Saleem *et al.*
EURASIP Journal on Information Security (2024) 2024:9
https://doi.org/10.1186/s13635-024-00155-6

EURASIP Journal on
Information Security

RESEARCH **Open Access**

Intelligent multi-agent model for energy-efficient communication in wireless sensor networks

Kiran Saleem[1], Lei Wang[1], Salil Bharany[2*], Khmaies Ouahada[3], Ateeq Ur Rehman[4*] and Habib Hamam[3,5,6,7]

Abstract

The research addresses energy consumption, latency, and network reliability challenges in wireless sensor network communication, especially in military security applications. A multi-agent context-aware model employing the belief-desire-intention (BDI) reasoning mechanism is proposed. This model utilizes a semantic knowledge-based intelligent reasoning network to monitor suspicious activities within a prohibited zone, generating alerts. Additionally, a BDI intelligent multi-level data transmission routing algorithm is proposed to optimize energy consumption constraints and enhance energy-awareness among nodes. The energy optimization analysis involves the Energy Percent Dataset, showcasing the efficiency of four wireless sensor network techniques (E-FEERP, GTEB, HHO-UCRA, EEIMWSN) in maintaining high energy levels. E-FEERP consistently exhibits superior energy efficiency (93 to 98%), emphasizing its effectiveness. The Energy Consumption Dataset provides insights into the joule measurements of energy consumption for each technique, highlighting their diverse energy efficiency characteristics. Latency measurements are presented for four techniques within a fixed transmission range of 5000 m. E-FEERP demonstrates latency ranging from 3.0 to 4.0 s, while multi-hop latency values range from 2.7 to 2.9 s. These values provide valuable insights into the performance characteristics of each technique under specified conditions. The Packet Delivery Ratio (PDR) dataset reveals the consistent performance of the techniques in maintaining successful packet delivery within the specified transmission range. E-FEERP achieves PDR values between 89.5 and 92.3%, demonstrating its reliability. The Packet Received Data further illustrates the efficiency of each technique in receiving transmitted packets. Moreover the network lifetime results show E-FEERP consistently improving from 2550 s to round 925. GTEB and HHO-UCRA exhibit fluctuations around 3100 and 3600 s, indicating variable performance. In contrast, EEIMWSN consistently improves from round 1250 to 4500 s.

Keywords Context-awareness, Border surveillance, ThingSpeak, IFTTT, Twilio, MATLAB, Intelligent decision support mechanism, Energy efficient, Communication routing protocol

---

*Correspondence:
Salil Bharany
salil.bharany@gmail.com
Ateeq Ur Rehman
202411144@gachon.ac.kr
Full list of author information is available at the end of the article

© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

1 Introduction

A pervasive computing environment is a context-aware system based on ubiquitous computing, which is a computational everyday environment that enables devices and people to communicate with their surroundings. Moreover, context-awareness systems consist of sensors that are able to collect data from their environment, interpret it, and, after analyzing, change its behavior according to its environment [1]. In wireless sensor communication networks, addressing the disparity in energy consumption and minimizing delivery latency poses a significant challenge. The battery dependency of sensor nodes presents a challenge in terms of recharging or replacing them once they are deployed in the environment [2]. The depletion of energy in a sensor node has a significant impact on the transmission of data. When the sensor node's energy level is depleted, it undergoes a decrease in its transmission capability, leading to network failure. The importance of implementing a reliable mechanism to prolong the operational lifespan of sensor nodes while maintaining efficient data transmission has become imperative [3]. In addition, wireless sensor networks (WSN) have been proven quite promising, such as in e-health, military, and smart applications for users' daily lives, which have created a smart environment where WSN is involved and embedded everywhere, as shown in Fig. 1 [4–6]. Likewise, the transmission of data is a primary object when dealing with serious situations. Therefore, monitoring and keeping an update on WSN is quite crucial.

Especially when WSN communication encounters numerous limitations, such as limited bandwidth, limited power, limited mobility, and latency issues, within the terrestrial environment [3].

Therefore, in this paper, we develop a context-aware artificial intelligence system for WSNs to overcome the limitations of wireless sensors. Leveraging a combination of context awareness and multi-agent techniques in energy-aware wireless sensor networks for smart environments yields significant advantages.

By continuously monitoring environmental factors, node mobility, and energy constraints, situation-aware agents can dynamically adapt link schedules, optimizing energy efficiency and reducing latency [7]. Multi-agent coordination further enhances network resilience, mitigates interference, and enables intelligent cooperation among wireless sensors. This approach not only conserves energy but also extends network lifetime [1].

Concisely, this paper's contributions are as follows:

- We develop a multi-agent context-aware network provided by the Endsley model in WSNs to resolve energy consumption constraints. We enhance the sensor intelligence by using the BDI reasoning mechanism to avoid latency and data collisions while transmitting the data. Wireless sensors get aware (external knowledge of the environment) of their surroundings by the context-aware paradigm and use the BDI rea-

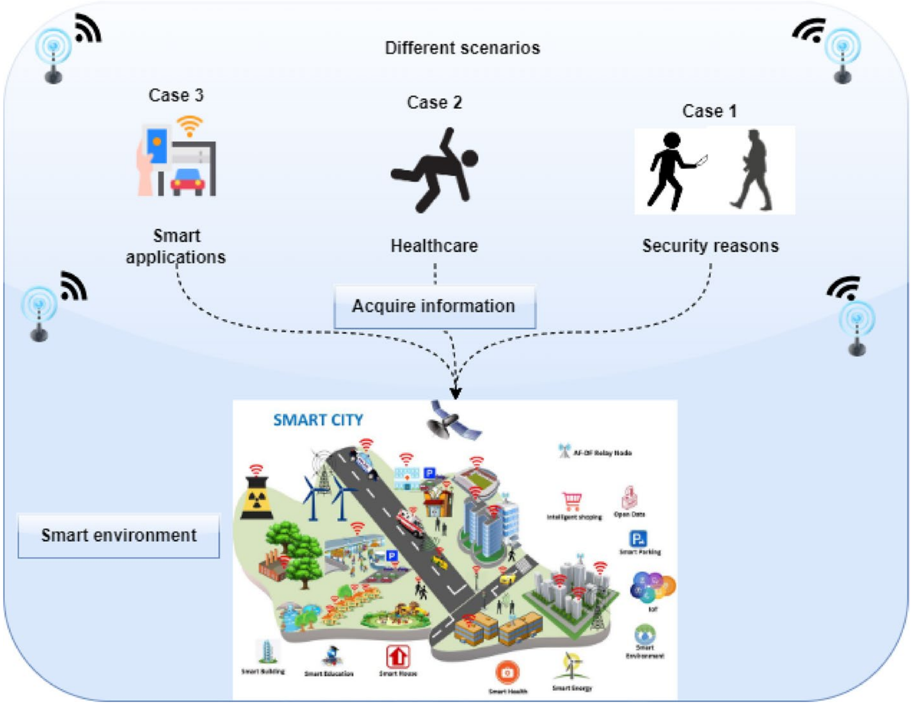


Fig. 1 WSN communication in our daily lives

soning mechanism to find the optimal solution for the dynamic nature problem of the environment.

- We develop a case study for the security border formalism in which sensor nodes can make decisions intelligently without human involvement, adapt themselves according to the environment, and infer a plan within time to prevent the damages caused by suspicious entities.
- The proposed energy-aware intelligent mechanism for WSN enhances the sensor node intelligence among each other. It uses the Endsley model for communication; whenever the node's energy level drops to a certain point, it informs every other node in the network to stop its activities due to energy depletion to avoid unnecessary energy consumption and data transmission.

2 Related review

In the prior work, we solely focused on the WSNs based on emergent situation assessment due to the concept for our case study, emergent situation alerts. Ambient intelligence is vital in healthcare, especially during emergencies such as the COVID-19 pandemic. The paper proposed a situation-aware mechanism using wearable sensors to monitor patients continuously. It employs a belief-desire-intention intelligent reasoning mechanism to detect COVID-19 symptoms early and alert users for self-awareness and precautionary measures. The system utilizes temporal logic, and the proposed framework is modeled and simulated using NetLogo, demonstrating its effectiveness in handling pandemic situations [1]. Likewise, in the past decade, smart computing has gained attention, especially in ubiquitous environments, improving everyday human life. Dynamic interactions with systems using various modalities are facilitated in smart computing. The Multi-Context System (MCS) is crucial for linking diverse context domains in a distributed environment. However, interaction among knowledge sources can lead to inconsistencies and asynchronous communication. This article proposed a framework based on contextual defeasible reasoning in a multi-agent environment to address inconsistent information in MCS. A NetLogo simulation validates the framework, and a Parkinson's disease case study formalism further demonstrates its efficacy [8].

