Engineering and Technology Journal e-ISSN: 2456-3358
Volume 07 Issue 10 November-2022, Page No.-1740-1748
DOI: 10.47191/etj/v7i11.10, I.F. – 6.484

A Novel Algorithm for Reducing Energy Consumption in WSN and RFID Integrated Networks

Mahia Samani[1], Ahmad Khademzadeh[2], Kambiz Badie[3]
[1]Dep of Computer Eng, Qom branch, Islamic Azad University, Qom, Iran.
[2,3]Iran Telecom. Research center, Tehran, Iran.

ABSTRACT: Wireless sensor networks (WSN) and radio frequency identification (RFID) are base technologies employed in decentralised dynamic environments. In the hybrid network that is induced by integrating RFID and WSN, RFID data can be used applying WSN protocols for multi-hop communications. RFID data, however, includes a significant amount of duplicate information, which lengthens response time and consumes more energy, wasting a variety of resources. The hierarchical RFID-sensor topology, network RFID-sensor topology, reader-sensor nodes topology, and mixed topology are the four most commonly used RFID-WSN integration architectures. In this article, a novel plan for a WSN–RFID integrated network was proposed. The entire network is divided into clusters, and Huffman algorithm is used to reduce energy consumption in sending information to the base station. Further, we propose two algorithms to overcome redundancy of the data on the hybrid network. Our simulation findings demonstrate that the studied method decreases redundant data, energy consumption and processing duration in comparison with existing methods.

KEYWORDS: Redundant data, Data filtering, Integration, Radio Frequency Identification, wireless Sensor network, RFID projects, Reducing energy consumption.

1. INTRODUCTION

A sink node (or base station) and a number of compact, lightweight, and inexpensive devices known as sensor nodes are used to construct wireless sensor networks (WSNs) [1, 2]. Data processing and sensing capabilities allow sensor nodes to perceive environmental factors including temperature, pressure, sound, light, and vibration, and collect data according on those factors [3]. Head nodes provide these data to base stations. The sensor networks are implemented in various applications, including monitoring of the environments, especially border controlling, industrial controlling, army, and medical care [4.5]. However, these sensor networks are unable to recognize the objects in their surroundings. In contrast, networks that combine WSN with radio frequency identification (RFID) make it possible to identify objects and sense the surroundings, simultaneously [6]. Numerous establishments, including chain store management and healthcare services, implement similar networks [7,8].

An RFID administration includes a tag, software, and a data reader. Data is stored in the data reader's memory after being read from tags that are connected to objects [9]. A multi-hop from one reader to others is not supported by RFID. However, the combination of RFID and WSN enables the transmission of data via the sensor network protocol from one data reader to another, ultimately leading to the base station. [10, 11]

The following phases of the study are organized as follows. Section 2 demonstrates the method of research. Section3 contains the related works. The demonstration of the suggested algorithm is performed in section 4 The findings of simulations are presented in section 5 and finally, section 6 mentions the conclusion.

2. RESEARCH METHODS

The stages of the research method in this project are as follows:

A. Study and investigation in the field of integration of RFID and WSN
B. Finding out the problems in the integration of RFID and WSN
C. Study and review the research done to solve the above problem and present new hypotheses to solve it.
D. Hypothesis testing
E. Evaluation and conclusion

A. Study and investigation in the field of integration of RFID and WSN

Four popular RFID–WSN integration architectures exist:

- Hierarchical RFID-sensor topology,
- Network RFID-sensor topology,
- RFID reader-sensor nodes topology
- Mixed topology

Hierarchical RFID-Sensor Topology

Adding a sensor to an RFID tag is an important way to integrate the two technologies (Figure 1). Sensor tags with limited communication capacity communicate with the reader. Each tag is assigned to an object, person or animal with a unique ID, while the sensors on the tag sense the information needed [19]. According to the tag's power, this integration can be divided into three groups: passive tag with a sensor, semi-passive tag with a sensor and active tag with a sensor [20, 22].

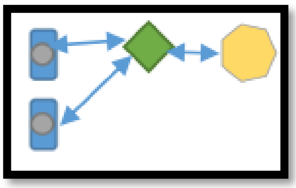


Figure 1. Hierarchical RFID-sensor topology

Network RFID-Sensor Topology

RFID tags can be added to the sensor nodes (Figure 2). Consequently, these merged sensor tags can perform communications with others and different wireless devices. Therefore, these integrated sensor tags have increased their communication capacity and can form a collaborative ad hoc network.

