Wireless Networks (2021) 27:747–763
https://doi.org/10.1007/s11276-020-02482-1

Internet of things for healthcare monitoring applications based on RFID clustering scheme

Abdulrahman Abuelkhail[1] · Uthman Baroudi[1] · Muhammad Raad[1] · Tarek Sheltami[1]

Accepted: 12 October 2020 / Published online: 3 November 2020

Abstract

COVID-19 surprised the whole world by its quick and sudden spread. Coronavirus pushes all community sectors: government, industry, academia, and nonprofit organizations to take forward steps to stop and control this pandemic. It is evident that IT-based solutions are urgent. This study is a small step in this direction, where health information is monitored and collected continuously. In this work, we build a network of smart nodes where each node comprises a Radio-Frequency Identification (RFID) tag, reduced function RFID reader (RFRR), and sensors. The smart nodes are grouped in clusters, which are constructed periodically. The RFRR reader of the clusterhead collects data from its members, and once it is close to the primary reader, it conveys its data and so on. This approach reduces the primary RFID reader's burden by receiving data from the clusterheads only instead of reading every tag when they pass by its vicinity. Besides, this mechanism reduces the channel access congestion; thus, it reduces the interference significantly. Furthermore, to protect the exchanged data from potential attacks, two levels of security algorithms, including an AES 128 bit with hashing, have been implemented. The proposed scheme has been validated via mathematical modeling using Integer programming, simulation, and prototype experimentation. The proposed technique shows low data delivery losses and a significant drop in transmission delay compared to contemporary approaches.

Keywords IoT · Tracking systems · RFID · Smart node · Energy consumption · Optimization · Simulation and experiment · Data collection · Clustering

1 Introduction

Coronavirus will have a long-term impact overall world. The most significant impact will manifest itself in the penetration of IT surveillance and tracking. Wireless Sensor Networks (WSNs) become very efficient and viable to a wide variety of applications in many aspects of human life, such as tracking systems, medical treatment, environmental monitoring, Intelligent Transportation System (ITS), public health, smart grid, and many other areas [1]. Radio Frequency Identification (RFID) is a wireless technology with a unique identifier that utilizes the radio frequency for data transmission; it is transferred from the device to the reader via radio frequency waves. The data is stored in tags; these tags can be passive, active, or battery-assisted-passive (BAP). The active and BAP tags contain batteries that allow them to communicate on a broader range that can go up to 1 km for enterprise users and over 2 km in military applications. Unlike battery-powered tags, passive tags use the reader's RF signal to generate power and transmit/receive data [2]. Using WSNs and RFID is a promising solution, and it becomes prevalent in recent years. Its low cost and low power consumption, RFID is easy to install, deploy, and combine with sensors [3]. These features make RFID combined with sensors a viable and enabling technology for IoT.

✉ Uthman Baroudi
ubaroudi@kfupm.edu.sa

Abdulrahman Abuelkhail
g201536490@kfupm.edu.sa

Muhammad Raad
raad@kfupm.edu.sa

Tarek Sheltami
tarek@kfupm.edu.sa

[1] King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

With a wide variety of increasingly cheap sensors and RFID technologies, it becomes possible to build a real-time healthcare monitoring system at low price with very high quality. The RFID system is considered the strategic enabling component for the healthcare system due to the energy autonomy of battery-less tags and their low cost. In addition, RFID can be attached to the monitored items to be recognized, and hence enhancing the efficiency of monitoring and managing the objects [4–7].

Having real-time data collection and management is very important, especially in health-related systems. For instance, the United Nations International Children Emergency Fund (UNICEF) and the World Health Organization (WHO) reported in 2016 that more than 295 thousand women die every year from causes related to pregnancy and childbirth [8]; this is due to the unavailability of timely medical treatments. Moreover, the report stated that the main reasons of cancer-related deaths are due to the late detection of the abnormal cellular growth at the last stage. Many lives can be saved by utilizing real-time IoT smart nodes that can continuously monitor the patient's health condition. Hence, it empowers the physicians to detect serious illnesses such as cancer in the primary stage.

The motivations for the proposed framework are threefold: low cost, high performance, and real-time collection of data. An RFID Reader cannot rapidly get data from tags because of its static nature and short transmission range. Therefore, high power and costly RFID Reader is required to extend the range for quick information gathering. However, this would result in an increase in the price of the framework considering the high cost of RFID Reader with a high transmission range (not less than $500) and the increased expenditure of initiating the connection between backend servers RFID Reader. The question can we limit RFID readers' quantity, while still accomplishing sufficient information accumulation?

Moreover, in customary RFID observing applications, such as tracking luggage in Airlines, an RFID Reader is necessary to rapidly handle many tags at various distances. An RFID Reader can just read tags within its range. Many limitations could negatively affect the data collection's performance, such as multi bath fading and limited bandwidth; these issues can be maintained by transmitting information in short separations through multi-hop information transmission mode in WSNs. Besides, in every data collection system, the most critical challenge is to consider the real-time requirements. Combining RFID Tags with RFID readers and WSNs helps significantly in solving this challenge [9–11].

In this paper, we develop a framework that integrates RFID with wireless sensor systems based on a clustering scheme to gather information efficiently. Essentially, our framework utilizes a smart node proposed by Shen et al. [3]. The smart node contains an RFID tag, reduced function RFID reader (RFRR), and a wireless sensor. The cluster's construction depends on multi-criteria in choosing the clusterhead among smart nodes in the same range. For instance, each node can read the tag ID and battery level of all smart nodes in its range; the node with the highest battery level will be chosen as the clusterhead. The cluster consists of a clusterhead and cluster members; each member in the cluster transmits their tag information to the clusterhead. Then, the RFID readers send the collected data to the backend server for data management and processing. Also, to protect exchanged data from potential attacks, we have applied two levels of security algorithms.

The proposed technique can lend itself to a wide range of applications, for example, collecting data in smart cities, aiming to monitor people's healthcare in large events such as festivals, malls, airports, train stations, etc. The specific contributions of this paper are listed below:

- We exploit the smart nodes to develop an efficient healthcare monitoring scheme based on a collaborative adaptive clustering approach.
- The proposed clustering scheme reduces the reader's burden to read every node and allows them to read only the node within its range. This approach minimizes the channel access congestion and helps in reducing any other interference. It also reduces the transmission delay, thus collecting the information between nodes efficiently for a large-scale system.
- We formulate the clustering problem as a mathematical programming model to minimize the energy consumption and the interference in a large-scale mobile network.
- To protect the collected data by the proposed approach from security threats that might occur during data communication among smart nodes and primary readers, we secure the exchanged data by two security levels.
- We develop a small-scale prototype where we explore the performance of the proposed approach. The prototype is composed of a set of wearable smart nodes that each consists of RFID tag, reduced function RFID reader, and body sensor. Also, all exchanged data among the smart nodes have been encrypted.

The rest of the paper is organized as follows. Section 2 presents the related work on health care monitoring applications. In Sect. 3, the proposed system is discussed, starting with explaining the problem statement followed by the proposed clustering approach. In Sect. 4, the cluster formation is modeled as an integer program. In Sect. 5, we present and discuss the three used methods to evaluate our proposed approach. First, the optimal solution using integer programming is discussed. Given the long-running time required for integer programming, the proposed system is simulated using Matlab, where the local information is employed to construct the clusters. Thirdly, a small-scale prototype is built to test the approach. Finally, we conclude this paper with our findings and suggestions for future directions.

2 Literature review

This section summarizes some of the previous work related to health care monitoring applications. Many researchers have focused on solving this problem by using either RFID or WSN as the short-range radio interfaces. However, very few of these solutions are suitable for the problem (health care monitoring applications for a large-scale system) that addresses a crowded area with high mobility.

Sun Microsystems, in collaboration with the University of Fribourg [12] proposed a web-based application called (RFID-Locator) to improve the quality of hospital services. RFID-Locator tracks the patients and goods in the hospital to build a smart hospital. All patients in the hospital are given an RFID based on wristband resembling a watch with a passive RFID tag in it. All patient's history and treatment records are stored in a centralized secure database. Doctors have RFID-enabled personal data assistant (PDA) devices to read the patient's data determined on the patients' RFID bangles. The results are promising, but too much work is needed in the security and encryption of the collected data.

Dsouza et al. [13] proposed a wireless localization network to follow the location of patients in indoor environments as well as to monitor their status (e.g., walking, running). The authors deploy static nodes at different locations of the hospital that interact with a patient mobile unit to determine the patient's position in the building. Each patient carries a small mobile node that is composed of a small-size Fleck Nano wireless sensor and a three-axis accelerometer sensor to monitor his/her physical status. However, using everybody's smartphone GPS and Wi-Fi is not an energy-efficient solution because it requires enormous power.

Chandra-Saharan et al. [14] proposed a location-aware WSN to track people in a disaster site using a ranging algorithm. The ranging algorithm is based on received signal strength indicator (RSSI) environment and mobility adaptive (REMA).

Like [15, 16], the authors in [17] focused on the healthcare area and provided a survey that shows the current study on RFID sensing from the viewpoint of IoT for individual healthcare also proves that RFID technology is now established to be part of the IoT. On the other hand, the paper reveals many challenging issues, such as the reliability of the sensors and the actual dependence of the reader's node. There are even more advanced solutions in [18]; the authors proposed iHome approach, which consists of three key blocks: iMedBox, iMedPack, and the Bio-Patch. RFID tags are used to enable communication capabilities to the iMedPack block also flexible, and wearable biomedical sensor devices are used to collect data (Bio-Patch). The results are promising, but the study didn't consider monitoring purposes. Another smart healthcare system is proposed in [19] to monitor and track patients, personnel, and biomedical devices automatically using deferent technologies RFID, WSN, and smart mobile. To allow these different technologies to interoperate a complex network communication relying on a CoAP, 6LoWPAN, and REST paradigms, two use cases have been implemented. The result proved a good performance not only to operate within hospitals but to provide power effective remote patient monitoring. The results are promising, but their approach needs more infrastructures of the wired and wireless sensor network.