In [9], Bhadwal et al. propose a wireless sensor-based border security system. When suspicious activity is detected, alerts and images are sent to the main system. The system warns the person, and if ignored, it transitions to an auto-combat system, shooting the intruder. The hardware includes stepper motors, a Raspberry Pi interface, and a camera controlled by sensors.

In [10], Nitin et al. introduce a long-range border security system using LDR and ultrasonic sensors. The LDR detects obstacles with beam light, and the ultrasonic sensor observes obstacles that safely cross the beam lights. Rule-based reasoning enhances context-awareness in ambient intelligence (AmI) according to [11]. The approach validates rules, identifies conflicts, and recommends sensors for improved reasoning, combining rule-based systems with ontologies.

Authors [12] propose a technique for reasoning over dynamic contextual information in ambient intelligence. They use a multi-agent approach, incorporating artificial intelligence planning to handle dynamic changes in context. The paper reviews existing techniques and presents a planning and reasoning approach illustrated through a context-aware tourist guide system in ambient intelligent environments.

Building on this foundation, reference A introduces the pivotal role of AI and ML in enhancing the management of smart buildings and energy systems, illustrating how these technologies can be applied to optimize energy consumption and efficiency in WSNs [13]. Similarly, reference D's exploration of energy-efficient UAV flight path modeling for cluster head selection presents a novel approach to extending network lifetimes and improving energy efficiency, offering valuable insights into the potential applications of UAVs in WSN optimization [14]. These studies underscore the importance of integrating advanced technologies and methodologies to address the challenges of energy management and network optimization in WSNs, further enriching our discussion on emergent situation assessment and ambient intelligence.

Algorithm 1 Detection and notification algorithm

```
Input:
Camera Agent: $C^i$, Authorized Person: $AP^x$, Head Officer: $HO^x$, Agent Database: $AO^x$, Controller Agent: $CA^i$, Suspicious Activity: $SA^i$, Image $E^x[img]$, Flag: a numerical value (0 or 1) for system continuation or halt.
Output: Notify OnCall Officer: $OC^i$.
Start
Let $E^x$ be detected by camera sensor, and $AO^x \in CA^i$ database.
for $E^x$ in $C^i$ do
    if $E^x == AP^x$ and $(AP^x == AO^x$ or $AP^x == HO^x)$ then
        if $AP^x \neq SA^i$ then
            return True
        end
    end
    else
        Notify $CA^i$
        for all agents $n$ in $BVS$ do
            if $\exists E^x \leftarrow C^i$ then
                if $E^x == P^i$ then
                    $CA^i \leftarrow C^i$.loc
                    Notify $OC^i$ about $E^x$

                end
            end
        end
    end
end
End
```

3 Core notions of proposed system

3.1 Multi-agent system

Motivational models propose that incorporating principles from human psychology, such as open-ended learning and autonomous skill acquisition, benefits artificial agents. Multi-agent systems and swarms are contextual scenarios, representing a logical progression from individual agents. Software-based intelligent agent models aim to enhance cognitive abilities, enabling agents to engage in deliberative processes and choose advantageous plans for improved decision support systems [1].

3.2 Context-awareness

Originating from pervasive computing in 1994, context-aware computing involves systems that perceive and comprehend their environment, adapting behavior based on contextual cues [15]. This includes factors like proximity of individuals, lighting conditions, ambient noise, social environment, and network connectivity. Advanced knowledge technologies like broadcast connections, sensors, and the Internet of Things contribute to adaptive learning through context-aware technology, crucial for acquiring pertinent contextual knowledge [1, 15].

Algorithm 2 Animal detection and response algorithm

```
Input:
Camera Agent: $C^i$, Animal Image: $A^i$, Auto-Combat System: ACS, Flag: a numerical
value (0 or 1) for system continuation or halt.
Output: Shoot the Animal.
Start
Let $E^x$ be detected by camera sensor.
for $E^x$ in $C^i$ do
    if $E^x == A^i$ then
        if ACS is active then
            Generate Alert
        end
        else
            Shoot the Animal
        end
    end
end
End
```

4 Proposed energy-aware intelligent mechanism for border formalism in WSN

The algorithm is designed for detecting suspicious objects or persons at a country's border. The process involves the camera agent (Ci) sending images to the controller agent (CAi), initially categorizing entities as suspicious. If no suspicious activity (SAi) is detected, no alert is generated. If SAi is identified, an alert is sent to CAi. If the entity is an authorized person (APx), defined as either an army officer (AOx) or head officer (HOx), no alerts are generated. If the entity is neither AOx nor HOx, it is categorized as suspicious, and alerts are sent to CAi.

Algorithm 3 System control algorithm

```
Input:
Flag: a numerical value (0 or 1) for system continuation or halt, Action performed.
Output: System Control.
Start
if Flag == 1 then
    Halt System
end
else
    Continue the System
end
if Action performed then
    Flag = 1
end
else
    Flag = 0
end
```

CAi, upon notification, triggers the system by sending the culprit's location to an on-call officer (OCi). OCi verifies and sends GPS coordinates to on-duty army officers (AOx) to apprehend the culprit. If a suspicious object is identified as an animal, an alert with GPS coordinates is sent to CAi. CAi checks for the availability of the auto-combat system (ACS). If ACS is available, a request is generated to automatically shoot the animal; otherwise, commands are sent to on-duty army officers (AOi x) for manual intervention.

A Boolean flag is used, with 0 indicating the system should continue and 1 indicating a halt. The decision to continue or halt depends on factors like border and armed forces protocols, policies, and the nature of the suspicious entity. The final system state is under human control, determined by the army officer in charge. If the flag is 0, the system continues; otherwise, it is halted.

4.1 Energy-aware intelligent mechanism for WSN in emergent situations

The provided algorithm outlines a communication initiative for a node, referred to as Node^i, within a network. The algorithm considers various parameters to optimize the communication process, such as the desired data (SD_i), source (src_n), and destination (dst_n) nodes, two possible communication topologies (S_{Hop} and M_{Hop}), packet acknowledgment and failure indicators (PA^i and PF^i), transmission and reception powers (tx and rx), distance (dis), delay (d), packet size (PS^i), link availability (LA^i), interference parameters (n and In_p), link availability states (*Running*, *Busy*, *Idle*), total energy consumption (TEC), node energy (E^i), energy depletion ($ED\ src_n$), and a danger level for unsuspicious activity (DL^i).

The algorithm begins by initializing variables and checking if the desired data transmission is required by Node^i. If so, it initializes transmission and reception powers, energy, and packet size. The algorithm then calculates the distance between the source and destination nodes. Based on this distance, it selects an appropriate communication topology, either S_{Hop} or M_{Hop}, and adjusts the transmission power accordingly. If the distance is below a certain threshold, it uses S_{Hop}; otherwise, it employs M_{Hop} and invokes Algorithm 2 for further adaptation.

Subsequently, the algorithm checks the link availability (LA), node energy (E^i), and the danger level for unsuspicious activity (DL^i). It calculates the total energy consumption (TEC). If the link is both idle and running, it proceeds to check reception, interference, and the danger level.

If a danger level is detected, the algorithm assesses the node's energy level. If the energy is sufficient, it transfers data to the destination node; otherwise, it broadcasts an energy depletion message.

Finally, the algorithm handles cases where the link is not both idle and running, checking link availability and recalculating the total energy consumption. In essence, this algorithm aims to make communication decisions based on dynamic factors such as distance, link availability, energy levels, and the danger level for unsuspicious activity, ensuring efficient data transmission while considering the energy constraints of the nodes in the network.

