A Novel Sensor Data Transferring Method Using Human Data Muling in Delay Insensitive Network

Anas Basalamah,
ambasalamah@uqu.edu.sa
Umm Al-Qura University

Abstract
In this paper, a novel data transferring method is introduced that can transmit sensor data without using data bandwidth or an extra-processing cycle in a delay insensitive network. The proposed method uses human devices as Mules, does not disturb the device owner for permission, and saves energy while transferring sensor data to the collection hub in a wireless sensor network. This paper uses IP addressing technique as the data transferring mechanism by embedding the sensor data with the IP address of a Mule. The collection hub uses the ARP sequence method to extract the embedded data from the IP address. The proposed method follows WiFi standard in its every step and ends when data collection is over. Every step of the proposed method is discussed in detail with the help of figures in the paper.

Key words:
Mule, sensor data, delay insensitive network, ARP sequence, WiFi standard, wireless sensor network.

1. Introduction

The wireless sensor networks (WSNs) consists of sensor nodes deployed for monitoring events and collecting data in different hostile areas [1]. Smart devices are also considered as a sensor node of WSNs as different sensors are embedded in these devices. Several methods already exist for collecting sensor data from mobile devices, computers, smart wearable devices, and other electronic devices. Wireless infrastructure padded with extra security is used to collect data from these devices. This paper proposes a method for collecting data from the smart devices to the collection hub in an inexpensive and delay tolerant mode considering these devices as Mules.

Generally, data is collected in real-time through different sensors attached with the device for non-military type applications, for instance- humidity, maximum rainfall, or high/low temperature of the day. These collected data are used only for statistical purposes and collected securely through enterprise network infrastructure using virtual private network or virtual private channels. It becomes challenging to collect these data from many locations where network infrastructure is unavailable. Establishing a node only for collecting these sensor data becomes expensive for the enterprise. Therefore, enterprises use wireless cell-network to collect non-real time data, which requires SIM cards. If this cell-network coverage fails to reach any hostile location, this above method also fails to collect data.

This paper proposes a novel method and process for non-real-time data transmission to the collection hub over the wireless network considering the human data muling technique. Human data muling technique is the technique of collecting data from sensors to the collection hubs by utilizing human devices as mules. This method of carrying data through human devices is a novel idea.

The presented method is non-invasive for both humans and their carrying devices. The data is collected through these human devices using existing wireless protocols when these devices pass by the nearest access points. This data collection method is new and inexpensive as it does not use sensors and infrastructure owned by enterprises. Therefore, investment on devices and infrastructure does not exist.

The proposed method is called non-invasive because it uses mapping function between IP address and sensor data to transmit data from the mule to the collection hub. It demonstrates the use of Access Point cloaking that behaves familiar to the smart device. The proposed method works with all types of smart devices such as- smart phone, tablets, smart watch, and etc. which uses standard WiFi protocol. Moreover, this proposed method saves extra bandwidth and processing cycles that are required for normal data transfer.

The proposed method is fault tolerant and scalable. The idea emphasizes on collecting data from a mule of a particular location and send it to the collection hub through the access point nearest to that location. Other features and advantages of the proposed method is discussed in the following part of the paper. The remaining part of the paper is structured as the following- background of this study and its motivation is discussed in section , application and contribution of the proposed method are discussed in the section 3, detailed process of the proposed method is discussed in the section 4, and eventually this paper concludes with the section 5.

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.3

2. Background

Collection of sensor data to serve different purposes is not a new idea. It has been in application since the last century. In [2], the authors studies an underwater sensor data collection system that consists two modalities, namely- ultrasonic and optical. The authors state that the ultrasonic communication system is highly used for data underwater data transmission, but it has the low propagation speed. On the other hand, optical communication system is fast and capable of transmitting higher bandwidth. A dual combination of these two enables many applications in underwater sensor networks since it provides low-speed broadcast and high-speed data transfer.

The authors in [3] studies an approach consisting an abstraction layer for collecting, processing, or combining health sensor data. The approach initiates a communication session between the second party device and the multi-modality device associated for transmitting the sensor data, configuring multi-modality devices, or providing health information based on the collected data.