Gope and Hwang [20] proposed a secure IoT healthcare application using a body sensor network (BSN) to monitor patient's health using a collection of tiny-powered and lightweight wireless sensor nodes. Also, the system can efficiently protect a patient's privacy by utilizing a lightweight anonymous authentication protocol, and the authenticated encryption scheme offset codebook (OCB). The lightweight anonymous authentication protocol can achieve mutual authentication, preserve anonymity, and reduce computation overhead between nodes. The OCB block cipher encryption scheme is well-suited for secure and expeditious data communication as well as efficient energy consumption. The results are promising, but their approach needs infrastructure. Furthermore, an Intelligent Framework for Healthcare Data Security (IFHDS) has been proposed to secure and process large-scale data using a column-based approach with less impact on data processing [21]. The following table comapres the proposed approach with the existing literature. It shows that there is no similar work to the proposed approach.

References	Techniques	F-1	F-2	F-3	F-4	F-5	F-6	F-7	F-8	F-9
[3]	A hybrid RFID and WSN system for efficient data collection	Y	Y	Y	Y	N	Y	N	N	N
[22]	An efficient data collection method in WSN	N	N	Y	N	N	N	N	N	N
[23]	An efficient data collection technique by integrating RFID and WSN	Y	Y	Y	Y	N	N	N	N	N
[24]	Analytical model to analyse the optimal cluster ratio for cluster-based	N	N	Y	N	N	N	N	N	N
[25]	Technique for monitoring emergency Ad-Hoc Networks	N	N	Y	N	N	N	Y	N	Y
[26]	Concurrent data collection trees method in WSN	N	N	Y	N	N	N	Y	N	N
[27]	Method to optimize the clustering structures	N	N	Y	N	N	N	Y	N	N
[28]	A data management technique based on clustering scheme in WSN	N	N	Y	N	N	N	N	N	N
[29]	Energy-efficient routing scheme for dynamic clustering networks	N	N	Y	N	N	N	Y	N	N
[30]	A hybrid RFID and WSN system for efficient data collection	Y	Y	Y	Y	N	N	N	N	N
[31]	A smart real-time healthcare monitoring and tracking system based on mobile clustering scheme	N	N	Y	N	N	N	Y	N	Y
[32]	A data collection method based on mobile edge computing for WSN	N	N	Y	N	N	N	Y	N	N
[33]	Energy-efficient large-scale tracking systems based on mobile clustering scheme	N	N	Y	N	Y	N	Y	N	N
[34]	A data collection scheme based on timer mechanism in WSN	N	N	Y	N	N	N	Y	N	N
[35]	Energy-efficient large-scale tracking systems based on two-level hierarchal clustering	N	N	Y	N	Y	N	Y	N	N
Proposed approach		Y	Y	Y	Y	Y	Y	Y	Y	Y

Feature 1 (F-1): the smart node is a wearable smart node that includes a Reduced Function RFID reader (RFRR), a body sensor (BS), a RFID tag and a microcontroller, where in the RFID reader has a greater transmission range than the RFRR, where in the RFRR reads other smart nodes' tags and stores this data into its own RFID tag

Feature 2 (F-2): aplurality of smart nodes, which integrate radio-frequency identification (RFID) and wireless sensor network (WSN)

Feature 3 (F-3): the clustering scheme in which each node reads the tag id of all nodes in its range and a cluster head is a node which has the highest cost function (e.g. battery level); The cluster consists of a clusterhead and cluster members

Feature 4 (F-4): the data collection scheme in which an RFID reader receives all packets of node data from the CH, and the RFID reader sends the collected information to a back-end server for data processing and management

Feature 5 (F-5): formulating a novel mathematical programming model which optimizes the clustering structures to guarantee the best performance of the network. The mathematical model optimizes the following objective functions: (1) minimizing the total distance between CHs and CMs to improve positioning accuracy; and (2) minimizing the number of clusters which reduces the signal transmission traffic

Feature 6 (F-6): two level security is obtained by when a node writes data to its RFID tag, the data is signed with a signature, which is a hash value, the obtained hash is encrypted with a AES 128 bits shared key

Feature 7 (F-7): mobility where the proposed approach considers the movements of the users while studying its impact

Feature 8 (F-8): formation adaptability, where the proposed approach is changing its formation according to preset thresholds (e.g, battery level)

Feature 9 (F-9): prototype (proof-of-concept), this work presented a small-scale porotype as a proof of concept

3 The proposed system

In this section, the proposed system is discussed, starting with explaining the problem statement followed by the proposed solution.

3.1 The problem statement

During healthcare monitoring of people, the main challenge is to ensure safety, efficient data collection, and privacy. People stay in a bounded area, embedded with various random movements in their vicinity. Different technologies have been suggested to collect data from crowds and can be categorized as Passive and Active sensing. Passive sensing, such as computer vision, does not need any connection with the user. They can aid in movement detection, counting people, and density approximation [36, 37]. However, these approaches fail to deliver accurate identification of individuals in addition to the need for ready infrastructure, which is very costly. There are also some active systems such as RFID tags that can be attached to the individual and obtain user's data. Nevertheless, these systems require an expensive infrastructure for organizing RFID readers at points of data collection [38].

Therefore, to deliver accurate identification of individuals in addition to reduce the cost of the infrastructure and to attain efficient large-scale data collection for healthcare monitoring applications, we suggest employing a system of mobile smart nodes that is composed of RFID and WSN. The mobile smart nodes are clustered to minimize data traffic and ensure redundancy and delivery to the command center. However, clustering RFID nodes into groups comes with many technical challenges, such as achieving accurate positioning, collecting information in each cluster, and reporting this information from clusters head to the server for processing it. In addition, there are also many challenges related to clustering, which is crucial to managing the transmission to avoid interference. Furthermore, the RFID tag is susceptible to malicious attacks; therefore, we implemented two levels of security algorithms to protect the stored data from potential attacks.

3.2 The proposed approach

This section discusses the proposed data collection technique that can efficiently collect the health information (e.g., temperature, heartbeat) and make them available to the backendback-end server in real-time. The main components in our system architecture include smart nodes, RFID readers, and a backend server, as shown in Fig. 1.

The smart node integrates the functionalities of RFID and wireless sensor node. It consists of Body Sensor (BS), RFID tag, and Reduced-Function RFID Reader (RFRR). Unlike standard sensors, BS does not have a transmission function. BS is responsible for collecting the body-sensed data, such as heartbeat, muscle, temperature. The RFRR is an RFID reader with a small range compared to the traditional RFID reader. The protocol is composed of two phases: cluster construction and data exchange.

In the beginning, each node reads the tag particulars (e.g., id, battery level) of all nodes in its range. Then, the node, for example, with the highest battery level, is autonomously nominated as a clusterhead for this group of nodes. All smart nodes initiate a table of the nominees to be the clusterhead of the newly constructed cluster. The clusterhead sends a message to all nodes within its range to inform them that I am a clusterhead to join its group. Secondly, the node accepting the offer from this clusterhead node sends an acknowledgment message; this is important to avoid duplicate association with multiple nodes. This step ends the cluster construction.

Once the cluster is formed, it reads other smart nodes and stores their data into its local tag. The clusterhead tag works as a data storage. Finally, when an RFRR comes across RFID, the stored data are transferred to RFID and the backendback-end server for further processing. This feature helps reach remote nodes and hence enhance the system reliability and reduce the infrastructure cost.

This process is repeated periodically; new clusters are formed, and new clusterheads are selected along with their children. This technique guarantees fair load distribution among multiple devices to attain the network's maximum lifetime and avoid draining the battery of any individual smart node. The pseudo-code for our algorithm is shown below.

THE PSEUDO-CODE FOR THE PROPOSED ALGORITHM

```
Receive CH candidates from an RFID reader
For each CH candidate do
    Find the CH which has highest BL
End for
Choose the CH with highest BL
If it is CH and meet its CM then
    Read data from the cluster member
End if
If it is CH and meet an RFID reader then
    Send its data to the RFID reader
End if
```

Figure 2a demonstrates the timeline of the transactions that are carried out by smart nodes, while Fig. 2b shows the timeline of the transactions carried out between smart nodes and the primary RFID reader.

4 The mathematical model

The ultimate goal of this research is to design an optimum healthcare monitoring application based on the RFID clustering scheme. To meet the practical requirements for applying the system in large-scale environments, the proposed system's energy consumption should be minimum, and communication quality must be high. Therefore, the integer programming model presented below aims to optimize the following objectives:

- Minimizing the total distance between clusterheads (CHs) and cluster members (CMs).
- Minimizing the number of clusters.

The first objective, which is to minimize the total distance between all CHs and their respective CMs, is meant to enhance tag detectability. Also, shorter distances improve the signal quality and reduce the time delay of transmissions within each cluster. For example, in traditional RFID monitoring applications, such as supply chain management and baggage checking in Delta Airlines, an RFID reader is required to process several tags at different distances in a short time frame. An RFID reader can only read tags in its range. Limited communication bandwidth, background noise, multi-path fading, and channel accessing contention between tags would severely deteriorate the performance of the data collection [3].