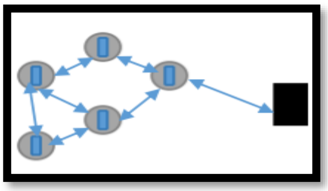


Figure 2. Network RFID-sensor topology

RFID Reader-Sensor Node Topology

An alternative method for the integration of RFID and sensor networks is to add a sensor to the RFID reader (Figure 3). These nodes can be considered RFID data readers with enhanced sensor capacity and the ability to transmit information [14]. They can also act as a router and deliver messages to the destination. These nodes are responsible for collecting information from simple RFID tags within their control range. They also communicate with each other to transmit this information to the sink [22, 23].

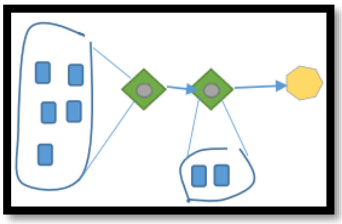


Figure 3. RFID reader-sensor nodes topology

Mixed Topology

In the mixed model, RFID tags and sensor nodes are separate devices, while they physically exist in an integrated network and work separately [21].

B. Finding out the problems in the integration of RFID and WSN

Some of the challenges that WSN and RFID integrated networks are facing are as follows: authentication, real-time performance, energy consumption, data filtering, and data cleaning. Data filtering is a process that deletes, replaces, or modifies incorrect data [12,13]. Redundant data may be categorized into three groups: [15,16]

1) Without any change in the data of the tag, the tag is read by the reader several times. (reading tags in close time intervals).
2) The interrogations of two or several readers be overlapped, as a result, the tags that be placed in this area are read by several readers. (figure 4: The data of two tags-sensor (st1, st2) are read by two data reader (SR2, SR1))

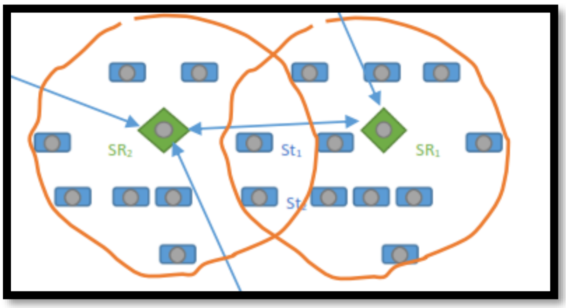


Figure 4. Redundant Readers

3) To rise reliability and reduce the false data rate, a few tags with one EPC may be connected to one object. (Figure 5) [15,16]

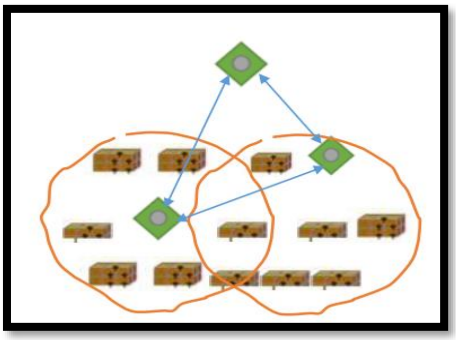


Figure 5. Data level duplication

C. Present New Hypotheses to Solve it.

Many theories have been proposed to solve the data redundancy problem in RFID-based systems. This paper discusses INPFM, CLIF and EIFS and solutions for the data redundancy problem. Two algorithms are presented and explained in detail in Section 4.

D. Hypothesis Testing

In this work, simulation is used for hypothesis testing. These simulations were carried out under C language and an Intel Core i5 processor with 1.4 GHz CPU and 8GB RAM running on Windows ten. A more detailed explanation of hypothesis testing is presented in section 5.

E. Evaluation And Conclusion

The evaluation and conclusion are given in sections 5 and 6, respectively.

