behavior and (ii) Theory of Panoptic. We combined these two to create a new model named as "Planned Behavior Abortion Tower" (PBAT) for surveillance in the forest reserve environment.

5.2. The Conceptual Tower Base station

The theoretical model in (i) explains the established concept that for every planned behavior, there is a possible control mechanism to abort the intention fueling that behavior. In (ii) we present the conceptual framework depicting the practical design of the WSN Surveillance Control Tower as shown in Figure 6.

Figure 6. Represents the conceptual base station which is mounted on a guyed tower of 60ft (18.3 meters) in height in the forest; depending on the land curvature. The base station clearly visible in long range view but portable in size and shaped in equiangular for easy positioning on top of tower. *Label A*, on Figure 6 is the automated visual surveillance that picks priority frames only as and when it happens within 360^0 for energy conservation and avoiding redundant object data. *Label B* is the central processing unit of the integrated circuit. *Label C* represents the active sensors that are deployed on grounds using BBC-LEACH routing protocol to communicate with the base station. *Label D* is the GSM or satellite interface for online remote monitoring. *Label E* is a direct GSM SIM slot to aid voice call broadcast to via embedded speakers in the base station to the illegal miners on intrusion detection alert. Security is not merely about arrest; rather creating awareness to abort planned behaviour as some of these illegal miners are well armed with ammunition to fight back on the military. *Label F* is the energy source for the base station. Energy harvesting for WSN is on the rise; given more lifetime to the network. *Label G* is the data storage center. Label H is the artificial neural unit which support the event-driven cameras to first learn their environment and to understand events that are considered as priority frames for recording in a highlight rays at midnight. *Label I* serves as input/output device slots for peripheral devices and operation & maintenance ports. It is called an integrated tower base station system looking at the system units' culmination.

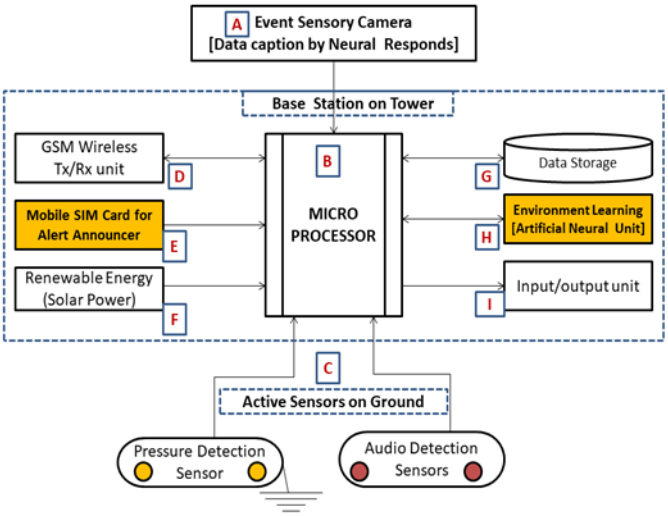

Figure 6: Integrated Tower-based WSN in Forest Surveillance

6. RESULTS AND DISCUSSIONS

The Guyed tower (not shown in the graphical presentations) is a straight rod with wires grounding it on earth for support. To avoid intruders climbing towards the base station on the tower, we suggest using the guyed over the lattice tower type which is self-supported with triangular base for easy climbing. Any intrusion climbing is also sensed and reported at remote monitoring center in the military camp. The sensor nodes are scattered around the forest interest zones to communicate with the base station on the tower using the

RESEARCH ARTICLE

BBC-LEACH routing protocol to attain deployment scalability in wider forest area.

Over the course of the Delphi technique for system analysis with the networking experts, the use of WSN for illegal mining surveillance was 100% significant in their judgement of choice on WSN compared to drones for surveillance in our case study. One respondent during the oral interview recording commented that the use of drones flying in the air will be scary to the peasant farmer from going to the bush for legitimate farming. The attention of community on the operations of the drones is pointer to unproductivity; there are people whose personality is easily distracted for any reason on task and they can watch the drones throughout the day without productive work done. Best quality drones work for 30minutes and have to recharge; whiles professional drones may have extra battery banks to work closer to 20 hours before recharge. As time goes on the battery life drains faster for continuous use. The perceived usefulness factor analysis of WSN for Ad-hoc surveillance received high appraisal. However, one was skeptical as to if network application can deter these aggressive and hungry illegal miners form executing their operations. The perceive-ease-use factor got a higher rating due to the fact that the WSN is not new; it is only an emergent technology in the location of study [23].