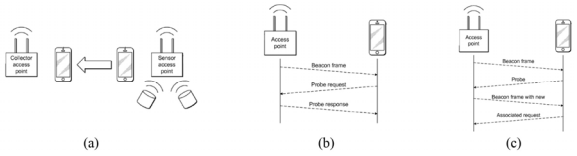

Figure 1: (a) Illustration of the sensor access point that collects data using the sensor nodes (smart device), (b) Communication between an access point and a sensor node to identify each other, and (c) Diagram of message sequence for availability discovery of access points.

In [4], the authors present a media access control (MAC) layer address translation system that is associated with the fiber to the home system which provides an interface of packet data network in a passive optical network (PON). The MAC layer translation system consists of a host system, a MAC address table, and a home network unit (HNU). The host system is coupled with the network's HNU and associated with its MAC layer address to the HNU. A MAC address table is maintained to replace the host's MAC address with the secondary MAC address of it while performing outgoing data transmission from the host.

Intelligence reflecting surface(IRS) carried by unmanned aerial vehicle (UAV) for secure data collection in wireless sensor network is investigated in [5]. The authors design a IRS reflection coefficients to obtain maximum secrecy while sensor data collection, and develop a non-iterative sub-optimal solution that maximizes the secrecy rate. The authors find that the randomness and UAV flight time greatly affect secrecy performance in the distributive sensor network when sensor nodes are placed and interchanged among different areas.

The authors in [6] study a mobile sink based wireless sensor data collection method that is energy and coverage sensitive. The authors intend to solve the energy hole problem in the wireless sensor network while collecting sensor data. The authors intend to incorporate a coverage parameter for preserving the network coverage despite containing die nodes. The proposed algorithm in [6] ensures the minimum data delivery delay by following minimum hop routing while disseminating each cluster data.

Another work in [7] presents single-hop and multi-hop sensor data collection network that helps to collect labelled data for anomaly detection. The authors state that this collected data set can be useful for various machine learning and deep learning applications for anomaly detection to the research community.

The authors in [8] study a survey on the recent advancement in sensor data collection techniques for both wired and wireless sensor networks for various applications. The authors claim that this work first time highlights and discusses different special features and issues of sensor data collection. In addition, their paper investigates various approaches for control message dissemination, which is the key component for network control and management in WSNs, and affects the performance of sensor data collection.

Nowadays, sensor data collection method uses back haul node and a fixed wireless access network for collecting visual sensing data such as- camera collected data. Some sensor nodes buffer and wait for a mobile sensor node to come by the access points from where data is transferred to the collection hub. The city service data of a city municipal services department such as- parking information is also collected 24×7 through a wireless node to know the parking and time expiry status. The collected data can be hard-real-time or soft-real-time in nature based on the acquisition process. The collected data can lead to inconsistency or catastrophe in the final collection and decision making using the hard-real-time data acquisition method if there is a loss of a single datum. Therefore, this paper requires a very secure and delay intolerant channel for carrying data to the collection hub.

Generally, soft-real-time sensor data are collected for various non-military type applications using sensors and carried securely through private secure channels to the collection hub in real time. This collection procedure is expensive as the infrastructure and auxiliary equipment belongs to the network enterprises. This paper brings a new

idea into the table that opens a cost-efficient way of sensor data collection through human devices.

Overall, the above study shows that there are different methods exist for collecting sensor data in wireless networks. This paper first-time proposes human data muling approach for sensor data collection. The remaining part of the paper demonstrates step-by-step procedure of human data muling-based sensor data collection in wireless networks.

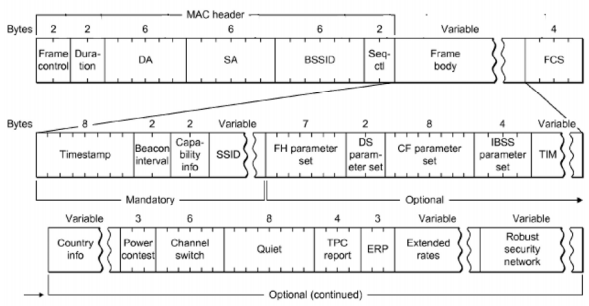

Figure 2: Frame format for the Beacon frames, which shows AP presence can be identified with the help of SSID broadcasting.