The second objective is pursued because minimizing the number of clusters reduces signal transmission traffic, lowering the interference between signals. This results in reducing the use of energy and maximizing the lifetime of the network. For instance, RFID tag data usually is collected using direct transmission mode, in which an RFID reader communicates with a tag only when the tag moves

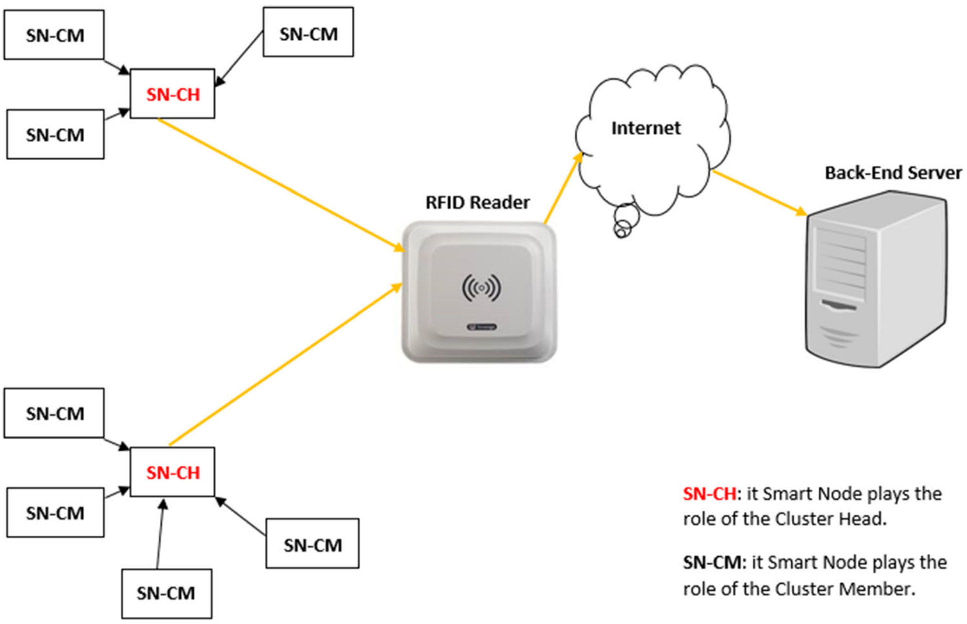

SN-CM
SN-CM
SN-CH
SN-CM
Internet
Back-End Server
RFID Reader
SN-CM
SN-CH
SN-CM
SN-CM
SN-CM
SN-CH: it Smart Node plays the role of the Cluster Head.
SN-CM: it Smart Node plays the role of the Cluster Member.

Fig. 1 The architecture of the healthcare monitoring system

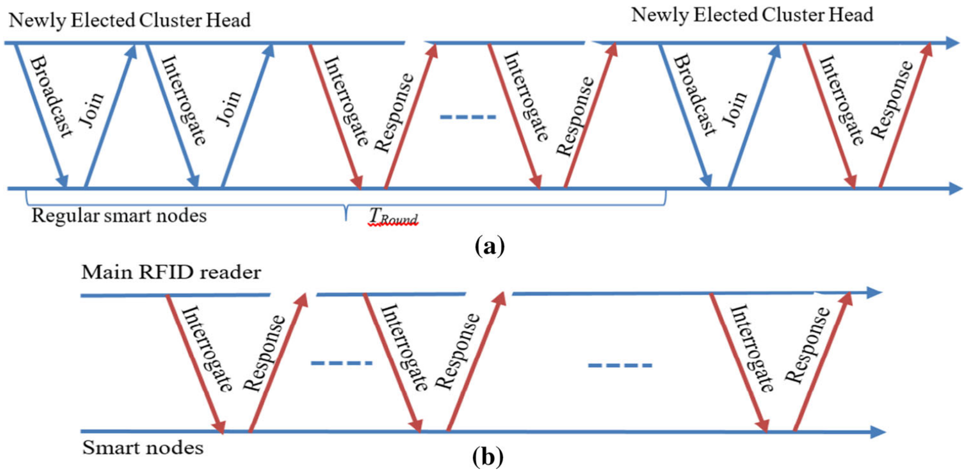


Fig. 2 **a** Timeline of the transactions carried out between smart nodes, **b** timeline of the transactions carried out between smart nodes and the main RFID reader

into its transmission range. If many tags move towards a reader at the same time, they contend to access the channels for information transmission. When a node enters the reading range of an RFID reader, the RFID reader reads the node's tag information. Suppose several nodes enter the range of RFID reader at the same time. In that case, the RFID reader gives the first meeting tag the highest priority to access the channel, reducing channel contention and long-distance transmission interference [38]. In the clusterhead based algorithm, cluster members replicate their tag data to the clusterhead. When a clusterhead of a particular cluster reaches an RFID reader, the RFID reader receives all nodes' information in this cluster. This enhanced method significantly reduces channel access congestion and reduces the information exchanges between nodes. The method is suitable for a wide range of applications where monitored objects (e.g., zebras, birds, and people) tend to move in clusters.

4.1 Definitions

Let i = 1 to n denote the *CM* number, j = 1 to n denote the *CH* number, *Dij* denotes the distance between *CMi* and *CHj*, and *F* denotes the fixed cost per *CH*. The user's battery level (*BL*) is defined as in (1), $\propto$ which is a predefined node energy threshold. Expressions (2) and (3) define the decision variables, *Xij* and *Yj*, which are integer binary variables.

$$BL_j = \begin{cases} 1, & \text{if device } j \text{ has } BL \geq \propto \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

$$X_{ij} = \begin{cases} 1, & \text{if CM } i \text{ is in the cluster of CH } j \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

$$Y_j = \begin{cases} 1, & \text{if node } j \text{ is a CH} \\ 0, & \text{otherwise} \end{cases}. \tag{3}$$

4.2 The Mixed Integer Programming

The complete integer-programming model of the clustering problem is given by (4). The first expression in (4) is the objective function Z, which consists of two terms. The first term is the total distance between CHs and CMs, and the second term is the total number of clusters in the network.

The objective function Z is minimized subject to four sets of constraints. Constraint (I) ensures that every CM has a CH, so we avoid any isolated smart nodes. Constraint II controls the maximum cluster size (CS). Constraint III ensures that all cluster members are within the CH's RFID range, i.e., not more than $\boldsymbol{d_{max}}$ away (e.g., two feet). Finally, constraint IV ensures that a CH node's battery level must be at least $\propto$ (e.g.. 50%). The fixed cost of each CH is denoted by F, which is analyzed later.

$$\begin{aligned} & Min\, Z = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(D_{ij}X_{ij}\right) + F\sum_{j=1}^{n} Y_j \\ & \text{Subject to} \\ & \sum_{j=1}^{n} X_{ij} = 1, \quad i = 1,\ldots,n \\ & \sum_{i=1}^{n} X_{ij} \le CSY_j, \quad j = 1,\ldots,n \\ & \sum_{j=1}^{n} D_{ij} \le d_{\max}, \quad i = 1,\ldots,n \\ & Y_j \le BL_j, \quad j = 1,\ldots,n. \end{aligned} \tag{4}$$

5 Performance evaluation

In this section, the performance of the proposed approach is evaluated using three methods: the integer programming, simulation, and a small-scale prototype.

5.1 Optimum solution

The General Algebraic Modeling System (GAMS) is designed for modeling and solving linear programming (LP), nonlinear programming (NLP), and mixed-integer programming (MIP) optimization problems [39]. Since the above model described in Eq. (4) is a binary integer program, it is solved by the MIP feature of GAMS. We use GAMS Version 24.3.3.

We consider two different scenarios. The first scenario tackles the problem by considering the two terms in the objective function that aims at minimizing the number of clusters and the total distance between *CHs* and *CMs* to find the optimal cluster size (*CS*) in Constraint II. The second scenario applies sensitivity analysis by fixing the total number of nodes to n = 400, 500, 600, 700, and 800; this is done while changing the fixed cost of each *CH*, *F*, and calculating the optimal value of the number of clusters and the total distance as well. Both scenarios are analyzed under the condition that the service region's size is set as 10 * 30 ft^2. To achieve a 95% confidence level, we have repeated each experiment 10 times using different random input for nodes' locations and the battery level for each node.

It can be observed from Fig. 3 that the total distance between the *CHs* and the *CMs* is reduced on average when *CS* is equal 6 (i.e., one clusterhead and five cluster members) for 400 nodes and 500 nodes. The total distance between the *CHs* and the *CMs* is also reduced on average when *CS* is equal 7, 8, 9 for 600 nodes, 700 nodes, and 800 nodes, respectively. For example, with 400 nodes, the minimum accumulated distance between all clusters and their members is about 200 ft when cluster size is equal 6, whereas, with 10 cluster size, it is about 350 ft. Similar to 800 nodes scenario, the minimum distance is about 460 ft when cluster size is equal to 9, whereas, with 5 cluster size, it is about 685 ft and 535 when cluster size is 10. Therefore, the clustering approach is effective in reducing the total distances when *CS* is equal to 6 for 400 nodes and 500 nodes, and 7, 8, 9 for 600 nodes, 700 nodes, and 800 nodes, respectively.

Figure 4 displays the number of clusters while the cluster size is changing. It can be observed that the number of clusters drops when the cluster size increases. However, we are interested not only in minimizing the number of the clusters, but we are also interested in minimizing the total distances between the clusterhead and the cluster member to achieve the accuracy of positioning and maximize the lifetime of the network. For instance, with 400 nodes, the optimum minimum distance is about 200 ft when cluster size is equal 6, and with 800 nodes, the optimum minimum distance is about 460 ft when cluster size is equal 9. Therefore, the optimum value of cluster size is equal to 6 for 400 nodes and 500 nodes, and 7, 8, 9 for 600 nodes, 700 nodes, and 800 nodes, respectively.