3. RELATED WORK

Redundant data filtering is one of the key challenges in RFID applications. Most organisations want access to only one copy of data (i.e., data without redundancy). Many studies have been conducted with the aim of filtering redundant data in servers. The transfer of redundant data from nodes to the server may affect the energy of the nodes, resulting in network overhead and shortening network life. In order to reduce such unnecessary transmissions, redundant data must be filtered within the network. INPFM[1] [17] and CLIF[2] [18] filter redundant data inside the network, but these approaches involve high costs for calculations and are not able to remove all the barriers. Each K-hop reader uses the INPFM algorithm, which uses the tree structures to filter out excessive data. The issue is that INPFM examines redundant data in every hop, increasing calculation costs; nevertheless, if these data are verified after a few stages, some excessive data will reach the network, increasing the network load. The two phases of CLIF's application of clustering topology are (a) redundant data identification and (b) redundant data filtering. The duplicate data in this system is divided into two categories: 1) Excessive information within a cluster, and 2) Excessive information among clusters. If a receiving node is the cluster head, it filters the data after determining whether the data come from that cluster or a neighboring cluster; Otherwise, the data would be moved to the subsequent cluster. The issue with CLIF is that only excessive data from each cluster and its neighboring clusters will be filtered, leaving some excessive data in the overlaping zones potentially unfiltered and susceptible to transmission to the sink. When there is additional data redundancy in the overlap zones, this issue might be more obvious. The EIFS[3] algorithm employs a clustering structure [15]. Moving the excessive data to the sink without filtering will solve the issue in CLIF, and if this operation is repeated numerous times, the data delivery path would change (thus, some thresholds are considered). But, under some circumstances, this route adjustment can cause the data delivery path to be extended to the sink. Table 1 lists the limitations of each of the three methods outlined above.

Table 1. Comparison of evaluated approaches

APPROACHES	Weak Points
INPFM [17]	Some redundant data may have remained. The computation cost is not appropriate.
CLIF [18]	The computation cost is not appropriate and includes delays Inter-cluster redundant data may be not filtered.
EIFS [15]	Inducing delays. In some cases, changing the route causes that route becomes longer.

4. PROPOSED ALGORITHM

Entire network is divided into clusters. Clustering hierarchical routing algorithm [24] is used for transferring data from head nodes to the base station. In order to reduce energy consumption in transmitting information to the base station, clusters with more nodes were placed near the base station using Huffman's algorithm. Next, Huffman's algorithm is explained with an example.

Suppose there are eight RS (Reader-Sensor) with the following weights. Table (2) (the weight of each RS is equal to the number of tags covered by it)

Table 2: Example of a network with 8 RS and 94 tags.

Reader-Sensor	A	B	C	D	E	F	G	H
Weight(tags numbers)	21	4	10	18	3	10	24	4

Huffman algorithm obtains a tree with the minimum path length of the given weight among all binary trees with eight nodes and eight given weights. Huffman's algorithm works in such a way that in each step it combines two trees that have the minimum root (adds their weight together). The node with less weight is placed on the left side. The first two stages of Hoffman's algorithm will be as follows: Figure (6)

---

[1] In-network phased filtering mechanism

[2] cluster-Based in network phase Filtering scheme

[3] Energy Efficient RFID data filtering scheme

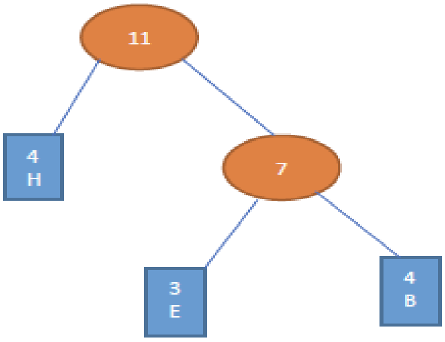


Figure 6. Execution of the first two stages of Hoffman's algorithm

Finally, the Huffman tree will be as follows. Figure (7)