3. Contributions and applications of the proposed method

The proposed scheme provides a new dimension to sensor data collection through human data muling, which is a novel idea of collecting sensor data and transferring it to the collection hub. The followings are some particular contributions of the proposed method:

1) The proposed novel method of data muling comprises of several key steps-
   a) Collecting sensor data from the smart device through sensor access points (SAPs) and embedding the data with IP address.
   b) Retrieving the data from the IP address using address resolution protocol (ARP) sequence in a collection hub.
   c) Forcing the smart device (Mule) to initiate the ARP request to associate the device with the access point uniquely.
   d) Finally, transferring the data from the device to the collection hub.
2) The proposed method neither involves the owner of the smart device nor creates interference in its use while maintaining the IEEE WiFi 802.11 protocol to the collection hub.
3) The proposed method does not require extra-processing cycle and bandwidth while transmitting data to the collection hub, which makes this method cost and energy efficient comparing to the other existing data collection methods.
4) The access point terminates the association with the mule when the sensor data is received by the collection hub.

The above contributions make this data collection process unique than other existing works and justify the novelty of this method. The contributions made by this paper is applicable to all wireless networks which operate maintaining the IEEE 802.11a/b/g/n/ac standards. Moreover, this process also works with general standard like ARP and DHCP internet protocol networks. This method completes the data collection procedure without generating any permission token to the mule which takes time to get authorized, hence this method is time efficient. The collection process works silently and seamlessly in the background without bothering the device owner. This unique method is immediately applicable since the majority of the smart devices have WiFi features in-build. This process works on the devices that show the previous IP/MAC connectivity. All apple devices are having this feature nowadays.

4. Detailed process of human data muling

This paper presents a process of transferring sensor data from the smart devices, considering them as mules, to the collection hub. A detailed description with apparatus to be used is investigated in this work. Transferring sensor data using wired infrastructure is impossible in remote places where wires infrastructure is unavailable or not capable enough. For example- remote border areas, hill stations or mountainous places, remote islands, and etc. do not have wired network infrastructure that can facilitate the data collection process. In such cases, wireless networks that are padded with extra security insurance are used.

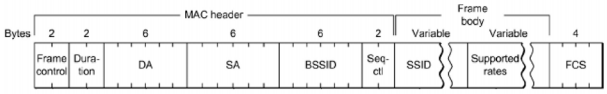

Figure 3: Frame format for the Probe Request sent by the Smart device.

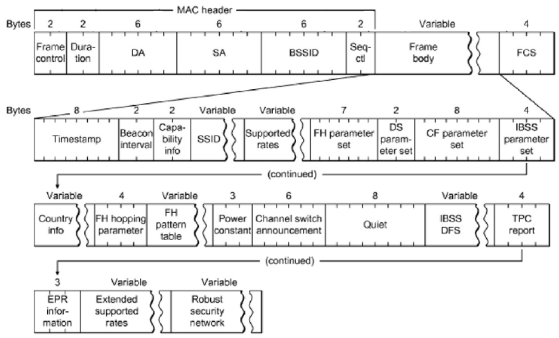

Figure 4: Frame format for the Probe Request that shows the responding process of the smart device to the AP where AP advertises all connection parameters.

As mentioned in section 2, the collected data through sensors can be of two types, namely- hard-real-time and soft-real-time data. In soft-real-time data collection, loss of a small portion of the collected data is tolerated because decision can still be made with the data reached so far in the collection hub. On the other hand, hard-real-time data collection method does not tolerate any missing sequence in the data. Therefore, this paper adopts the soft-real-time data collection method that can handle the data missing problem, and is delay tolerant and inexpensive.

In general, soft-real-time data are collected through sensors for serving non-military types applications. Enterprise security is such an application where data are collected and carried through the enterprise network infrastructure. These enterprise networks are owned by the enterprises, and data collection using these networks is costly. Therefore, this paper considers human devices as mules and collects data through wireless infrastructure, which does not necessarily need dedicated data transmission channels. This method is inexpensive and independent of dedicated infrastructural hazards. Since wired data transmission is considered as safe, the proposed method ensures highly secured data transfer using standard protocols.

The proposed data collection method is intended to be applied in the statistical purposes such as- estimating maximum rainfall of a day, measuring the humidity of weather, measuring maximum or minimum temperatures, and etc. Nowadays, smart devices are in use from the big cities to the remote villages. The above stated data can be collected through sensors of smart devices and carried out to the nearest collection hub using wireless network, when the smart device reaches the nearest access points. Hence keeping weather, rainfall, or temperature records for different geographical locations including remote areas will be easier to maintain.