Figure 5 demonstrates the model's total distance when the fixed cost per master F is equal to 10^{E}, where E = 0, 1, 2…, 6. For 400 nodes, the optimal (minimum) total distance is 200 ft, which is obtained when F is equal to 100 (E = 2). For the case of 800 nodes, the optimal total

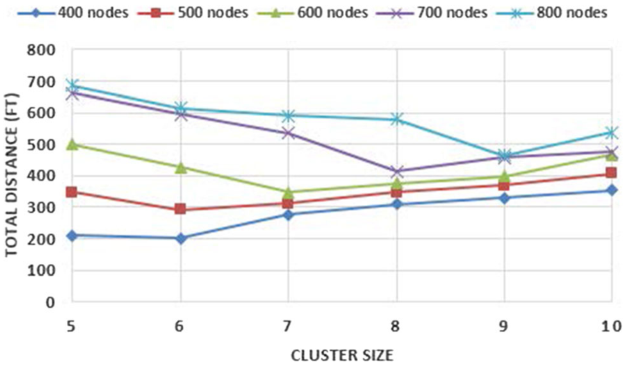


Fig. 3 The average total distance when changing CS from 400 to 800 nodes

distance is 460ft, which is also obtained when F is equal to 100. These numbers indicate that the clustering approach is well-suited for large-scale monitoring applications.

Figure 6 illustrates the optimal number of the clusters when the value of fixed cost per master F is equal to 10^E where E = 0, 1, 2…, 6. For 400 nodes, the optimal (minimum) number of the clusters is 72 clusters, which is obtained when E = 2, or F = 100. For the case of 800 nodes, the optimal number of clusters is 94 clusters, which is also obtained when F = 100. Therefore, the best value of F for both terms in the optimization function in Eq. (4) to work effectively is 100.

5.2 Analytical analysis

In this section, we formulate the energy consumption of the proposed clustering approach and the traditional approach analytically.

In the beginning, we define the following parameters:

R: RFID_Maximum_Data_rate, bps
P_A: RFID_Active_Power, W
P_I: RFID_Idle_Power, W
$T^A_{Tag} = L/R$: RFID tag active time in second, where L is the data length, bits.
T^I_{Tag}: RFID tag idle time, second.
K: Number of clusters.
Cj: Number of members (i.e., smart nodes) in the jth cluster.
β_i: The average number of retransmissions.
T^A_{RFRR}: Reduced RFID reader active time, second.
T^I_{RFRR}: Reduced RFID reader idle time, second.
T_{Round}: Round time, second.

We define the total energy consumption for the traditional approach as follows.

$$E_{Total} = P_A T^A_{Tag} \sum_{i=1}^{N} \beta_i \tag{5}$$

For the traditional approach, $T^A_{Tag} = T_{Round}$. Given the current advancement in RFID technology, we can assume that the collision rate is very low with confidence. Hence, $\beta_i \approx 1$. Then,

$$E_{Total} \approx P_A T_{Round} N \tag{6}$$

For the proposed approach, we define the following specific parameters.E_{CH}: Total Energy Consumption per Clusterhead, E_{Total}: Total Energy Consumption

$$E_{Total} = \sum_{j=1}^{K} E^j_{CH} \tag{7}$$

$$E^j_{CH} = P_A\left(T^A_{RFRR} + T^A_{Tag}\sum_{i=1}^{C_j}\beta_i\right) + P_I\left(T^I_{RFRR} + \sum_{i=1}^{C_j} T^I_{Tag}(i)\right) \tag{8}$$

Given the current advancement in RFID technology, we assume the collision rate to be minimal. Hence, $\beta_i \approx 1$ and $T^I_{Tag}(i) \approx T_{Round} - T^A_{Tag}$, for $\forall i$. Besides, in order not to miss any data, the clusterhead is set on for the whole round period, hence, $T^A_{RFRR} = T_{Round}$ and $T^I_{RFRR} = 0$. Equation (9) can be rewritten as

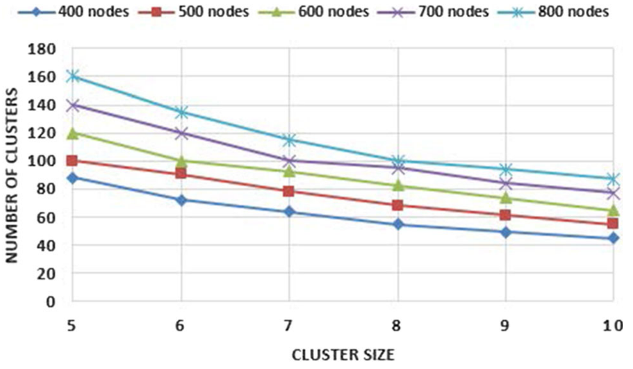


Fig. 4 Number of clusters when changing CS from 400 to 800 nodes

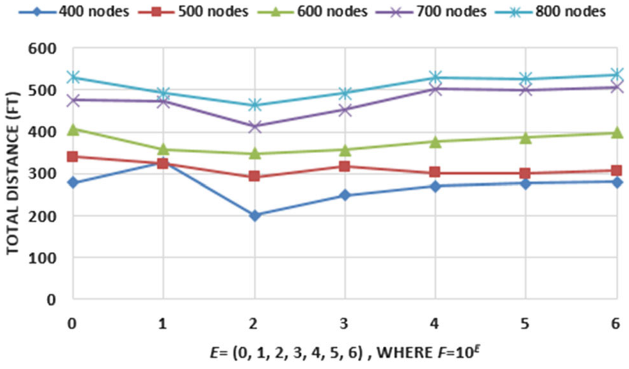


Fig. 5 The total distance when changing F from 400 to 800 nodes

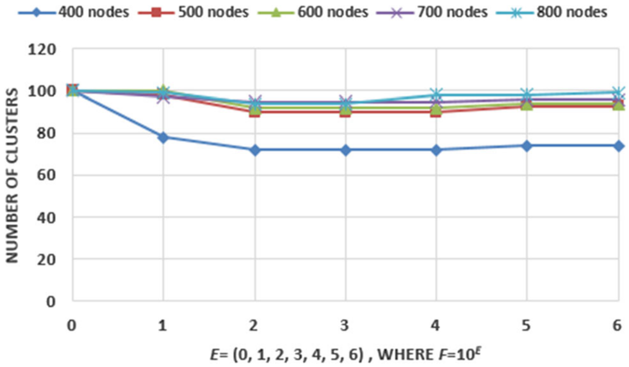


Fig. 6 Number of clusters when changing F from 400 to 800 nodes

$$E_{CH}^{j} \approx P_A\left(T_{Round} + C_j T_{Tag}^{A}\right) + P_I\left(T_{Round} - T_{Tag}^{A}\right)C_j. \quad (9)$$

5.3 Simulation experiments

We have implemented the proposed system for monitoring the health parameters using Cisco Packet Tracer 7.0 since it supports IoT, RFID, and many other functions. Figure 7 shows the smart node components as built using Cisco Packet Tracer. The smart node consists of RFRR, BS, RFID tag, and the microcontroller. The RFRR is a standard RFID reader with a limited range. We program the RFRR to perform two tasks: the first task is reading data from the attached body sensors[1] and storing data into its tag. The second task is reading the data from other smart nodes within its transmission range and storing it into its tag. The body sensor is responsible for collecting body-sensed data such as temperature, heartbeat. The RFID tag works as data storage. On the other hand, the microcontroller (MCU) is used to monitor, verify, and process smart nodes readings.

The transmitted data between smart nodes and RFID readers has three fields. A unique smart node ID assigned to each user (1 byte), the sensed-data (1 byte), and the timestamp, which records the time at when the data is collected (2 bytes). Furthermore, to protect the collected data from potential attacks, we apply Rivest-Shamir-Adleman (RSA) algorithms [37].

Figure 8 shows the components of the RFID reader and its connectivity with the backend server. The RFID readers are responsible for collecting the data from smart nodes and delivering them to the backend server. The transmission range of the RFID reader is much greater than that of the RFRR. Upon reading the smart node tag data, it sends that data directly to the backend server wirelessly carried by UDP packets. Rivest-Shamir-Adleman (RSA) algorithms are also applied for the transmitted data from smart nodes to primary readers.

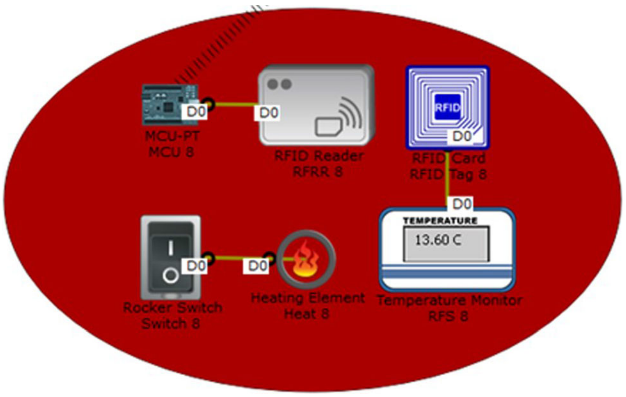


Fig. 7 The smart node components as built-in packet tracer

Using the above setup, we start by studying the performance of the packet delay, and the number of delivered packets have been calculated for the traditional approach and the cluster approach. In the traditional approach, every node sends its packets directly to an RFID reader. In the clustering approach, every node sends its packets to its clusterhead, and the clusterhead forwards them to an RFID reader. Each node sends ten packets every minute, and the simulation has been tested for 10 min to achieve a 95% confidence interval.

The average delay per packets is calculated using Eq. (10), where n is the number of delivered packets and R_t is the receiving time and S_t is the sending time.

$$\text{Average delay per packet} \quad = \frac{1}{n}\sum_{1}^{n}(R_t - S_t) \quad (10)$$

Table 1 shows a sample of the collected data at the backend server before and after implementing the RSA algorithm. The smart node appends the timestamp to the sensed data[2] and stores the information in its tag through RFRR. As stated before, the transmitted data between smart nodes and RFID readers has three fields, namely, unique smart node ID, the sensed data, and the timestamp when the data was collected.