Algorithm 4 Initiative of communication with energy awareness

```
Input: Node$^i$ wants to send data ($SD_i$), Source node ($src_n$), Destination node ($dst_n$), Topology I ($S_{Hop}$), Topology II ($M_{Hop}$), Packet acknowledgment ($PA^i$), Packet failure ($PF^i$), Tx power ($tx$), Rx power ($rx$), Distance ($dis$), Delay ($d$), Packet size ($PS^i$), Link availability ($LA^i$), Number of interference ($n$), Interference+noise power ($In_p$), Link availability parameters ($Running$, $Busy$, $Idle$), Total energy consumption ($TEC$), Energy ($E^i$), Energy depletion ($ED\ src_n$), Danger level ($DL^i$).

Output: Check Topology to adapt.

Initialization:
foreach $Node^i$ in $Nodes^n$ do
    foreach Corresponding authority $\gamma^{i}$ do
        Let $SD_i$ be required by Node$^i$
    end
end
if $SD_i$ required by $Node^i$ then
    Initialize $tx$, $rx$, $E^i$, $PS^i$
    Calculate $dis \rightarrow$ Speed of Sound (m/s) $\times$ Time (s)
    if $dis \leq threshold$ then
        $tx$ assigns 100 dB
        Use $S_{Hop}$
    else
        $tx$ assigns 190 dB
        Use $M_{Hop}$
        Invoke Algorithm 2 $\rightarrow \gamma^{i} (\theta(\alpha^i))$
    end
    Check $LA$, $E^i$, $DL^i$
    Calculate $TEC$

    if $LA$ is Idle && Running then
        Check $rx$, $n$, $In_p$

        if $DL^i$ detected then
            Check $E^i$

            if $E^i$ is sufficient then
                Transfer data to $dst_n \rightarrow \gamma^{i} (\theta(\alpha^i))$
            end
            else
                Broadcast energy depletion message
            end
        end
    else
        Check $LA$
        Calculate $TEC$
    end
end
```

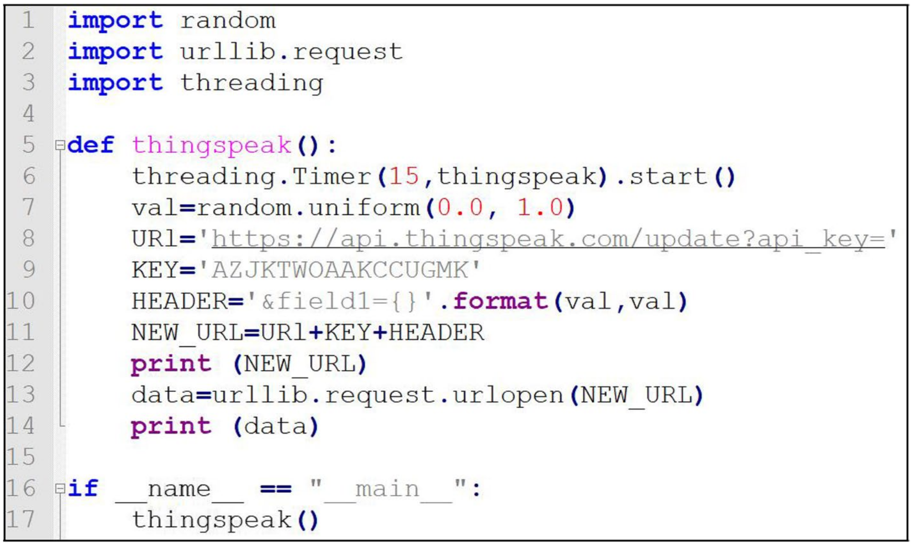
5 Theoretical results for smart surveillance system using ThingSpeak

This section covers the prototypal implementation of the proposed work. The prototype is developed to check the validity and the correctness of this work. The physical implementation of this work is currently not possible due to time, budget, and technical constraints. For prototypal implementation, Spy Detecting, Suspicious Activity Monitoring, and Unauthorized Person agents were developed in python programming language using Notepad++ editor [16]. The agents was connected with the ThingSpeak website channel, which allows the visualization of data sent by the agent. This data is saved on the ThingSpeak cloud [17]. ThingSpeak is integrated with MATLAB thus allowing for the analysis of data received on the ThingSpeak website. MATLAB has also been used to generate an alert email and send it to the user's mail account [18]. Other than this, an alert notification is sent on the user's chosen device with the help of the IFTTT application. The IFTTT application is installed on the chosen device and a notification can be developed on the IFTTT website and sent to the IFTTT application on the device to generate a notification when a specific situation occurs during data acquisition [19]. Furthermore, a message is sent using the Twilio application. This application sends a message on a specified number when a certain condition is met during data acquisition [20].

5.1 ThingSpeak channels

For the prototypal implementation of the proposed work, a ThingSpeak channel by the name of "Smart Border Patrol System (Control Agent)" was made. A Spy Detecting agent gathering data about the person's identity has been developed in python programming language using notepad++ editor for this work. Figure 2 shows the coding of the agent.

Figure 3 shows the channel developed for this work. The figure shows the name of the channel developed, along with the unique channel ID. Every channel in ThingSpeak is provided with its unique channel ID which can be used for accessing the channel during data sending and retrieving. The channel also contains information about when the channel was created, when was it last entry was made, and the total number of entries made in the channel. The access of this channels is made public so that anyone who has the channel ID or the channel link (weblink of the channel, in the web browser search bar) can easily access it. Other than this, the access can be made private so that

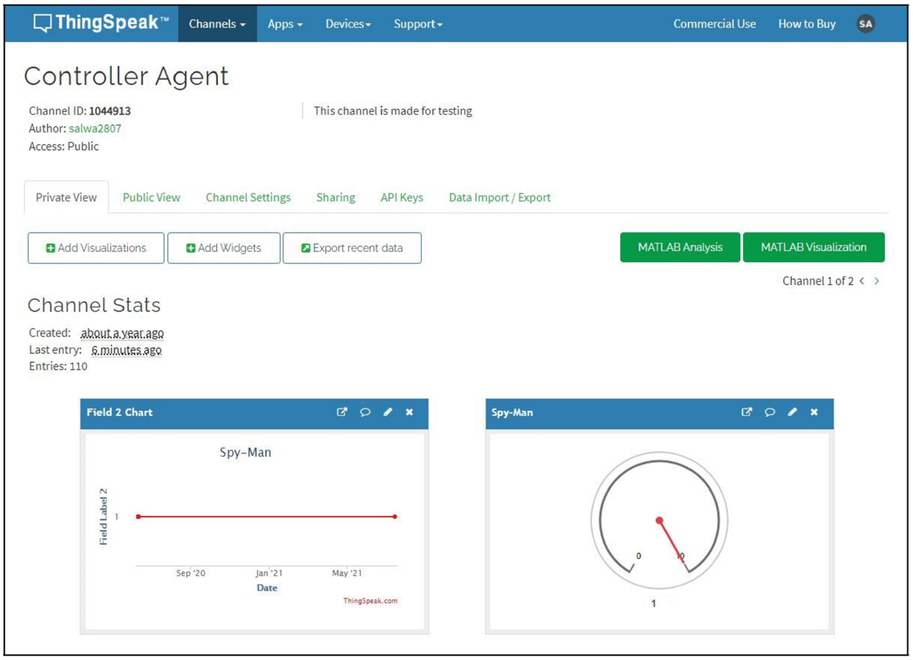


```
import random
import urllib.request
import threading

def thingspeak():
    threading.Timer(15,thingspeak).start()
    val=random.uniform(0.0, 1.0)
    URl='https://api.thingspeak.com/update?api_key='
    KEY='AZJKTWOAAKCCUGMK'
    HEADER='&field1={}'.format(val,val)
    NEW_URL=URl+KEY+HEADER
    print (NEW_URL)
    data=urllib.request.urlopen(NEW_URL)
    print (data)

if __name__ == "__main__":
    thingspeak()
```

Fig. 2 Python code for agent



Controller Agent

Channel ID: 1044913
Author: salwa2807
Access: Public

This channel is made for testing

Channel Stats

Created: about a year ago
Last entry: 6 minutes ago
Entries: 110

Fig. 3 ThingSpeak channel for controller agent

only the user can access it, or the access to the channel can be given to specific people by sending the channel information to their email address.

5.2 ThingSpeak react

ThingSpeak react is an application associated with ThingSpeak. It generates a "reaction" using the data obtained on the ThingSpeak channel. This reaction can be an email, a notification on a device, or a tweet. For this work, an SMS, an email and a notification has been used.