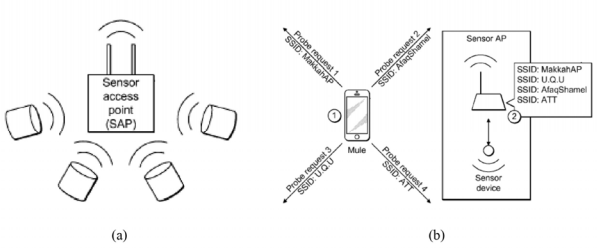

Figure 5: (a) Demonstration of a typical Sensor Access Point (SAP) and (b) depiction of the behavior of SAP and smart devices.

This proposed method provides a novel idea of using human devices and carrying the collected data without using enterprise networks. Enterprise networks use 4G or LTE wireless connectivity for data transfer but in rural or mountainous areas these networks often fail to provide coverage. Data collection in those areas is more effective using the proposed method. The collected data is only sent to the collection hub when the mule gets near to an access point. Many mules are available without any cost. Therefore, this method is cost effective. The idea of using human devices as mules is a novel idea.

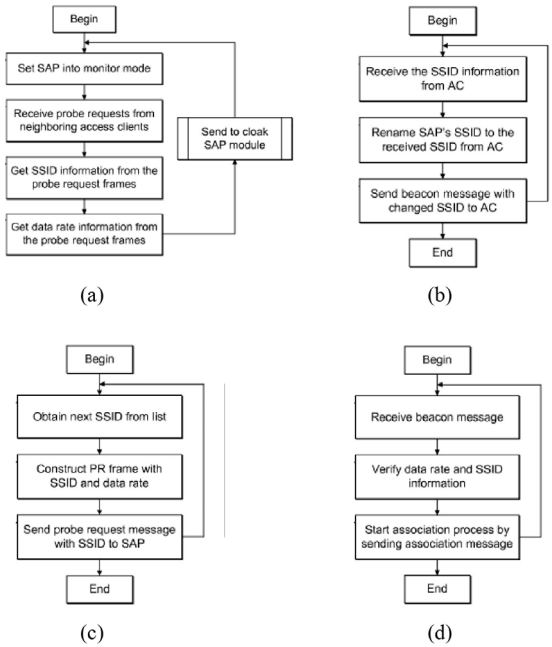

Figure 6: (a) Probe Request registration process in SAP, (b) Process of SAP cloaking that acts as an AP with SSID, (c) Probe request message sending process to the SAP with the list of previously associated SSIDs, and (d) Smart device association process with the SAP.

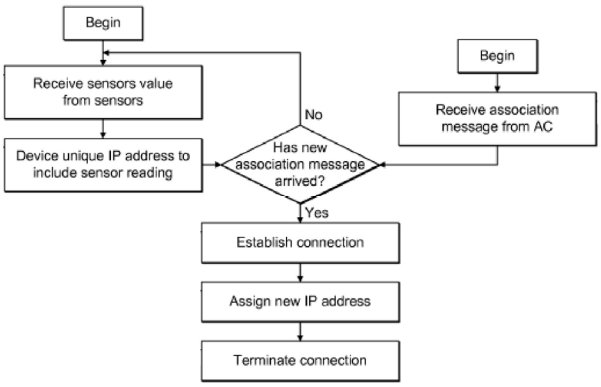

Figure 7: Steps of the mapping function of SAP.

The disclosed method is non-invasive for both the humans and their carrying devices. This method uses standard wireless protocol for both data collection and transfer process. Therefore, it does not hampers daily activities of humans and their phones. As these devices work as sensor nodes, it help to reduce the cost of sensor node installation for data collection. The proposed method presents a mapping function between the sensor access point and the device for non-invasive data collection.

In addition, this paper shows an access point cloaking method to confuse the devices so that the access point seems familiar to the device, and the devices are forced to assume that the AP is used by it previously. The trick works in every types of smart devices that use standard WiFi protocol such as- android, windows, or apple. The collected data is embedded with the IP address and extracted at the CAP when reached there. This method does not require extra processing cycles or bandwidth for processing messages that might seem unusual to the device owner.