Figure 9 illustrates the average transmission delay per packet for a different number of nodes. We can notice that the traditional approach's delay per packet is almost fixed regardless of available smart nodes. This behavior can be attributed to the fact that each node would meet the RFID readers for forwarding its packets with equal probability. On the other hand, when the clustering approach is employed, the delay drops significantly; for example, when n = 30, the packet delay drops by 63%. The higher is the number of smart nodes, the lower is the packet delay; this happens because when the number of smart nodes increases in the same area, the density increases, as well as the

[1] In this setup, a temperature sensor is used.

[2] In this setup, a temperature sensor is used.

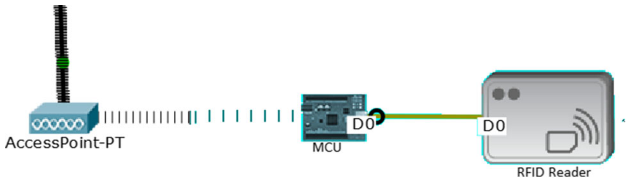


Fig. 8 The components of the primary RFID reader, as implemented in the simulation setup

number of clusterheads. Therefore, the probability of a regular node meets a clusterhead increases, which leads to reduce the delay in delivering the collected data to the primary reader and then to the back-end-server.

Figure 10 displays the number of delivered packets for different numbers of nodes. In the clustering approach, the system delivers exactly 300 packets, which are the total number of packets generated by all smart nodes. On the other hand, in the traditional approach, the system suffers packet loss (e.g., 20% loss for n = 30) due to the increase in channel access congestion as the number of nodes increases.

Next, we study the traditional approach's energy consumption, the optimal approach, and the proposed clustering approach. In the traditional approach, every node sends its packets directly to an RFID reader. In the clustering approach, as explained in Sect. 3.2, every node reads the tag particulars (battery level[3]) of all nodes in its range. The node with the highest battery level is then chosen as a clusterhead for this group of nodes. Then, the clusterhead broadcast a message to all nodes within its range to inform them that I am a clusterhead to join its group. Then, the node accepting this clusterhead node's offer sends an acknowledgment message; this is important to avoid duplicate association with multiple nodes. Once the cluster is formed, the clusterhead remains active, and the cluster member remains in sleep mode. The clusterhead reads other smart nodes and stores their data into its local tag. The cluster member switches to active mode every 10 s to store its data into its own local. Finally, the clusterhead sends the data to an RFID reader, then to the backend server for further processing and management. This process is repeated every 1 min; new clusters are formed, and new clusterheads are selected along with their children. This technique guarantees fair load distribution among multiple devices to attain the maximum lifetime of the network and avoiding draining the battery of any individual smart node.

The relative performance of the three methods has been evaluated using Matlab. It is assumed that each node can send data traffic at a rate of 250 kbps, and it can send frames with sizes up to 4 bytes (one byte for the ID tag number, one byte for the data (heartbeat) and two bytes for timestamp and sequence number). Table 2 shows the RFID hardware energy consumption parameters, as specified by Sparkfun [40]. In order to achieve a 95% confidence interval, each simulation experiment was repeated 10 times using different random topologies. For each simulation run, the total energy consumption for each round was calculated for different values of the number of nodes (N = 400, 500,…, 800).

Table 1 A sample of the collected data at the backend server

Smart node ID	Temperature	Time stamp
4	30	0:5:58
10	39	0:6:58
5	28	0:6:07
2	13	0:5:40
7	16	0:6:35
11	41	0:7:05

Figure 11 and Table 3 show the average total energy consumption for the traditional approach, the clustering algorithm, and the optimal GAMS solution of the integer programming model. Figure 11 shows that the clustering solution's total energy consumption is close to the minimum total consumption obtained by the optimal GAMS solution. The clustering algorithm's total energy becomes closer to the optimal value as the number of nodes increases. This result is clear from Table 3, which shows a difference of 8% between the clustering algorithm's performance and the optimal GAMS solution when the number of nodes is equal to 400, but only a difference of 3.26% when the number of nodes is equal to 800. This feature shows that the proposed clustering algorithm can produce high-quality, near-optimum solutions for large-scale problems. As shown in Table 3, the traditional approach's energy consumption is 455.14% higher than the optimal consumption specified by GAMS when the number of nodes is equal to 400, and 741.07% higher when the number of nodes is equal to 800. The traditional approach (without clustering) is not a practical solution method for large-scale systems.

5.4 Prototype setup and results

In this section, we evaluate the performance of the proposed approach using a small-scale prototype. We begin by describing the experimental setup and then discuss the experimental results.

[3] It can easily be generalized to include other parameters such as service time.

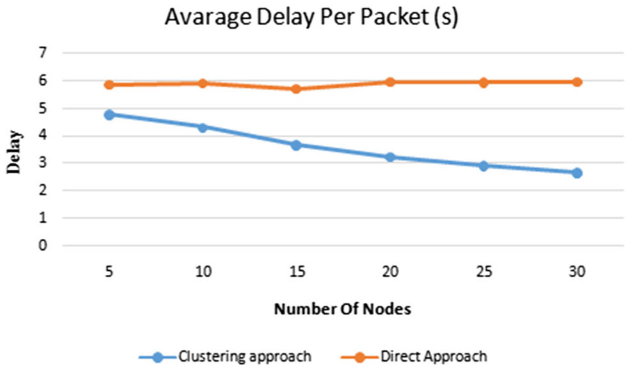


Fig. 9 Comparison of the average transmission delay

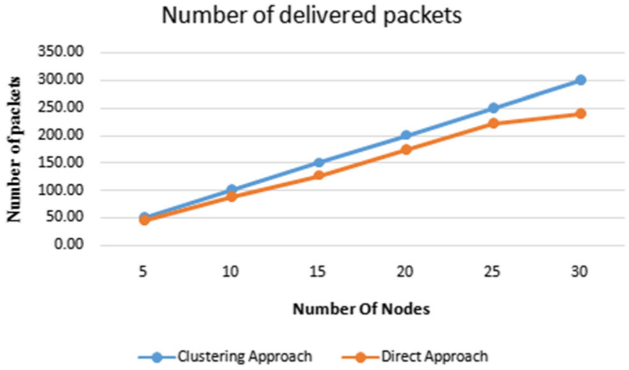


Fig. 10 Comparison of delivered packets

Table 2 Simulation parameters and values [40]

Parameter	Values	Comments
P_A	0.84 W	RFID power in active mode
P_I	0.00025 W	RFID power in sleep mode
R	250 Kbps	RFID data rate

5.4.1 Experimental setup

Figure 12 shows the smart node components in our prototype testbed. The smart node consists of RFRR, BS, RFID tag, and the microcontroller. The RFRR is a standard RFID reader with a limited range, which can read up to two feet as in spark fun specification with onboard antenna [40]. We program the RFRR to perform two tasks. The first task is reading the heartbeat, and the muscle sensed data from the BS (via pulse sensor, and muscle sensor), respectively, and storing this data into its tag. The second task is reading the data from other smart nodes within its transmission range and storing it into its tag. BS is responsible for collecting the body-sensed data such as heartbeat and muscle data. The RFID tag works as a packet memory buffer for data storage. Arduino's read board is a microcontroller that is used to monitor, verify, and process smart nodes readings. The transmitted data between smart nodes and RFID readers has three fields, smart node ID, the sensed data, and the sequence number of the data to know when the data was recorded.

5.4.2 Data structure

For each node, three packets of data are needed to be published so that other nodes can get their information. Therefore, we need only four bytes of data entries: node ID (1 byte), heart rate information (1 byte), and the sequence number (2 bytes). The sequence number helps in discovering how recent the carried information is, and helps other nodes in deciding whether to record newly read data or discard it.

Each RFID tag has a 64-byte capacity; the first 48 bytes are divided into chunks of 4 bytes where each is used to store information of one node, this sums to a total of 12 data slots. The remaining 16 bytes are used for authentication. The first data slot is reserved for one's tag. Other data slots are initially marked as available; that is, they do not contain data about other nodes and are ready to be utilized for that purpose. Figure 13 shows the flowchart that presents the process of handling new data. When a new data arrives and is to be stored, the controller tries to find whether a slot that contains data for the same ID exists. If so, the slot is updated if the sequence number is less than the new sequence number; otherwise, the new data is discarded. If the controller does not find a previous record for that ID, it stores its data in a new available slot, which means some data to be lost.

5.4.3 Security policies

We implement two levels of security algorithms to ensure the integrity of the arrived data, as well as to authenticate the source of data in our scheme. When a node writes the 48 bytes data into its tag, the data is signed with 16 bytes signature, which is used for authentication. To obtain the signature, the controller calculates the MD5 128 bits hash value of the 48 data bytes. Then, the obtained hash is encrypted with the AES 128 bits shared key. The result is the signature and is stored on the tag. To verify a newly read tag, the controller computes the hash of the new data (but not the signature), encrypts it with the shared key, and compares the result with the signature. The new data is valid if the result and its signature match each other. Otherwise, it is considered an invalid node, and its data is discarded.