One thing ensured during the interview was to hide the source of the design to avoid convenient responses to please the interviewer. No respondent was aware if the designs or models are my conceptual development throughout the interview. There were presented with model options to compare and provide candid judgment based on efficiency and effectiveness in applications. This gives credence to the method applied data gathering using the Delphi technique with the few experts as shown in Figure 4. Delphi technique allows a minimum of five (5) experts to be selected for a study; provided they have experience in that field [22] [24].

We have performed analytical modelling of WSN for surveillance in illegal mining in forest reserves. We found that Planned Behaviour Abortion Tower model is possible to compliment surveillance efforts in the fight against illegal forest mining in the tropics with gold deposits.

7. CONCLUSION

We also observed that designing a special integrated base station for the purpose and mounting it on top of a guyed tower is secured from intrusion attacks on the base action. Comparing the WSN to drone technology for surveillance, there is a significant acceptance of WSN over drones due to limitations assessment of the two surveillance systems. Satellite and GSM links; depending on link availability in the forest can be connected for access at the remote network monitoring center (NMC). Analytical modelling has its inherent limitations on findings and conclusion; our work inherited limitations such as convenient responses form the experts to reduce time for the interview as these men are highly engaging professionals. However, there was prior notice for them to choose appropriate time for the system analysis. Subjectivity cannot be ruled out; although it was highly restricted. It is thereby relevant testing the analytical modelling in real world prototype to improve on reliability of findings. Finally, we have considered here the wireless sensor network application for surveillance on illegal gold mining in forest reserves in Ghana. But the Planned Behaviour Abortion tower can be tried in various fields for generalization as it is built on existing theory by [8]. We have observed that an integrated base station (*bespoke design*) is relevant to suit the purpose and application environment than using *off-the shelf* WSN architecture. There must exist a general and hopeful elegant surveillance tower in the forest to monitor illegal mining activities imparting on water pollution, food security and extinction of some animals due to the search of gold. We have found that planned behavior abortion tower model is key to the solution of illegal mining in deep forest reserves. The tropics are highly vulnerable to the climate change impart; depleting the natural reserves is already having devastating effect which has to stop for urgent land reclamation.

REFERENCES

[1] S. K. Jacobson, J. R. Seavey, and R. C. Mueller, "Integrated science and art education for creative climate change communication," Ecol. Soc., vol. 21, no. 3, p. art30, Sep. 2016.

[2] M. F. Othman and K. Shazali, "Wireless Sensor Network Applications: A Study in Environment Monitoring System," *Procedia Eng.*, vol. 41, pp. 1204–1210, 2012.

[3] World Health Organization, "Cyanide in Drinking-water Background document for development of WHO Guidelines for Drinking-water Quality," vol. 2, pp. 1–26, 2007.

[4] U. S. Agency, I. Development, U. F. Service, and I. Programs, "Ghana Climate Change Vulnerability and," no. June, 2011.

[5] V. Hsu, J. Kahn, and K. Pister, "Wireless communications for smart dust," Electron. Res. Lab. Tech. Memo. M98/2, pp. 1–22, 1998.

[6] "'Operation Vanguard'—A Timely Saviour of our Environment - Government of Ghana." [Online]. Available: http://www.ghana.gov.gh/index.php/media-center/features/3966-operation-vanguard-a-timely-saviour-of-our-environment. [Accessed: 28-Aug-2018].

[7] Y. Zare Mehrjerdi, "RFID-enabled systems: a brief review," Assem. Autom., vol. 28, no. 3, pp. 235–245, Aug. 2008.