The proposed method is fault tolerant and highly scalable. Each of the smart devices collects and stores a small amount of data into it. The idea is to let that data reach to the collection hub using several devices and following some action specific steps. The number of smart devices used in this process is not limited as the larger number of devices increases the chance of reaching data to the collection hub. However, the data can be transferred to the collection hub using both the wireless and wired networks. Sometimes the readers may get confused to understand the application of the presented method and to distinguish its application to the wireless network and wireless sensor network. Consequently, these two networks are discussed in the following to avoid such confusion.

1) **Wireless Network:** the presented method is applicable to the wireless network, where autonomous sensor nodes are connected via wireless links. Each of the sensor nodes are capable of sending and receiving data to communicate to the neighbouring nodes.

   In this proposed method, smart devices act as autonomous sensor nodes and communicate between each other and to the access points using IEEE 802.11 based WiFi standard protocol.

2) **Wireless Sensor Network:** the wireless sensor network consists of a set of sensors placed in different location and connected together using a wireless network. A wireless sensor network is indeed a wireless network with having at least one autonomous sensor. Otherwise, WSNs work similarly as wireless networks.

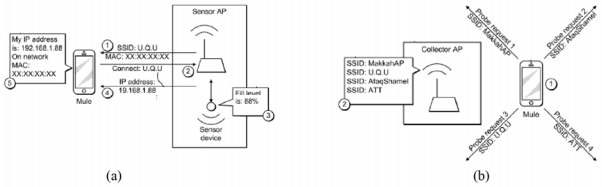

Figure 8: (a) Step-by-step demonstration of the association phase procedure with an example and (b) Steps to perform when the mule is near to the collection hub.

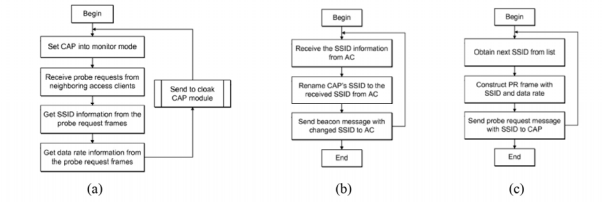

Figure 9: Illustration of- (a) the data collection method inside a CAP, (b) the cloak module inside CAP, and (c) steps of sending PR from the smart device to the CAP.

In Figure 1(a), the data collection by access points using various sensor nodes is depicted. Usually a smart device changes its location every now and then according to its owner's movement. When the device reaches close to an access point, the collected sensor data is transferred to the collection hub. All the participating devices in this whole process are operated using the standard WiFi protocol. The sensor node is connected to the access point and the smart device using the WiFi standard in Figure 1 (a). Similarly, the smart device operates and communicates using the same WiFi standard to the access point. Here, the collection access point is connected to the collection hub. This connection is used to send the sensor data (collected through mule) from the access point to the collection hub.

The end-to-end network used in this process has two sides, namely- collection side and the reporting side. On the

former one, there are multiple sensor nodes~108 that collects the data and maintain a connection with the sensor access point~110. The collected data from sensor~108 is sent to access point~110 in the collection side. On the latter one, the mule~104 and the collector access point~102 are present. In this part of the network, mule collects the data and collector access point sends the data to the collection hub.

Figure 1 (b) depicts communication between an access point and a sensor node. This communication follows standard WiFi protocol and helps the access point and the sensor node to identify each other. The Probe Request (PR) is sent by the sensor node(Mule) to the access points to request an association between them and the Beacon Frame (BF) is sent to the by the access point to notify its availability to the sensor node(Mule).

Diagram of message sequence for availability discovery of access points is depicted in Figure 1(c). The BF is periodically sent from access point for showing it presence. The smart device or sensor node that receives the BF, sends a PR with a SSID to the access point. Upon receiving the PR, the access point transmits another beacon frame with a new SSID to the sensor node. The sensor node/smart device/mule receives the new frame and sends an association request to the access point.

Frame format for the Beacon frames is depicted in Figure 2, which shows that the AP presence can be identified with the help of SSID broadcasting. Each message frame has a frame format maintaining the standard. Each of the frame contains a media access (MAC) layer and other optional or mandatory parameters.

In Figure 3, frame format for the Probe Request sent by the Smart device is shown. Information on the data rate and the SSID are contained by the advertisement from the smart devices to the access points. Data is transformed with respect to the supporting rate when the frame consists of MAC layer header and frame body.