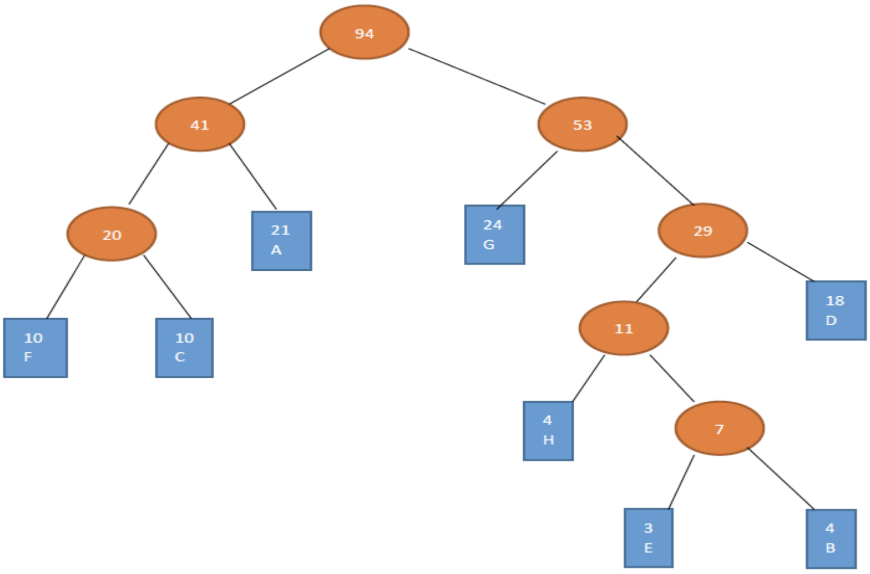


Figure 7. Execution of Huffman's algorithm

4.1. ARCHITECTURE

Figure 8 shows the architecture of the WSN and RFID hybrid network from in proposed plan that Sorted by Huffman's algorithm. It is composed of the five types of nodes as follows:

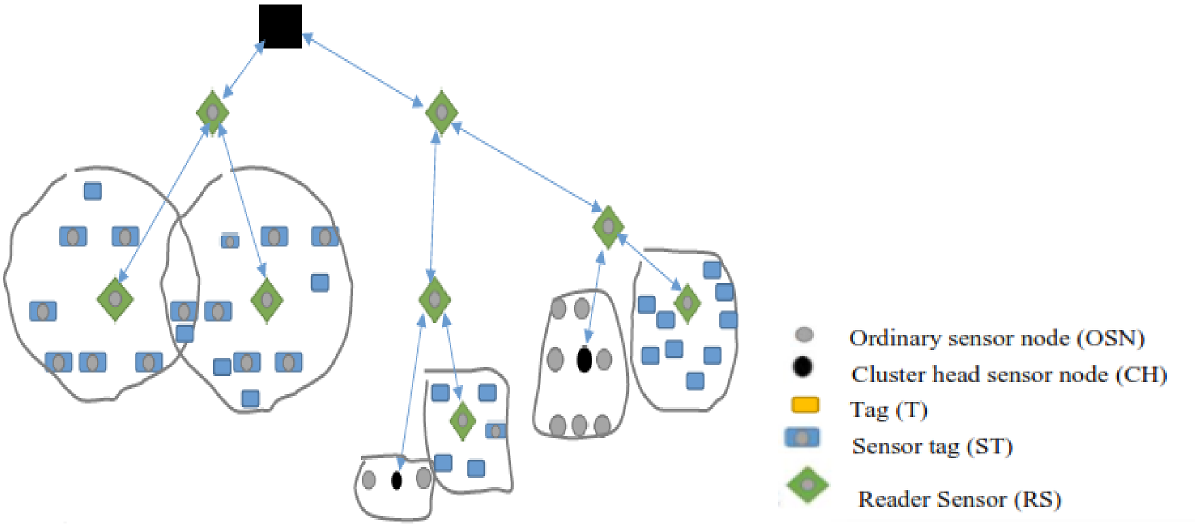


Figure 8. The architecture of the WSN and RFID hybrid network in the proposed plan.

Ordinary Sensor nodes identify the environmental conditions of and relay data to the CH. An example of an OSN is the cluster head node, which is also capable of processing and integrating data among other things. There is just one CH per cluster.

An ST node in this architecture is made up of an RFID tag and a sensor, and it has the ability to sense the surroundings in addition to identifying objects.

Active, passive, and semi-active are the three known types of ST. Batteries are not used by passive ST for sensing or communication. Reader sensor (RS), another component, is made up of an RFID reader and a sensor node that serves as a node. The RS nodes are capable of the several tasks [10]:

- Sensation of the conditions of the environment.

RS can be considered an RFID data reader with sensing capabilities thus, it can sense the conditions of the surroundings (such as temperature, pressure, sound, and …)

- Reading ID number from tag.

These nodes are able to gather information from simple RFID tags within their range. They also contact each other to transmit this information to the base station, in which the collection and process of data are performed by a human.

- Wireless communication with other sand inducing an ad_hoc network.
- Ability of transferring data to other SR nodes or sink nodes as a router

In this architecture, RSs act as head node. RSs and CHs may contact each other, perform as relays, and transfer data between CHs or RSs, or to a base station.

When an RFID data reader reads a tag, the following information is read by RFID reader from a tag:

- ➢ EPC /* Electronic product code */
- ➢ TS /*Time Stamp */

When the reader reads two items of data (for example: a, b), duplication happens if these conditions are satisfied:

1) EPC_a == EPCb.