5.2.1 Email

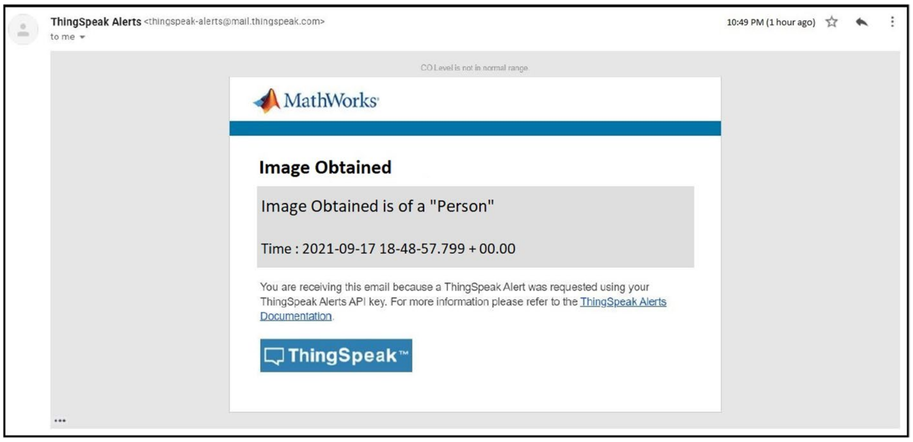
When that received data is above or below a certain point, an email is generated and sent to the email address associated with the owner of the ThingSpeak account, as can be seen in Fig. 4.

5.2.2 Notification

In addition to this, a notification is sent to the device of the account owner. This is done using the IFTTT applet. The connection of the device is established by installing the IFTTT application on the device where the notification is to be received. The connection of the IFTTT with ThingSpeak, the notification generation react creation, the resultant notification received in the notification panel, and the IFTTT application installed in the mobile device can be seen in Figs. 5, 6, 7, and 8 respectively.

5.2.3 SMS

Other than this, an SMS is sent to the device chosen by the account owner. This is done using the Twilio application. This application allows the sending of text messages to a device based on the ThingSpeak channel data. The connection of the Twilio application with ThingSpeak platform, the SMS generation react creation and the resultant SMS received can be shown in Figs. 9, 10, and 11 respectively.



ThingSpeak Alerts <thingspeak-alerts@mail.thingspeak.com>
to me

10:49 PM (1 hour ago)

CO Level is not in normal range

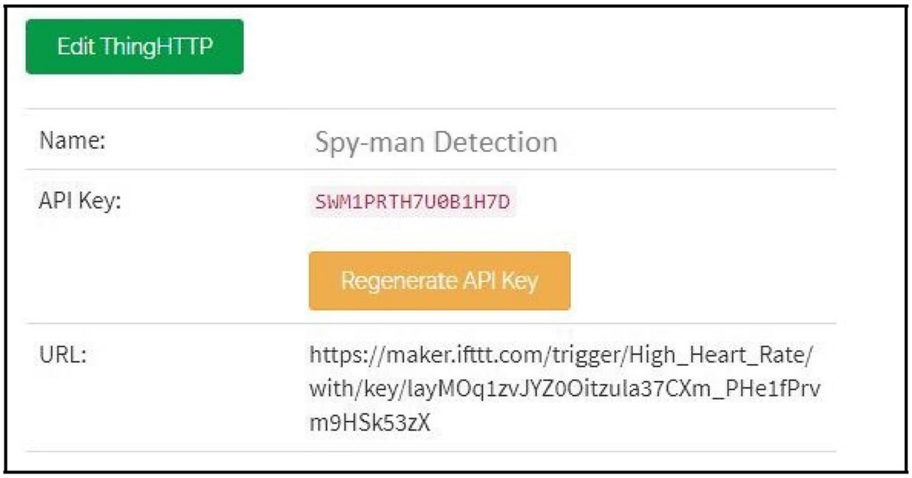
Image Obtained

Image Obtained is of a "Person"

Time : 2021-09-17 18-48-57.799 + 00.00

You are receiving this email because a ThingSpeak Alert was requested using your ThingSpeak Alerts API key. For more information please refer to the ThingSpeak Alerts Documentation.

Fig. 4 Email received

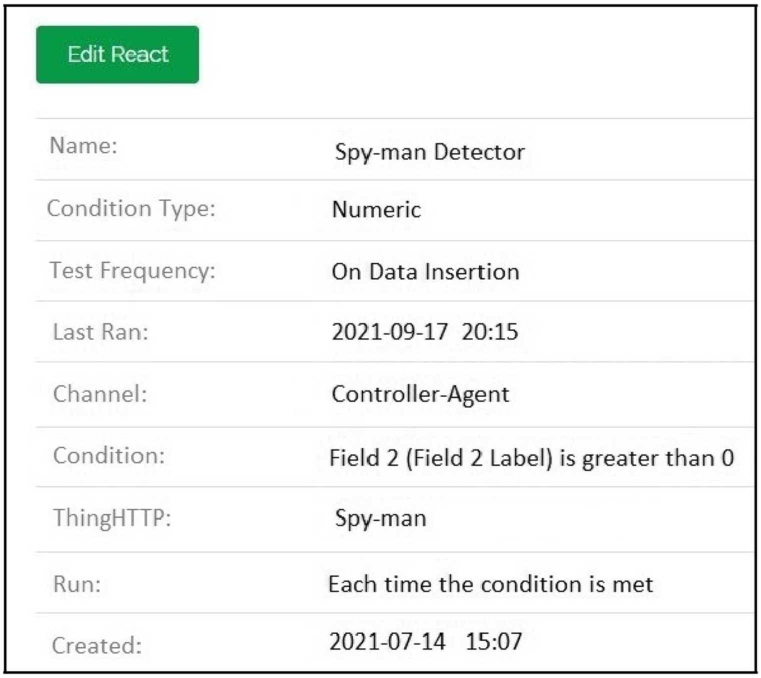


Name: Spy-man Detection

API Key: SWM1PRTH7U0B1H7D

URL: https://maker.ifttt.com/trigger/High_Heart_Rate/with/key/layMOq1zvJYZ0Oitzula37CXm_PHe1fPrvm9HSk53zX

Fig. 5 Notification connection with IFTTT



Name:	Spy-man Detector
Condition Type:	Numeric
Test Frequency:	On Data Insertion
Last Ran:	2021-09-17 20:15
Channel:	Controller-Agent
Condition:	Field 2 (Field 2 Label) is greater than 0
ThingHTTP:	Spy-man
Run:	Each time the condition is met
Created:	2021-07-14 15:07

Fig. 6 Notification generation react

6 Experimental results

This section represents a system requirements and simulation-based performance analysis of the WSN. The experimentation happens in Ubuntu 22.04.2 LTS with the Intel core processor i7 CPU@2.90GHzx16. We use the latest network simulator with 3.37 version to run the experimentation framework for WSN.

In order to transmit the data to the destination node, a network configuration consisting of 100 sensor nodes is shown in Fig. 12.

However, in our proposed algorithm, the primary purpose is to handle the dynamic nature of emergent situations and solve energy consumption in WSN. The sole purpose of using context-awareness is to tackle unpredictable situations in the environment where sensor nodes can learn from the environment and enhance the system intelligence more effectively.

6.1 Definition 1: Acquisition of context

Whenever sensor nodes collect information regarding the context it checks the rules for it where KB^i is a place where the rules are created into the Belief system of node^i $= \beta^{\ i}$, regarding a context $= \phi$ mentioned in the Eq. below:

$$\beta^i \epsilon Knowledge\ base. \tag{1}$$

where,

$$\beta^i \epsilon \begin{cases} Node_E = Node\ Energy \\ Interference = Traffic\ of\ nodes \\ dis_{link} = distance \\ channel_{freq} = Channel\ frequency \\ tx = transmission\ power \\ Emergent_P = P_{1,2,..n} \\ packet_{size} = packet\ size. \end{cases} \tag{2}$$

By using context acquisition, we deal with the energy consumption issue in WSN for emergent situations. For instance, at the time of context acquisition, we get the knowledge of node energy, which effects node depletion.