Frame format for the Probe Request that shows the responding process of the smart device to the AP where AP advertises all connection parameters is illustrated in Figure 4. Figure 4 shows that the SSID information is provided by the access point and the supporting rate is depended on the frame body and the MAC layer header.

Figure 5 demonstrates an access point that caters to sensor access points (SAPs). Generally, SAPs collect data from the sensors and become self-prepared to send that data to the collection hub through passing by smart devices. SAPs allow multiple sensors to be connected with it. The depiction of the behavior of SAP and smart devices is shown in Figure 10 (b). The PR sent by a mule communicates with SSIDs of previously associated networks. SAPs learn about those SSIDs to consider smart devices as mules. These mules carry the data from the sensor node to the sensor access point.

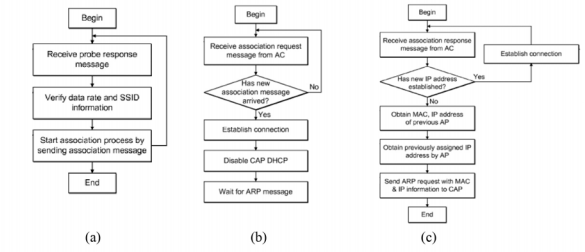

Figure 10: (a) Steps of a smart device after receiving the PR from the CAP, (b) steps for establishing the connection between a smart device and CAP, and (c) ARP initiation process between a smart device AC and CAP.

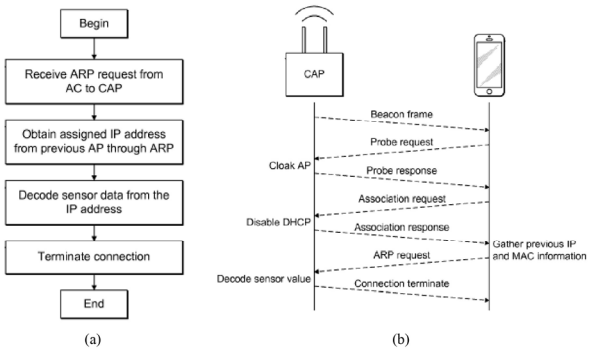

Figure 11: (a) Steps of data decoding procedure at CAP and (b) a complete messaging sequence between the CAP and the smart device AC.

Probe Request registration process in SAP, process of SAP cloaking that acts as an AP with SSID, probe request message sending process to the SAP with the list of previously associated SSIDs, and Smart device association process with the SAP is depicted step-by-step in Figure 6, Figure 6 (b), Figure 6 (c), and Figure 6 (d), respectively. In Figure 6(a), SAPs act as the monitoring nodes which receive the PR and collect the SSIDs of previous network association of the mules with the prospective data transfer rate. The idea of using smart devices as mules is shaped and moved forward using the key steps shown in the Figure 6 (b). The key steps are taken by the SAP since it receives the PR from the mule and sends SAP cloaking entry. The AP is cloaked by the SAP as if the AP is with another new SSID, which is shown in Figure 6 (c). SAP gets enabled to send BF messages with new SSID and forces the smart device to assume that the SAP is an AP and it has communicated with the AP previously. Afterward,

the smart device belevies that it has got the message from the SSID and can get associated for data transfer.

However, Smart device association process with the SAP is depicted in Figure 6(d). At first, the smart device sends PR to all the SSIDs available in its list with the data rate to be offered and SSID information. Then the AP with a particular SSID replies back with a Beacon Frame. The smart device verifies all the information including SSID and data rate, and it initiates the association process.

SAP mapping function is illustrated in Figure 7. It is shown that the SAPs receive association request from the smart device and connect with the device by assigning a new IP address. The new IP address is embedded with the sensor value before starting the data transmission from the device to the collection hub through access points.

In Figure 8(a), step-by-step demonstration of the association phase procedure with an example is depicted. In step~1, the SAP sends a Beacon message. Then the mule replies back with a PR and association message in step~2. The sensor node collects the data and the SAP establishes connection to the mule using a new IP address in step~3 and step~4, respectively. Step~5 shows that the connection between the SAP and the mule is established using the IP address. This entire process is very important and considered as key part of the human data muling. These steps help to communicate mule to the access point without creating any disturbance to the device owner.