2) $|TS_a \_TS_b| < t$ /* Constant t is a threshold for difference between TS_a and TS_b */

The duplication data can be divided into the following two types

1) The redundant data inside the cluster:
2) The redundant data between two clusters

These duplication data are filtered at every k hop reader by Proposed algorithm.

Two algorithms are presented. These algorithms are used for detecting duplicate of data and data filtering. As before said, in this architecture there are five type of nodes (RS, ST, T, CH, OSN) that is used in these algorithms. Pseudocodes of algorithms are explained in the following. (Algorithm 1 and Algorithm 2).

```
Filtering decision (params : in coming data )
Begin
 Updateflg =0;  k=0;
 Loop for incoming data
        If   I am a OSN        then   send sensored data to CH
        If   I am a ST or T    then   send data to RS.
        If   I am a CH         then   send data through the route.
        If   I am a RS
            Then  CL-id ← cluster id of incoming data
                   If   Cl-id == my clustered
                      Then    call    INTERNAL FILTERING STEP.
                      ELSE   if     k <  3
                              Then   {send data through the route; exit}
                               ELSE   if   k ==   3   then   Do   Updateflg =1;
                                                                call  EXTERNAL FILTERING STEP;  End.
                            End– if
                   End – if
        End – if
   If   Updateflg==1        then k=0;
                            Else k++;
 End loop
```

Algorithm 1. Filtering decision

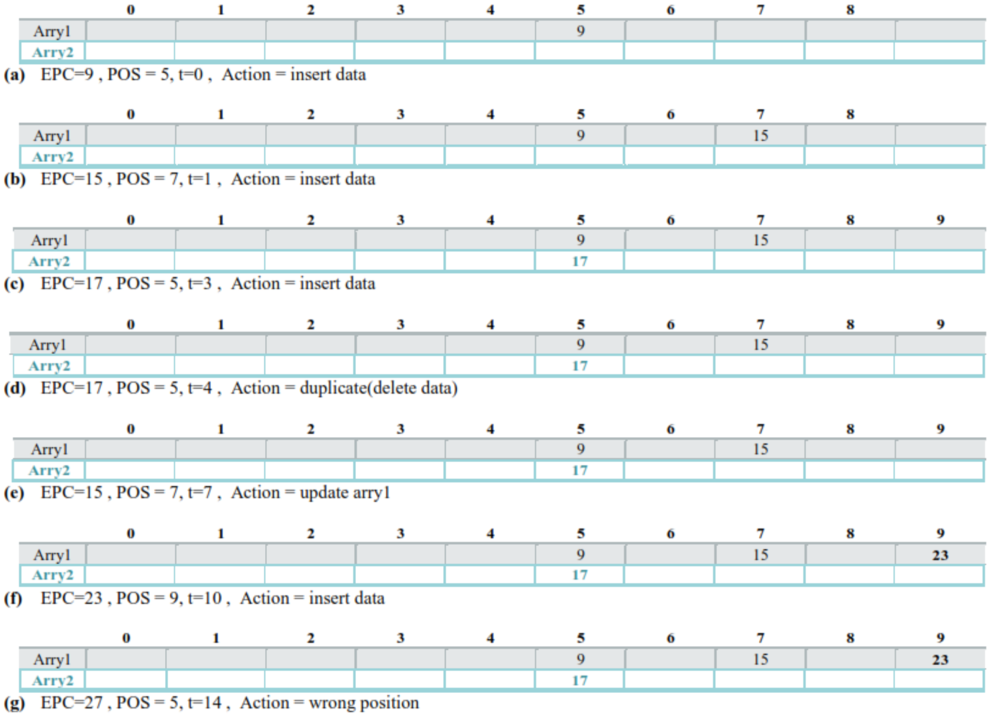
```
TAG {EPC ,
     time ,
     S-D    /*Sensored  data */
    }
EXT – FILTERING ( parameter : TAG )
{        P = hash ( TAG.EPC)
 If ARY1( p ). EPC = = TAG.EPC
   Then If  | ARY1 [p].time  –  TAG.time |  <   Threshold
             Then drop it / * redundant  data * /
             Else update ARY1( p) .
   Else If  | ARY2 [p].time  –  TAG.time |  <   Threshold
             Then drop it / * redundant  data * /
             Else update ARY2( p) .
             Else if  ARY1[p] = = NULL
                  Then ARY1[p] = TAG
                  Else if  ARY2[p] = = NULL
                  Then ARY2[p] = TAG
                  Else False Position.
`
```

Algorithm 2. EXT-Filtering step

Algorithm2 is explained using the read data shown in table 3. Figure 9 clarifies the sequences of read data mappings. In this example, duplication data happens when it is read only for one Tag ID and the time difference is under 3 seconds.