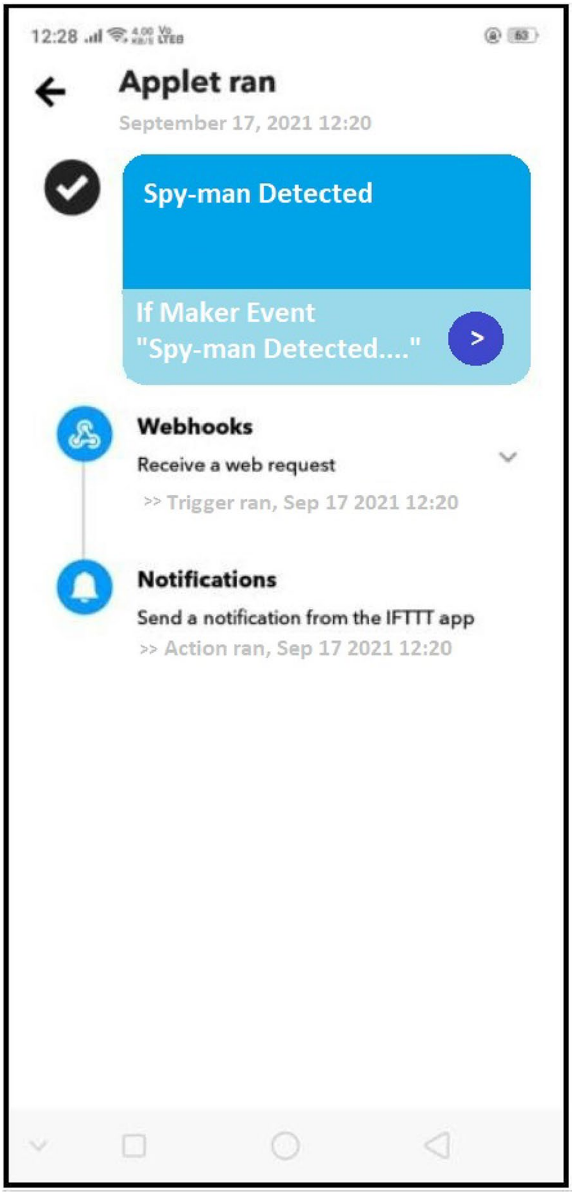
$$\{\ Node_E \propto 1/Node_{depl}. \tag{3}$$

Likewise, we get the knowledge of signal strength in context acquisition, which affects the system or network lifetime.

$$\{\ P_{tx} \propto 1/NLT. \tag{4}$$

6.2 Definition 2: Interpret the data

In that case, we find the emergent situation regarding the border formalism likewise, where the sensor node energy


12:28

Applet ran

September 17, 2021 12:20

Spy-man Detected

If Maker Event "Spy-man Detected...."

Webhooks

Receive a web request

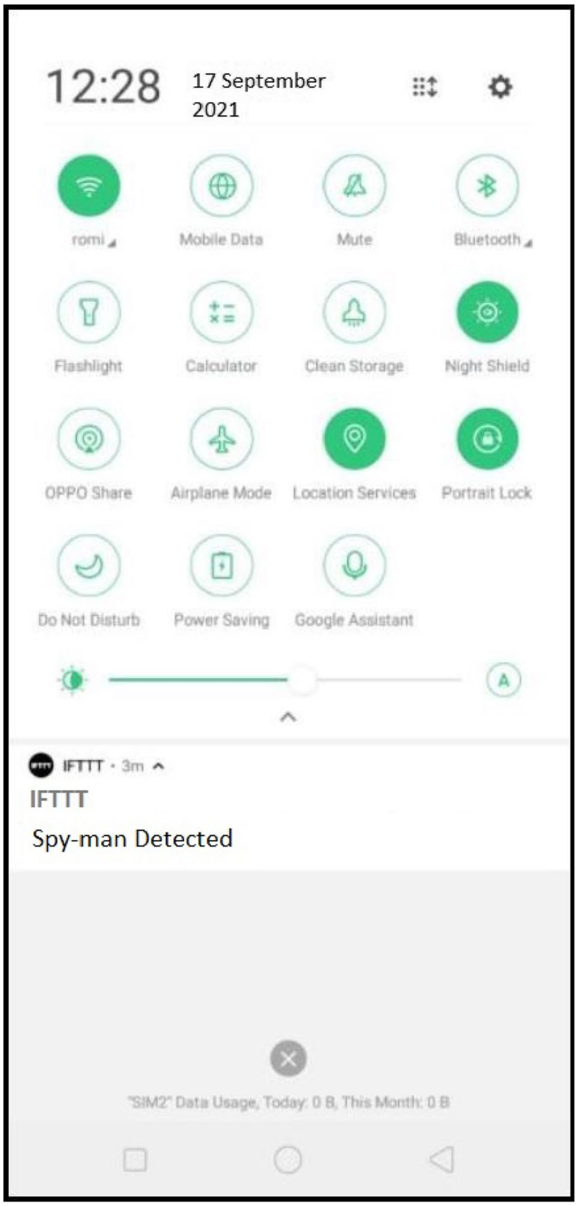
>> Trigger ran, Sep 17 2021 12:20

Notifications

Send a notification from the IFTTT app

>> Action ran, Sep 17 2021 12:20

Fig. 7 Received notification in the IFTTT application



12:28 17 September 2021

IFTTT · 3m

IFTTT

Spy-man Detected

"SIM2" Data Usage, Today: 0 B, This Month: 0 B

Fig. 8 Received notification in the notification panel

is also checked before sending the data in order to avoid compromised situations which can directly have an affect in data transmission.

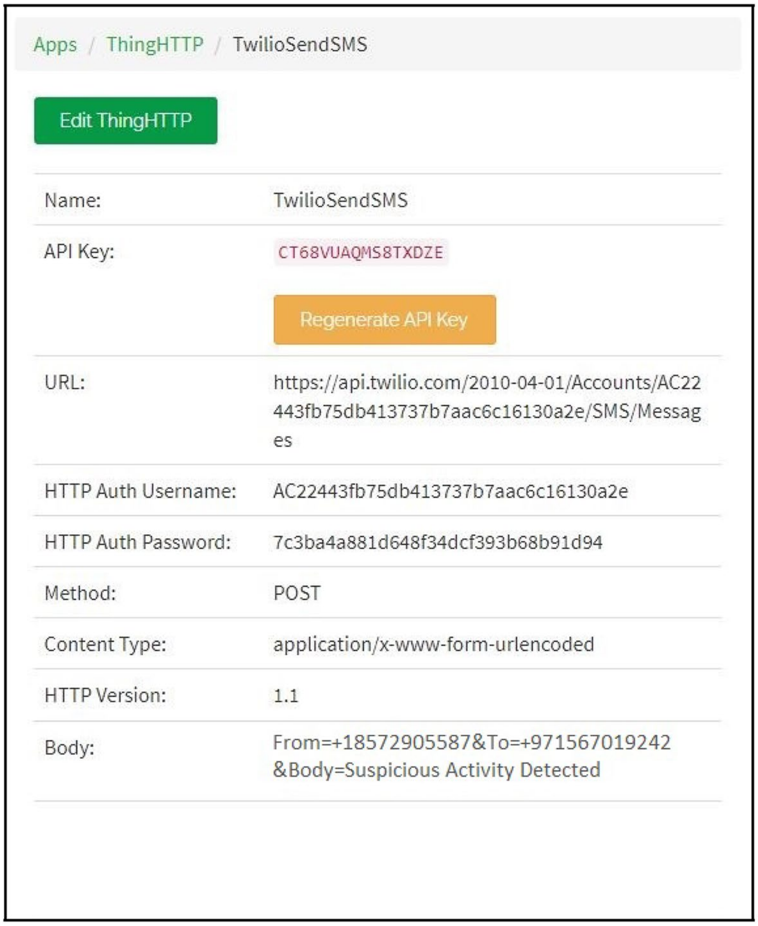
$$\left\{ L_{rate} \propto 1/Data_{transmission}. \right. \tag{5}$$

In addition, we choose the link cautiously to send the data from one point to other. Let us suppose if we choose a busy link to transmit the data in that case, a data collision can occur; therefore, to avoid data collisions, the system gets aware from the network situation before sending the data.

$$\gamma^{i}\left(\theta\left(\alpha^{i}\right)\right). \tag{6}$$

where,

$$\gamma^{i}\epsilon \begin{cases} Energy\ optimzation \\ Link\ optimzation \\ Power\ optimzation. \end{cases} \tag{7}$$



Name:	TwilioSendSMS
API Key:	CT68VUAQMS8TXDZE
URL:	https://api.twilio.com/2010-04-01/Accounts/AC22443fb75db413737b7aac6c16130a2e/SMS/Messages
HTTP Auth Username:	AC22443fb75db413737b7aac6c16130a2e
HTTP Auth Password:	7c3ba4a881d648f34dcf393b68b91d94
Method:	POST
Content Type:	application/x-www-form-urlencoded
HTTP Version:	1.1
Body:	From=+18572905587&To=+971567019242&Body=Suspicious Activity Detected