[8] "The Wi-fi, wireless security review in finding the best wireless security implementation." [Online]. Available:https://www.tenouk.com/wifisecurityfeatures.html. [Accessed: 24-Aug-2018].

[9] T. Sobh and K. Elleithy, Eds., Advances in Systems, Computing Sciences and Software Engineering. Dordrecht: Springer Netherlands, 2006.

[10] "Welcome to the Mobile Data Management and Applications Website." [Online]. Available: https://web.mst.edu/~mobildat/WMAN/index.html. [Accessed: 24-Aug-2018].

[11] "요청하신 페이지가 존재하지 않습니다." [Online]. Available: http://graduate2.korea.ac.kr/programs/programs01-3-06.jsp. [Accessed: 24-Aug-2018].

[12] D. K. Lobiyal, V. Mansotra, and U. Singh, Eds., Next-Generation Networks, vol. 638. Singapore: Springer Singapore, 2018.

RESEARCH ARTICLE

[13] H. Su and X. Zhang, "Energy-Efficient Clustering System Model and Reconfiguration Schemes for Wireless Sensor Networks," in 2006 40th Annual Conference on Information Sciences and Systems, 2006, pp. 99–104.
[14] H. M. Ammari, Ed., The Art of Wireless Sensor Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.
[15] "Smart Dust: Communication Systems and the Future World |ChaiOne." [Online]. Available: https://chaione.com/blog/smart-dust-communication-systems-and-future/. [Accessed: 24-Aug-2018].
[16] R. M. Howard, R. Conway, and A. J. Harrison, "A survey of sensor devices: use in sports biomechanics," Sport. Biomech., vol. 15, no. 4, pp. 450–461, Oct. 2016.
[17] ChipCon, "Single Chip Very Low Power RF Transceiver with 8051-Compatible Microcontroller," Fea.Kpi.Ua, 2002.
[18] H. M. Ammari, Ed., The Art of Wireless Sensor Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.
[19] I. Ajzen, "The theory of planned behavior," Organ. Behav. Hum. Decis. Process., vol. 50, no. 2, pp. 179–211, Dec. 1991.
[20] G. Elmer, "A diagram of panoptic surveillance," New Media Soc., vol. 5, no. 2, pp. 231–247, 2003.
[21] I. AJZEN, R. Netemeyer, and M. Van Ryn, "The Theory of Planned Behavior," Organ. {Behavior} {Human} {Decision} {Processes}, v, vol. 50, no. JANUARY 1991, pp. 179–211, 1991.
[22] M. R. de Villiers, P. J. T. de Villiers, and A. P. Kent, "The Delphi technique in health sciences education research," Med. Teach., vol. 27, no. 7, pp. 639–643, Nov. 2005.
[23] A. Alomary and J. Woollard, "How Is Technology Accepted by Users? A Review of Technology Acceptance Models and Theories," *IRES 17th Int. Conf.*, no. November, pp. 1–4, 2015.
[24] P. Lai, "the Literature Review of Technology Adoption Models and Theories for the Novelty Technology," J. Inf. Syst. Technol. Manag., vol. 14, no. 1, pp. 21–38, 2017.
[25] Eric, O. O (2018). Routing Protocol Redesign for Scalability in Wireless sensor Network Applications. (Unpublished doctoral thesis). Kwame Nkrumah University of Science and Technology. Kumasi, Ghana.

Authors

Eric Opoku Osei is doing his PhD Computer Science at KNUST, Ghana. His research interest includes wireless sensor network application for sustainable development in Africa, Cloud computing adoption and security in Africa and Educational technologies. Eric is also an assistant Lecturer at the University of Ghana, Legon, Accra.

James Ben Hayfron-Acquah is a PhD holder and senior lecturer at the department of computer science. KNUST, Ghana. He is a commonwealth scholar and received Emerald Highly Recommended Award in 2004 for the publication on Automatic Recognition by Gait and has published extensively.

Michael Asante is a PhD holder and a senior lecturer at the department of computer science, KNUST, Ghana. He has published extensively in computer networks and information security. He is the current Head of Department.