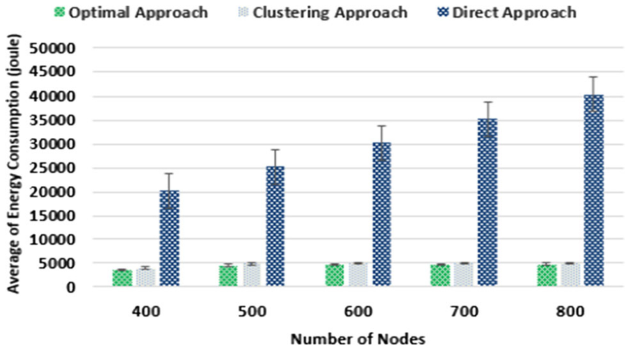


Fig. 11 Comparison of the average energy consumption

5.4.4 Prototype experimental results

The experimental prototype consists of three smart nodes (1, 2, 3) and one primary RFID reader, as shown in Fig. 14. Each smart node consists of RFID tag, microcontroller, pulse sensor, and RFRR, a regular RFID reader with a limited range, which can read up to two feet with an onboard antenna. The primary RFID reader is an RFID reader attached to an external antenna to increase its transmission range. In this prototype, node 3, which has the highest battery level, plays the role of the clusterhead, and node 1 and node 2 play the role of the cluster members. Node 3 reads tag information of node 2 and node 3. Then, the primary RFID reader receives all packets of node 1, node 2, and node 3 from node 3 when it moves into the primary RFID reader range. Then, the RFID reader sends the collected information to the backend server for data processing.

Figure 15 shows a sample of the collected data of the pulse sensor that includes the beat per minute (BPM), live heartbeat or interbeat interval (IBI), and the analog signal (AS) on the serial monitor. Each row in Fig. 15 includes BPM, IBI, and AS. For instance, the first row has 78 as BPM, 1670 as IBI, and 491 as AS. The typical readings of the beat per minute of the pulse sensor should be between 60 and 100. Otherwise, it is considered an emergency case.

It can be observed from Figs. 16 and 17 that a valid foreign tag # 1 is read and updated, and a valid foreign tag# 2 is read and then updated on the serial monitor, respectively. To verify a newly read tag, the controller computes the hash of the new data (but not the signature), encrypts it with the shared key, and compares the result with the signature. The new data is valid if the result and its signature match each other. Otherwise, it is considered an invalid node, and its data is discarded. Figures 16 and 17 shows that tag# 1 and tag# 2 are valid.

Table 3 Total energy consumption (joule) of three solution methods

No. of nodes	Clustering approach	Traditional approach	Optimal approach GAMS	Comparison versus GAMS	
				Clustering approach (%)	Traditional approach (%)
400	3936.2	20,160	3631.5	8.39	455.14
500	4844.7	25,200	4539.4	6.73	455.14
600	4896.7	30,240	4641.03	5.51	551.58
700	4948.6	35,280	4742.6	4.34	643.89
800	4950.2	40,320	4793.9	3.26	741.07

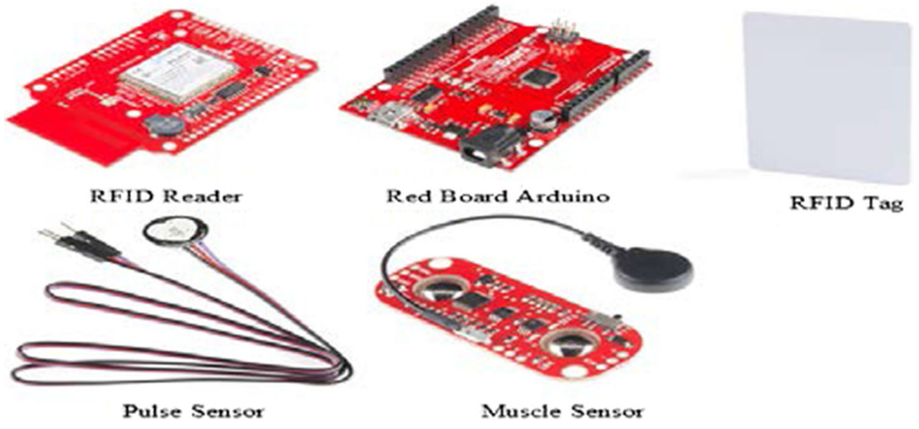


Fig. 12 The components of smart nodes

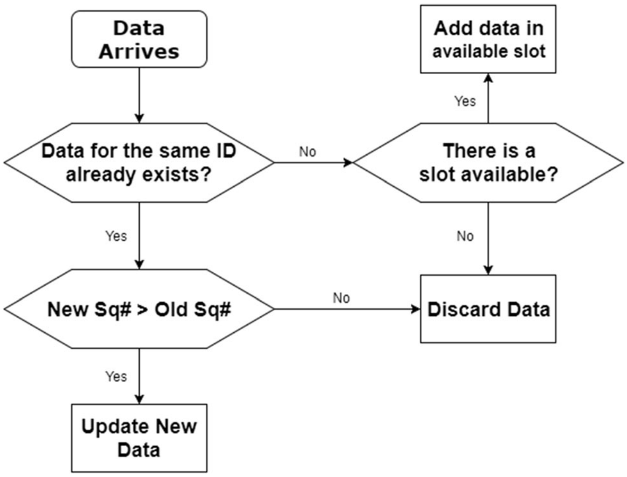

Data Arrives
Data for the same ID already exists?
No
There is a slot available?
Yes
Add data in available slot
Yes
No
New Sq# > Old Sq#
No
Discard Data
Yes
Update New Data

Fig. 13 Flowchart of the process of handling new data

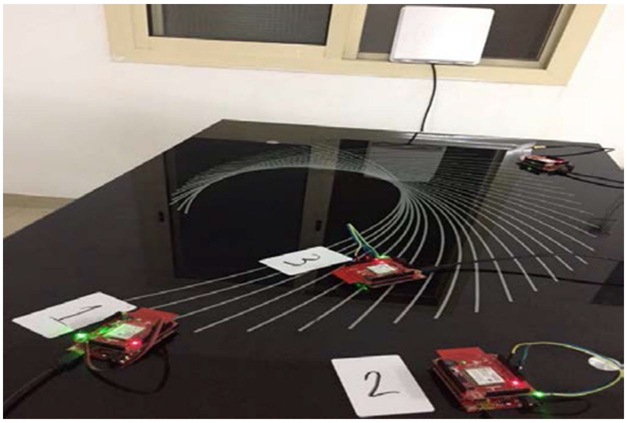


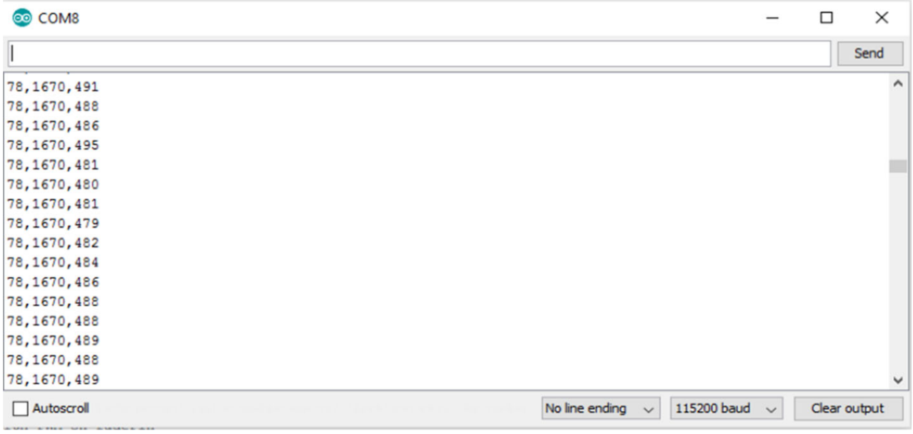
Fig. 14 A testbed of Wearable smart nodes in the KFUPM lab

Figure 18 shows the captured data packets in an invalid foreign tag. In this example, the reader using the authentication process, which the controller executed, reported that tag number four is invalid. The controller computes the hash of the new data, encrypts it with the shared key, and compares the result with the signature, so tag four is considered as an invalid node. Its data is discarded because the results and signature do not match.

6 Conclusions

In this paper, we presented a novel technique for IoT healthcare monitoring applications based on the RFID clustering scheme. The proposed scheme integrates RFID with wireless sensor systems to gather information efficiently, aiming at monitoring the health of people in large events such as festivals, malls, airports, train stations. The developed system is composed of clusters of wearable smart nodes. The smart node is composed of RFID tag, reduced function of an RFID reader, and body sensors. The clusters are reconstructed periodically based on specific criteria, such as the battery level. These clusters collect data from their members and when they come across RFID readers, they deliver the collected data to these readers. On the other hand, using the traditional approaches, only the nodes in the range of the RFID readers can send their tag data to the RFID readers. Hence, this will cause several performance problems such as long delay, dropped packets, missing data, and channel access congestion. The proposed clustering approach overcome all these problems. It demonstrated outstanding performance in reducing the packet transmission delay, inter-node interference, and better energy utilization. The experimental results have supported the above performance.