Fig. 9 ThingSpeak connection with Twilio for SMS generation

6.3 Definition 3: Optimal solution

The optimal solution for energy-aware routing situations in emergent situations is to avoid energy depletion constraints. To do so, each sensor node gets broadcast before the sensor node is dead to avoid data collision, data latency, and network failure which indirectly affects the network longevity.

$$L_s \propto \begin{cases} L_{rate} \propto 1/Data_{transmission} \\ P_{tx} \propto 1/NLT \\ Node_E \propto 1/Node_{depl}. \end{cases} \tag{8}$$

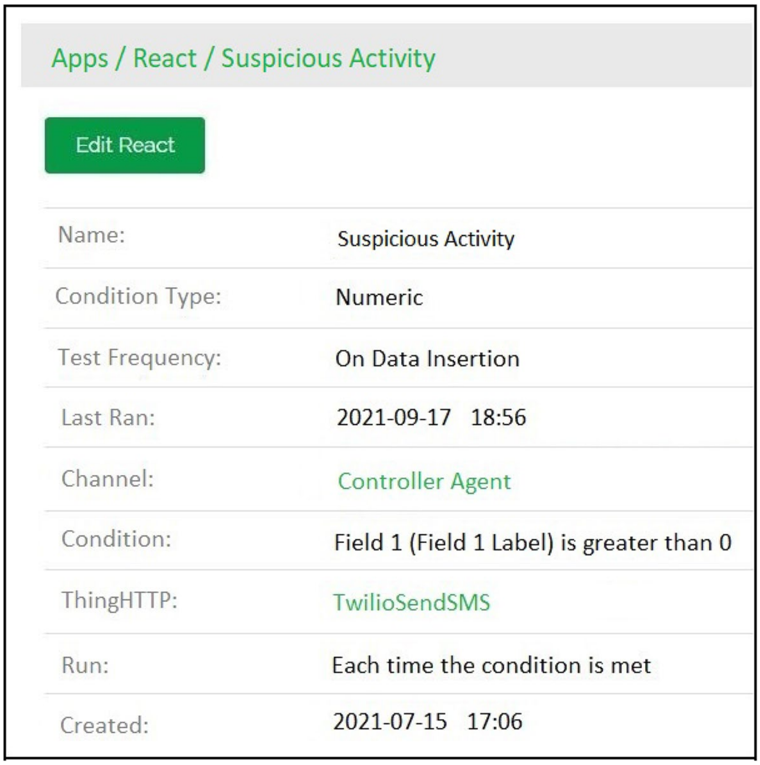
For energy consumption, the network metric we use are as follows:

$$E_{res}(R_k) = E_{init}(R_k) - E_{cons}(R_k). \tag{9}$$

by which,

$$E_{cons}(node_i) \propto \sum \begin{cases} Channel_{acoustic} = \\ Accoustic\ channel\ noise \\ dis_{link} = distance \\ rate_{data} = data\ rate \\ tx = transmission\ power \\ packet_{size} = packet\ size. \end{cases} \tag{10}$$

The end-to-end (E2E) delay is influenced by transmission and receiving delays, along with propagation delay. Notably, dis$link$, rate$data$, tx, and packet$_{size}$ are crucial factors affecting the average delay time. To optimize energy consumption, enhance network lifetime, and improve E2E delay, we employ context-awareness. This involves adapting the transmission power with respect to the distance, allowing for efficient management of resources, aligning with the principles discussed in reference A, which emphasizes the significance of leveraging machine learning and



Name: Suspicious Activity
Condition Type: Numeric
Test Frequency: On Data Insertion
Last Ran: 2021-09-17 18:56
Channel: Controller Agent
Condition: Field 1 (Field 1 Label) is greater than 0
ThingHTTP: TwilioSendSMS
Run: Each time the condition is met
Created: 2021-07-15 17:06

Fig. 10 SMS generation ThingSpeak react

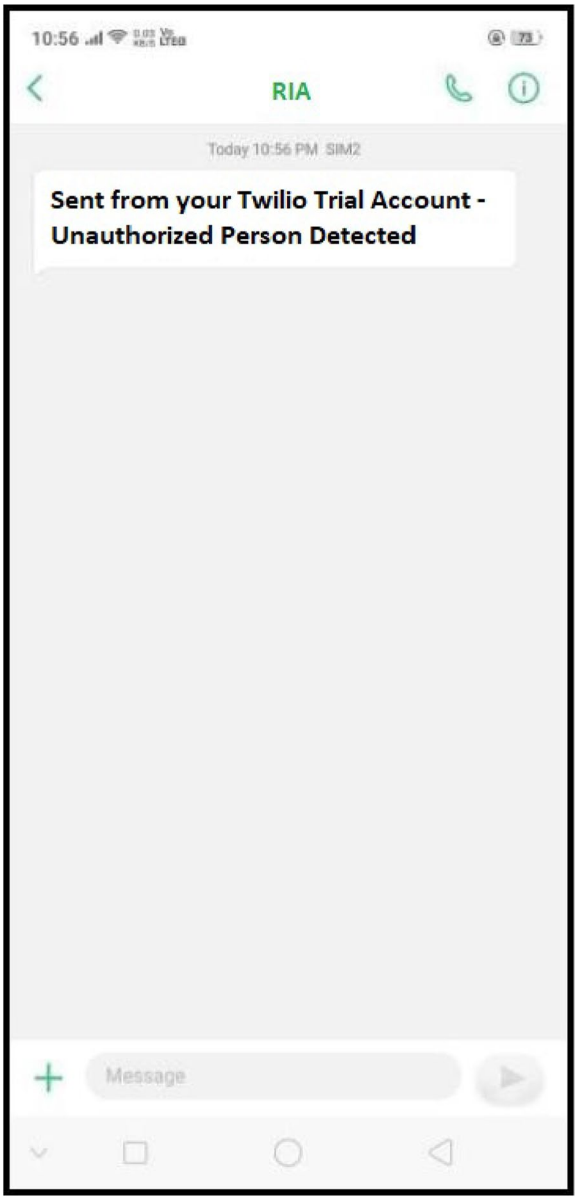
artificial intelligence in smart energy management [13].

6.4 Findings

6.4.1 *Energy optimization*

The Energy Percent Dataset illustrates the energy efficiency of four wireless sensor network techniques (E-FEERP, GTEB, HHO-UCRA, EEIMWSN) over 20 data points, each sending 1000 packets. E-FEERP consistently maintains high energy levels (93 to 98%), demonstrating its efficiency. This aligns with the findings in reference D, where energy-efficient UAV flight path models significantly contribute to optimizing WSN operations [14]. GTEB exhibits stable energy percentages (87 to 91%), while HHO-UCRA maintains reliable energy efficiency (91 to 94%), and EEIMWSN showcases impressive energy utilization (93 to 97%). These results emphasize the effective management of energy consumption by each technique, as depicted in Fig. 13a. The diverse energy efficiency characteristics of each technique are further highlighted by Balouch et al. (2022), who explore optimal scheduling of demand-side load management in smart grids, suggesting a parallel in the importance of strategic energy use [21].

The Energy Consumption Dataset provides insights into the energy utilization of four wireless sensor network techniques (E-FEERP, GTEB, HHO-UCRA, EEIMWSN) measured in joules over 20 data points. E-FEERP consistently demonstrates moderate energy consumption, ranging from 122 J to 130 J, mirroring strategies in smart building management for energy efficiency as discussed in [13]. GTEB exhibits varying energy consumption values from 120 J to 160 J, while HHO-UCRA maintains a relatively stable energy consumption profile, fluctuating between 140 J and 160 J. EEIMWSN showcases efficient energy consumption, with values ranging from 100 J to 112 J. These findings, reflecting the application of context-aware adjustments for energy optimization, are in line with the innovative approach of integrating distributed energy resources for optimal energy scheduling, as outlined by Sharma et al. (2022), providing a new perspective on managing energy in smart grids and WSNs alike [22]. Such insights into the joule measurements of energy consumption highlight the diverse energy



Sent from your Twilio Trial Account - Unauthorized Person Detected

Fig. 11 Received SMS

efficiency characteristics of each technique, as depicted in Fig. 13b, underscoring the broader implications of energy management in the evolving landscape of wireless sensor networks [23–25].