Figure 8(b) depicts the set of steps to perform when the mule is near to the collection hub. The collector access point has a wireless circle of influence. When a mule comes into the influence area, the collector access point establishes connection to the mule and collects the gathered information from the mule. The entire communication obeys the WiFi standard protocol.

The data collection method inside a CAP, the cloak module inside CAP, and steps of sending PR from the smart device to the CAP are illustrated in Figure 9(a), Figure 9(b), and Figure 9(c), respectively. The collector AP (CAP) receives PR from the mule and immediately deciphers the SSID and data rate. Then the collected information is sent to the cloak module for processing. The cloak CAP module change the SSID as per the standard so that the previous SSID can be used by the mule for associating with the CAP. The mule actually maintains a list of previously associated SSIDs with data rate. The PR frame is constructed using these information and sent to the CAP for association.

Figure 10(a), Figure 10 (b), and Figure 10 (c) depicts steps of a smart device after receiving the PR from the CAP, steps for establishing the connection between asmart device and CAP, and ARP initiation process between a smart device AC and CAP, respectively. When the mule receives PR from the CAP as reply, it verifies the SSID and data rate. Afterward, the association between the mule and the CAP is initiated. CAP disables the DHCP (Dynamic Host Configuration Protocol) and establishes the connection. An IP address is sent to the mule from the CAP upon request by ARP message transfer. If the mule receives a new IP address with the association response from the AC, the connection is directly established. Otherwise, the mule requires to obtain the MAC and IP address of the previous connection with the AP and send a new ARP with the MAC and IP.
\par In Figure 11(a), the steps of data decoding procedure at CAP is demonstrated. The flowchart shows that an ARP request is sent from the AC to the CAP. The collector AP decodes the message from the IP address and extract the sensor data. Afterward, the connection is terminated. Finally, a complete sequence of message transfer between the CAP and the AC of mule is illustrated in Figure 11 (b).

In sum, a BF is sent from the CAP to the AC of the mule at first. The mule replies back with a PR. In response to this PR, the CAP again replies back to the mule with a new SSID with the help of AP cloaking. Then the mule sends a association request to the CAP with SSID and data rate. The CAP disables the DHCP and responds to the association request. The mule gathers previously used IP address and MAC address information for sending the ARP request. Afterward, he connection gets established between the CAP and the AC of the mule. Finally, The CAP terminates the connection after decoding sensor collected from the embedded IP.

5. Conclusion

A novel data transferring method is introduced and discussed in this paper. The presented method of human data muling considers human devices as carriers and does not use enterprise network infrastructure. This method is effective for collecting sensor data in the remote areas where network infrastructure is not available. The proposed method is scalable, secured, and inexpensive. It uses standard WiFi protocol for all data transfer and communication.

References

[1] Senthilkumar, A., S. Lekashri, and D.R.M. Abhay Chaturvedi, DATA TRAFFIC TRUST MODEL FOR CLUSTERED WIRELESS SENSOR NETWORK. INFORMATION TECHNOLOGY IN INDUSTRY, 2021. **9**(1): p. 1225-1229.

[2] Vasilescu, I., et al. Data collection, storage, and retrieval with an underwater sensor network. in Proceedings of the 3rd international conference on Embedded networked sensor systems. 2005.

[3] Moore, A., System and method for providing a multi-modality device with abstraction layer support from a healthcare platform. 2014, Google Patents.

[4] Adcox, T.D. and M.D. Kimbrough, Media access control address translation for a fiber to the home system. 2011, Google Patents.

[5] Nnamani, C.O., M.R. Khandaker, and M. Sellathurai, Joint Beamforming and Location Optimization for Secure Data Collection in Wireless Sensor Networks with UAV-Carried Intelligent Reflecting Surface. arXiv preprint arXiv:2101.06565, 2021.

[6] Roy, S., N. Mazumdar, and R. Pamula, An energy and coverage sensitive approach to hierarchical data collection for mobile sink based wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 2021. **12**(1): p. 1267-1291.

[7] Suthaharan, S., et al. Labelled data collection for anomaly detection in wireless sensor networks. in 2010 sixth international conference on intelligent sensors, sensor networks and information processing. 2010. IEEE.8. Wang, F. and J. Liu, Networked wireless sensor data collection: issues, challenges, and approaches. IEEE Communications Surveys & Tutorials, 2010. **13**(4): p. 673-687.