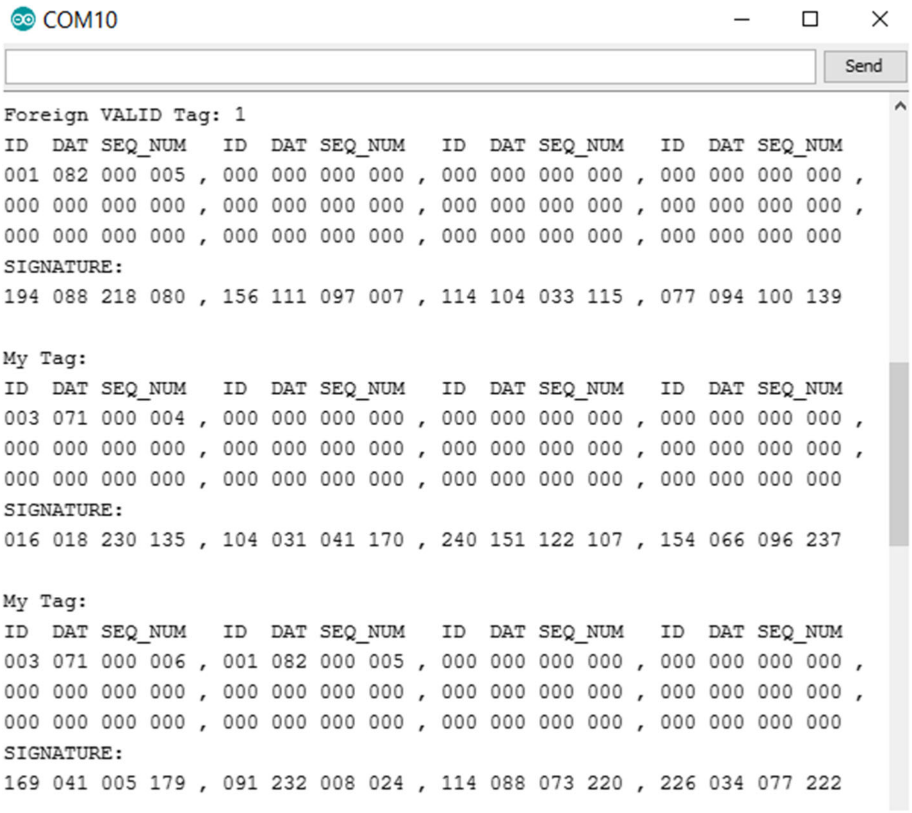
The proposed approach can lend itself easily to monitor and collect the health information of the society population continuously, especially in the current pandemic. As future research directions, we are planning to integrate the smart nodes with other sensors to ensure full health care application and test the new application in large-scale scenarios. There is also a need to improve the clustering algorithm to guarantee a high level of service quality of the deployed health applications.



```
78,1670,491
78,1670,488
78,1670,486
78,1670,495
78,1670,481
78,1670,480
78,1670,481
78,1670,479
78,1670,482
78,1670,484
78,1670,486
78,1670,488
78,1670,488
78,1670,489
78,1670,488
78,1670,489
```

Fig. 15 A sample of the collected data of the pulse sensor on the serial monitor

Fig. 16 A valid foreign tag#1 is read and then updated on the serial monitor

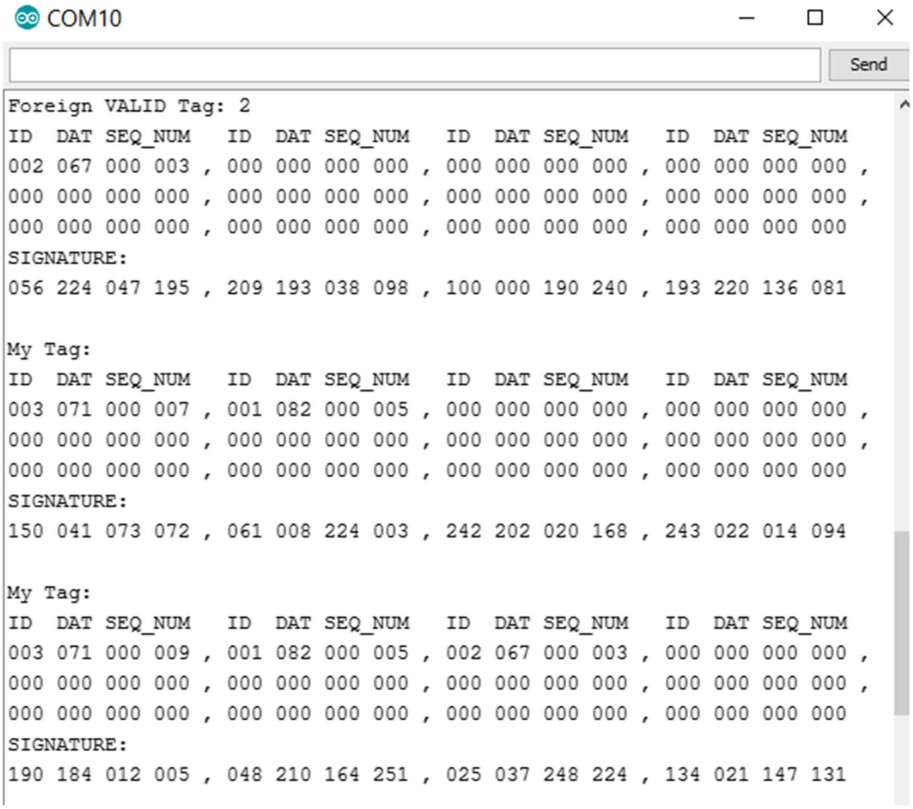


```
Foreign VALID Tag: 1
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
001 082 000 005 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
194 088 218 080 , 156 111 097 007 , 114 104 033 115 , 077 094 100 139

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 004 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
016 018 230 135 , 104 031 041 170 , 240 151 122 107 , 154 066 096 237

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 006 , 001 082 000 005 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
169 041 005 179 , 091 232 008 024 , 114 088 073 220 , 226 034 077 222
```

Fig. 17 A valid foreign tag#2 is read and then updated on the serial monitor

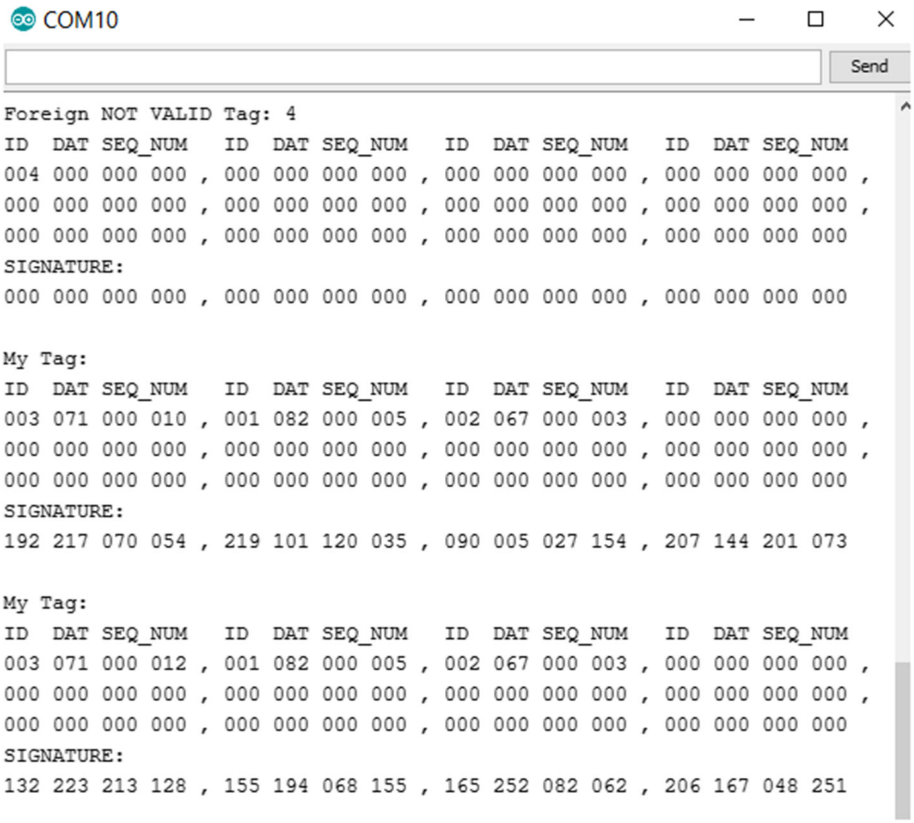


```
Foreign VALID Tag: 2
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
002 067 000 003 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
056 224 047 195 , 209 193 038 098 , 100 000 190 240 , 193 220 136 081

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 007 , 001 082 000 005 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
150 041 073 072 , 061 008 224 003 , 242 202 020 168 , 243 022 014 094

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 009 , 001 082 000 005 , 002 067 000 003 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
190 184 012 005 , 048 210 164 251 , 025 037 248 224 , 134 021 147 131
```

Fig. 18 Invalid foreign tag# 4 with signature is not updated



```
Foreign NOT VALID Tag: 4
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
004 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 010 , 001 082 000 005 , 002 067 000 003 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
192 217 070 054 , 219 101 120 035 , 090 005 027 154 , 207 144 201 073

My Tag:
ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM   ID  DAT SEQ_NUM
003 071 000 012 , 001 082 000 005 , 002 067 000 003 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000 ,
000 000 000 000 , 000 000 000 000 , 000 000 000 000 , 000 000 000 000
SIGNATURE:
132 223 213 128 , 155 194 068 155 , 165 252 082 062 , 206 167 048 251
```

Funding The authors Abdulrahman Abu Elkhail and Uthman Baroudi would like to acknowledge the support provided by the Deanship of Scientific Research (DSR) at King Fahd University of Petroleum and Minerals, under the Grant RG1424-1.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval The study only includes humans in roaming a large hall to test the connectivity of the established networks.