6.4.2 Latency

The dataset comprises latency measurements for four wireless sensor network techniques-E-FEERP, GTEB, HHO-UCRA, and EEIMWSN-within a fixed transmission range of 5000 m. The latency values, recorded over 30 data points, exhibit distinctive ranges for each technique. E-FEERP demonstrates latency ranging from 3.0 to 4.0 s, GTEB exhibits values between 4.0 and 4.5 s, HHO-UCRA displays a range of 3.0 to 5.0 s, and EEIMWSN showcases latency between 2.0 and 3.0 s. These values represent the time taken for data transmission in a single-hop wireless sensor network scenario, providing insights into the performance characteristics of the specified techniques under the given conditions as shown in Fig. 13g and for the multi-hop latency dataset presents 20 data points for E-FEERP, GTEB, HHO-UCRA, and EEIMWSN techniques. E-FEERP exhibits a latency range of 2.7 to 2.9 s, GTEB ranges from 3.6 to 4.2 s, HHO-UCRA spans 3.4 to 3.9 s, and EEIMWSN shows multi-hop latency between 1.7 and 1.9 s Fig. 13h.

6.4.3 PDR

The Packet Delivery Ratio (PDR) dataset reveals the consistent performance of four wireless sensor network techniques (E-FEERP, GTEB, HHO-UCRA, EEIMWSN) across 20 data points, maintaining a transmission range of 5000 m. E-FEERP achieves PDR values between 89.5 and 92.3%, highlighting its reliability. GTEB exhibits stable performance with PDR values ranging from 87.3 to 90.3%. HHO-UCRA demonstrates reliable packet delivery, fluctuating between 88.7 and 92.7%. EEIMWSN consistently performs well, with PDR values varying between 90.5 and 94.4%. These results emphasize the effectiveness of these techniques in maintaining successful packet delivery within the specified transmission range, as illustrated in Fig. 13c. Additionally, the Packet Received Data illustrates the efficiency of each technique in receiving transmitted packets, with E-FEERP, GTEB, HHO-UCRA, and EEIMWSN consistently demonstrating reliable reception performance, as shown in Fig. 13d.

6.4.4 Network lifetime

The result presents observations on network lifetime for E-FEERP, GTEB, HHO-UCRA, and EEIMWSN over five time points. E-FEERP shows a consistent increase, indicating improved network lifetime. GTEB and HHO-UCRA show changes that go up and down, indicating that their performance varies. On the other hand, EEIMWSN consistently goes down, which suggests a potential decrease in its performance

E-FEERP improves consistently from 2550 s. GTEB and HHO-UCRA fluctuate at 3100 and 3600 s, indicating

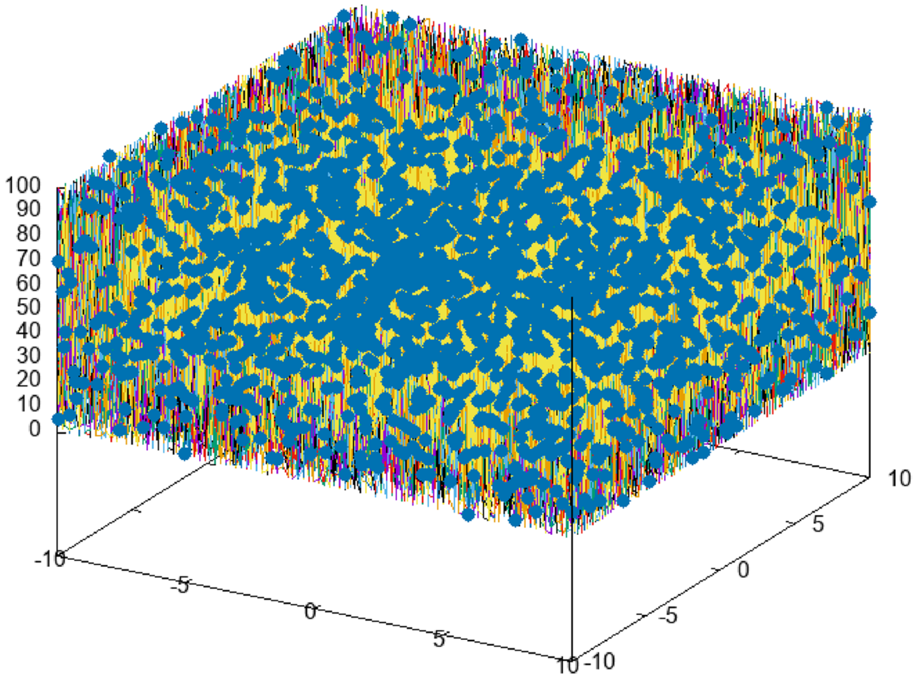


Fig. 12 WSN in an environment

variable performance. EEIMWSN starts at 4120 s, suggesting a potential decline in network lifetime as shown in Fig. 13f. In addition, E-FEERP consistently improves, starting at 910 round and reaching 925 rounds. GTEB and HHO-UCRA show fluctuations in network lifetime, with GTEB varying between 880 and 910, and HHO-UCRA fluctuating between 900 and 940. EEIMWSN, however, exhibits a declining trend, starting at 1250 to 1275 in rounds as shown in Fig. 13e.

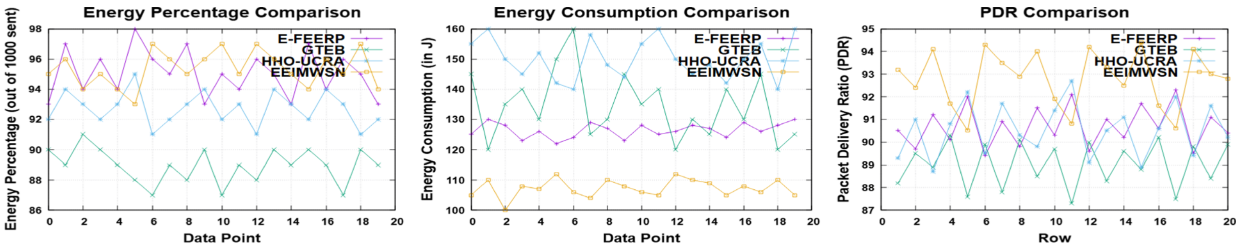
7 Conclusion

In conclusion, this research presents a comprehensive approach to address critical challenges in wireless sensor network communication, particularly in the context of military security applications. The proposed multi-agent context-aware model, utilizing the belief-desire-intention (BDI) reasoning mechanism, demonstrates a sophisticated and intelligent system for monitoring suspicious activities within prohibited zones, leading to timely alert generation. The accompanying BDI intelligent multi-level data transmission routing algorithm contributes significantly to optimizing energy consumption constraints and fostering energy-awareness among network nodes.

The energy optimization analysis, based on the Energy Percent Dataset, highlights the remarkable efficiency of four wireless sensor network techniques (E-FEERP, GTEB, HHO-UCRA, EEIMWSN) in maintaining consistently high energy levels. Notably, E-FEERP stands out with superior energy efficiency, ranging from 93 to 98%, showcasing its effectiveness in managing energy resources. The Energy Consumption Dataset provides a nuanced understanding of the joule measurements, revealing diverse energy efficiency characteristics across the analyzed techniques.

Latency measurements, crucial for assessing real-time performance, demonstrate E-FEERP's ability to maintain low latency values ranging from 3.0 to 4.0 s within a fixed transmission range of 5000 m. The multi-hop latency values further emphasize its efficiency, ranging from 2.7 to 2.9 s.

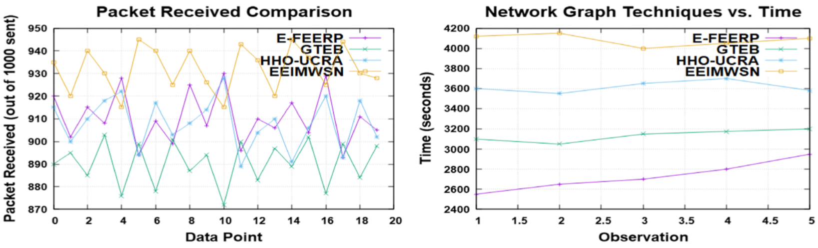
The Packet Delivery Ratio (PDR) dataset underscores the consistent performance of the analyzed techniques in achieving successful packet delivery within the specified transmission range. E-FEERP, in particular, showcases reliability with PDR values ranging between 89.5 and 92.3%. The Packet Received Data reinforces the efficiency of each technique in reliably receiving transmitted packets. Collectively, the proposed model and algorithms contribute significantly to advancing the capabilities of wireless sensor networks in military security applications, addressing energy consumption,



(a) Energy performance% amongst prior methods.

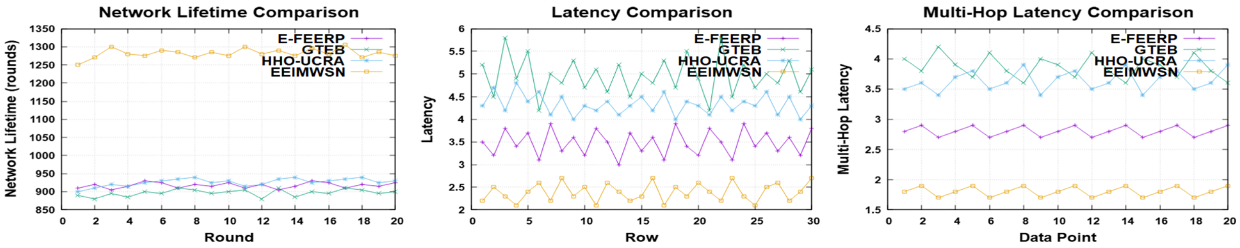
(b) Energy performance J amongst prior methods.

(c) Packet delivery ratio.



(d) Packet received.

(e) Network lifetime in rounds.



(f) Network lifetime in seconds.

(g) Latency performance with single hop.

(h) Latency performance amongst prior methods with multi-hop.

Fig. 13 Theoretical analysis vs proposed system

latency, and network reliability challenges. Furthermore, the network lifetime results reveal continuous improvement in E-FEERP, progressing from 2550 s to round 925. GTEB and HHO-UCRA demonstrate fluctuations around 3100 and 3600 s, suggesting variable performance. In contrast, EEIMWSN consistently enhances its performance, transitioning from round 1250 to 4500 s.

Authors' contributions

K.S., S.B., and L.W conducted the research and collected data. A.U.R, H.H., and K.O. analyzed the data and performed the statistical analysis. K.S and S.B. drafted the manuscript. S.B reviewed and edited the manuscript.

Funding

Not applicable.

Availability of data and materials

No datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Author details

[1]School of Software, Dalian University of Technology, Dalian, China. [2]Independ researcher, Amritsar 143001, India. [3]School of Electrical Engineering, University of Johannesburg, Johannesburg 2006, South Africa. [4]School of Computing, Gachon University, Seongnam 13120, Republic of Korea. [5]Faculty of Engineering, University de Moncton, Moncton E1A3E9, NB, Canada. [6]Bridges for Academic Excellence, Tunis, Centre Ville, Tunisia. [7]Hodmas University College, Taleh Area, Mogadishu, Somalia.

Received: 20 February 2024 Accepted: 20 March 2024
Published online: 08 April 2024

References

1. K. Saleem, M. Saleem, R.Z. Ahmad, A.R. Javed, M. Alazab, T.R. Gadekallu, A. Suleman, Situation-aware BDI reasoning to detect early symptoms of COVID 19 using smartwatch. IEEE Sens. J. **23**(2), 898–905 (2022). https://doi.org/10.1109/JSEN.2022.3156819. PMID: 36913222; PMCID: PMC9983688
2. S. Li, W. Qu, C. Liu, T. Qiu, Z. Zhao, Survey on high reliability wireless communication for underwater sensor networks. J. Netw. Comput. Appl. **148**, 102446–102446 (2019). https://doi.org/10.1016/j.jnca.2019.102446
3. Y. Noh et al., DOTS: A propagation delay-aware opportunistic MAC protocol for mobile underwater networks. IEEE Trans. Mob. Comput. **13**(4), 766–782 (2014)
4. S.M. Akhtar, M. Nazir, K. Saleem, H.M.U. Haque, I. Hussain, An ontology-driven IoT based healthcare formalism. Int. J. Adv. Comput. Sci. Appl. **11**(2), 479–486 (2020)
5. H. Mahfooz Ul Haque, K. Saleem, A. Salman Khan, Modeling belief-desire-intention reasoning agents for situation-aware formalisms. Concurr. Comput. Pract. Experience. **35**(15), e6417 (2023)
6. M. Nazir, H. Mahfooz Ul Haque, K. Saleem, A semantic knowledge based context-aware formalism for smart border surveillance system. Mob. Netw. Appl. **27**(5), 2036-2048 (2022)
7. A. Irfan, R. Taj, K. Inayat, J. Salman, M. Shahrulniza, U.M. Irfan, RACE-SM: Reliability and adaptive cooperation for efficient UWSNs using sink mobility. Front. Mar. Sci. **9**, 2296-7745 (2022). https://www.frontiersin.org/articles/10.3389/fmars.2022.1030113
8. S.M. Akhtar, M. Nazir, K. Saleem, R.Z. Ahmad, A.R. Javed, S.S. Band, A. Mosavi, A multi-agent formalism based on contextual defeasible logic for healthcare systems. Front. Public Health. **10**, 849185 (2022)
9. N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla, A. Kakran, in *2019 international conference on Automation, Computational and Technology Management (ICACTM)*, Smart border surveillance system using wireless sensor network and computer vision (IEEE, 2019), pp. 183-190
10. N. Srivastava, N. Gupta, B. Verma, P. Tiwari, L. Verma, M. Kaur, Border security system. IJRITCC. **5**(5), 283–285 (2017)
11. H. Aloulou, R. Endelin, M. Mokhtari, B. Abdulrazak, F. Kaddachi, J. Bellmunt, in *2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS)*, Detecting inconsistencies in rule-based reasoning for ambient intelligence (IEEE, 2016), pp. 235-240
12. H. Haiouni, R. Maamri, in *2016 International Conference on Advanced Aspects of Software Engineering (ICAASE)*, Context-aware planning for intelligent environments (IEEE, 2016) pp. 1-5
13. T. Mazhar, et al., The role of ML, AI and 5G technology in smart energy and smart buildings management. Electronics. **11**(23), 3960 (2022)
14. S.K. Haider, et al., Energy efficient UAV flight path model for cluster head selection in next-generation wireless sensor networks. Sensors. https://doi.org/10.3390/s21248445
15. B.S. Halakarnimath, A.V. Sutagundar, Multi-agent-based acoustic sensor node deployment in underwater acoustic wireless sensor networks. J. Inf. Technol. Res. **13**(4), 136–155 (2020)
16. E. Gladkauskas, Development of a water activity control and reaction monitoring system for acidolysis and transesterification reactions using immobilized lipases in a rotating bed reactor, MS Thesis, Lund University, Sweden (2019)
17. A.A.H. Mohamad, N.K. Jumaa, S.H. Majeed, ThingSpeak cloud computing platform based ECG diagnose system. Int. J. Comput. Digit. Syst. **8**(01), 11–18 (2019)
18. A. Muqeet, Real-time monitoring of electromyography (EMG) using IoT and ThingSpeak. Sci. Technol. Dev. **8**, 9–13 (2019)
19. A.H. Miry, G.A. Aramice, Water monitoring and analytic based ThingSpeak. Int. J. Electr. Comput. Eng. **10**(4), 3588 (2020)
20. J.I.V. Luna, F.J. Sánchez-Rangel, J.F. Cosme-Aceves, Monitoring system for doors and windows of a data center with IoT. Ingenius. **22**, 72 (2019)
21. S. Balouch, et al., Optimal scheduling of demand side load management of smart grid considering energy efficiency. Energy Res. https://doi.org/10.3389/fenrg.2022.861571
22. S. Balouch, et al., Feasibility of solar grid-based industrial virtual power plant for optimal energy scheduling: a case of Indian power sector. Energies. https://doi.org/10.3390/en15030752
23. D. Jain, P.K. Shukla, S. Varma, Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks. J. Ambient. Intell. Human. Comput. **14**, 10587–10604 (2023). https://doi.org/10.1007/s12652-022-03711-5
24. V. Narayan, A.K. Daniel, P. Chaturvedi, E-FEERP: Enhanced fuzzy based energy efficient routing protocol for wireless sensor network. Wirel. Pers. Commun. **131**, 371–398 (2023). https://doi.org/10.1007/s11277-023-10434-z
25. H.V. Chaitra, G. Manjula, M. Shabaz, A.B. Martinez-Valencia, K.B. Vikhyath, S. Verma, J.L. Arias-Gonzáles, Delay optimization and energy balancing algorithm for improving network lifetime in fixed wireless sensor networks. Phys. Commun. **58**, 102038 (2023)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.