References

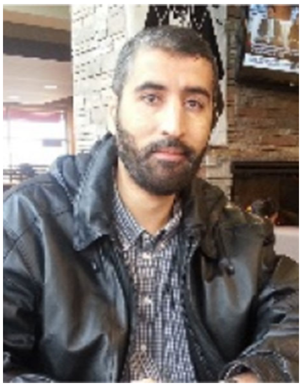
1. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 9th international conference on computational intelligence and security* (CIS), IEEE.
2. Finkenzeller, K. (2010). *Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near field communication* (3rd ed.). New York: Wiley.
3. Shen, H., Li, Z., Yu, L., & Qiu, C. (2014). Efficient data collection for large-scale mobile monitoring applications. *IEEE Transactions on Parallel and Distributed Systems, 25*(6), 1424–1436.
4. Vaerenbergh, S. M., & Legros, C. P. (2010). Influence of thermal boundary conditions on the double-diffusive process in a binary mixture. *International Journal of Thermal & Environmental Engineering, 1,* 109–129.
5. Haik, Y. (2003). *Engineering design process*. Pacific Grove: Brooks/Cole.
6. Toukourou, N. M., Gakwaya, B., & Yazdani, J. J. (2001). An object-oriented finite element implementation of large deformation frictional contact problems and applications. In *Proceedings of the 1st MIT conference on CFSM*, Cambridge, MA.
7. Perky, G. K. (2010). X-analysis integration (XAI) technology. Virginia technical report EL002-2000A.
8. Hofmeyr, G. J., & Qureshi, Z. (2016). Preventing deaths due to hemorrhage. *Best Practice & Research Clinical Obstetrics & Gynaecology, 36,* 68–82.
9. Liu, H., Bolic, M., Nayak, A., & Stojmenovic, I. (2008). Taxonomy and challenges of the integration of RFID and wireless sensor networks. *IEEE Networks, 22*(6), 26–35.
10. Daniel, J. Y., Holleman, J. H., Prasad, R., Smith, J. R., & Bp, Otis. (2009). NeuralWISP: A wirelessly powered neural interface with 1-m range. *IEEE Transactions on Biomedical Circuits and Systems, 3*(6), 379–387.
11. Sample, A. P., Yeager, D. J., &Smith, J. R. (2009). A capacitive touch interface for passive RFID tags. In *Proceedings of IEEE international conference on RFID 2009*, pp. 103–109.
12. Fuhrer, P. & Guinard, D. (2006). Building a smart hospital using RFID technologies. In *Proceedings of the 1st European conference on eHealth (ECEH'06)*, Vol. P-91, pp. 131–142.
13. D'Souza, M., Wark, T., & Ros, M. (2008). Wireless localization network for patient tracking. In *Proceedings of international conference on intelligent sensors, sensor networks and information processing*, pp. 79–84.

14. Chandra-Sekaran, A. K., Dheenathayalan, P., Weisser, P., Kunze, C., & Stork, W. (2009). Empirical analysis and ranging using environment and mobility adaptive RSSI filter for patient localization during disaster management. In *Proceedings of international conference on network and service management (ICNS'09)*, pp. 276–281.
15. Xiaoguang, Z., & Wei, L. (2008). The research of network architecture in warehouse management system based on RFID and WSN integration. In *Proceedings of IEEE international conference on automation and logistics*, pp. 2556–2560.
16. Doukas, C., & Maglogiannis, I. (2012). Bringing IoT and cloud computing towards pervasive healthcare. In *2012 Sixth international conference on innovative mobile and internet services in ubiquitous computing*, Palermo, pp. 922–926.
17. Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., & Marrocco, G. (2014). RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of Things Journal, 1*(2), 144–152.
18. Yang, G., et al. (2014). A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Transactions on Industrial Informatics, 10*(4), 2180–2191.
19. Catarinucci, L., et al. (2015). An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal, 2*(6), 515–526.
20. Gope, P., & Hwang, T. (2016). BSN-care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal, 16*(5), 1368–1376.
21. Essa, Y. M., Hemdan, E. E. D., El-Mahalawy, A., Attiya, G., & El-Sayed, A. (2019). IFHDS: Intelligent framework for securing healthcare bigdata. *Journal of Medical Systems, 43*(5), 124.
22. Saed, S. D., & Kathirvelkumaran, L. Effective data collection in multi-application sharing wireless sensor networks.
23. Sivabalasubramanian, A., & Me, V. J. A hybrid approach of rfid andwsn system for efficient data collection.
24. Jin, Z., Kim, D. Y., Cho, J., & Lee, B. (2015). An analysis on optimal clusterratio in cluster-based wireless sensor networks. *IEEE Sensors Journal, 15*(11), 6413–6423.
25. Kawadkar, M., & Dorle, S. S. (2015). Wireless regulation and monitoringsystem for emergency ad-hoc networks using nodes. In *2015 Global conference on communication technologies (GCCT)*, IEEE, pp. 874–879.
26. Cheng, C. T., Ganganath, N., & Fok, K. Y. (2016). Concurrent data collectiontrees for iot applications. *IEEE Transactions on Industrial Informatics, 13*(2), 793–799.
27. Fu, Y., Jiang, D., Zhang, D., Song, H., Wang, H., & Zhou, X. (2016). Acooperation-based routing algorithm in mobile opportunistic networks. In *2016 International conference on identification, information and knowledge in the internet of things (IIKI)*, IEEE, pp. 160–166.
28. Agarwal, A., & Dev, A. A data prediction model based on extended cosine distance for maximizing network lifetime of wsn.
29. Wang, S., Yu, J., Atiquzzaman, M., Chen, H., & Ni, L. (2018). Crpd: anovel clustering routing protocol for dynamic wireless sensor networks. *Personal and Ubiquitous Computing, 22*(3), 545–559.
30. Secure data transmission in hybrid radio frequency identification with wireless sensor networks. https://www.ijert.org/research/secure-data-transmission-in-hybrid-radio-frequency-identification-with-wireless-sensor-networks-IJERTCONV3IS07033.pdf.
31. Elkhail, A. A., & Baroudi, U. (2018). Real-time healthcare monitoring system using smartphones. In *2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)*, IEEE, pp. 1–6.
32. Li, X., Guo, S., & Li, P. (2019). Energy-efficient data collection scheme based on mobile edge computing in wsns. In *2019 15th International conference on mobile ad-hoc and sensor networks (MSN)*, IEEE, pp. 95–100.
33. Alfares, H. K., Elkhail, A. A., & Baroudi, U. (2020). Iterative clustering for energy-efficient large-scale tracking systems. *Wireless PersonalCommunications, 110*(2), 713–733.
34. Wang, J., Gao, Y., Liu, W., Wu, W., & Lim, S.-J. (2019). An asynchronous clustering and mobile data gathering schema based on timer mechanis min wireless sensor networks. *Computers Materials & Continua, 58,* 711–725.
35. Baroudi, U., Elkhail, A. A., & Alfares, H. (2020). Optimum bi-level hierarchi-cal clustering for wireless mobile tracking systems. *Wireless Networks, 26*(2), 1227–1242.
36. Kumar, D. (2009). Modeling and representation to support design-analysis integration. Master Thesis, Department of Civil Engineering, Indian Institute of Technology.
37. Zhan, B., Monekosso, D. N., Remagnino, P., Velastin, S. A., & Xu, L. Q. (2008). Crowd analysis: A survey. *Machine Vision and Applications, 19*(5–6), 345–357.
38. Rodriguez, M., Sivic, J., Laptev, I., & Audibert, J.-Y. (2011). 'Data-driven crowd analysis in videos. In *Proceedings of IEEE international conference on computer vision (ICCV)*, pp. 1235–1242.
39. GAMS Software GmbH. (2017). GAMS Specifications, GAMS Website. https://www.gams.com/.
40. The SparkFun specification. https://www.sparkfun.com/.

Abdulrahman Abuelkhail is a Ph.D. student in the Electrical and Computer Engineering Department at the University of Michigan, Dearborn, United State. He has a B.S. in Computer Engineering from Yarmouk University, Irbid, Jordan, and an M.S. in Computer Engineering from King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia. His areas of interest include wireless sensor and Ad Hoc networks, IoT, automotive cybersecurity, system and security. He has over 10 publications in referred reputable Journals and conference proceedings and 2 US patents.

Uthman Baroudi is currently an associate professor in the Department of Computer Engineering at KFUPM, Dhahran, Saudi Arabia. He received his B.Sc. and M.S. degrees from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia in 1988 and 1990, respectively, and in 2000, he received his Ph.D. from Concordia University, Montreal, Canada, all in Electrical Engineering. In 2000, he joined Nortel Networks, Ottawa, Canada, to work in R&D for next generation wireless networks. His research interests lies in the areas of cloud robotics networks, network design for IoT, wireless adhoc, and sensor and actuator networks. Dr. Baroudi has over 120 publications in referred reputable Journals and Conference Proceedings, and 35 US patents.

Muhammad Raad joined King Fahd University Petroleum Minerals, computer Eng Dept 1986, where he worked as a lecturer and researcher in the field of smart cards & RFID. He Obtained his Phd from University Bradford UK 2005 in embedded systems & signal processing. He gave consultation to a number of companies in the region, in addition to a number of workshops and tutorials on smart cards and RFID. In 2010, he established the first Smart Card & RFID university lab in the region to support student projects as well as conducting short courses for the industry in RFID/NFC. In the last two years he was involved in two funded projects: implementing RFID in MIT joined project for renewable energy & hajj project for tracking pilgrimage. Recently coordinated & taught a short course on introduction to IOT & industry 4.0 to Saudi Aramco.



Tarek Sheltami received his Ph.D. in Electrical and Computer Engineering from the Electrical and Computer Engineering Department at Queen’s University, Kingston, Ontario, Canada on April 2003. Dr. Sheltami is currently a Professor at the Computer Engineering Department at King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Kingdom of Saudi Arabia. He joined the department on August 26, 2004. He has been an adjunct professor with Jodrey School of Computer Science, Acadia University, Canada since 2010. He is currently collaborating with the Transportation Research Institute (IMOB) at Hasselt University, Belgium. He authored/co-authored more than 200 research articles. Before joining the KFUPM, Dr. Sheltami was a research associate professor at the School of Information Technology and Engineering (SITE), University of Ottawa, Ontario, Canada. He worked at GamaEng Inc. as a consultant on Wireless Networks (2002-2004). Also, he worked in several joined projects with Nortel Network Corporation. Dr. Sheltami has been a member of the technical program and organizing committees of several international IEEE conferences. His research interests include Ad hoc Networks, WSAN, IoT, Digitization, Computer Network Security and Performance Evaluation.