Table 3. An example of read data

time	Tag-EPC
0	9
1	15
3	17
4	17
7	15
10	23
14	27



(a) EPC=9 , POS = 5, t=0 , Action = insert data

(b) EPC=15 , POS = 7, t=1 , Action = insert data

(c) EPC=17 , POS = 5, t=3 , Action = insert data

(d) EPC=17 , POS = 5, t=4 , Action = duplicate(delete data)

(e) EPC=15 , POS = 7, t=7 , Action = update arry1

(f) EPC=23 , POS = 9, t=10 , Action = insert data

(g) EPC=27 , POS = 5, t=14 , Action = wrong position

Figure 9. The steps of inputting data in arrays

5. SIMULATION RESULTS

Simulated data is utilized in this part to analyze the effectiveness of the suggested algorithms function. As previously noted, the nodes are categorized according to cluster shape in this simulation, which was constructed and performed using the C programming language on a Windows 10 computer with an Intel Core i5 processor running at 1.4 GHz and 8GB of RAM. Table 4 shows the complete simulation environment.

Table 4. simulation environment

parameters	values
Area of field	100 × 100 m
Clusters’ number	35
Cluster’s Member	10 - 25
Nodes’ number	800
range of Reading	5m
range of Transmission	10m
Reading interval	3 s
Redundant data ratio	10% and 35%

5.1) False Position Rate (FPR)

In this article, FPR is the rate of unsuccessfulness of elements in the array for each exact number of readings. This is the equation for FPR, where ‘N’ is number of readings and ‘FR’ is number of incorrect positions.

$$\text{FPR} = \left[\frac{FR}{N}\right]\%$$

For finding the best size of the array for a certain value of “N”, some tests were performed.

Figure 10 demonstrates the FPR for distinct numbers of array size i = 10000, i = 20000, i = 30000. The frequency of readings is changed from 2000 to20000 with the increment of 2000 for each step. For all ‘I’ values, FPR hit the lowest point when the number of readings is 1000. The results show to get the minimum FPR, the array size “I” must be five time as much as the number of readings.

5.2) Comparative Analysis Of Filtering Performance

In this experiment, the array size is 50,000, which is five times the maximum read (10,000). Consequently, the FPR value is very low and almost zero. Because of the very small amount of FPR, almost all duplicate data are filtered after every three steps.

Figure 11 shows the amount of data filtering of four approaches (with 10% and 35% duplication). As can be seen, the proposed algorithm exhibits better filtering performance than the other approaches. This is especially evident when the number of readings increases.

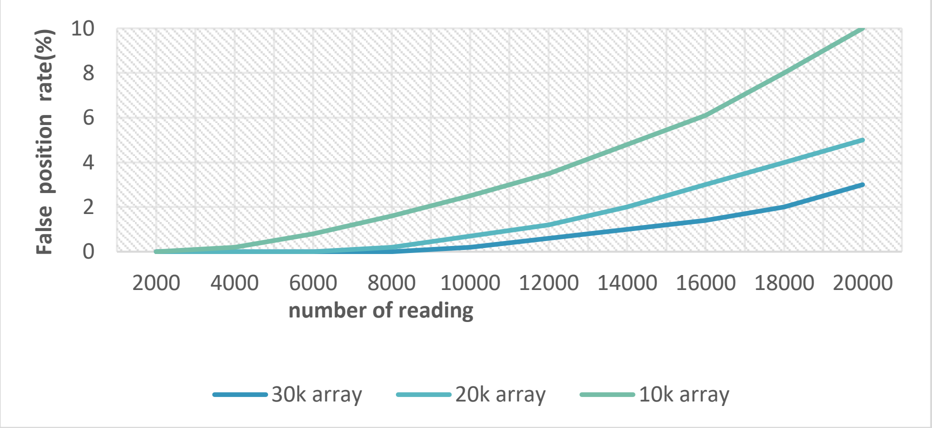


Figure 10. False Position Rate. (FPR)

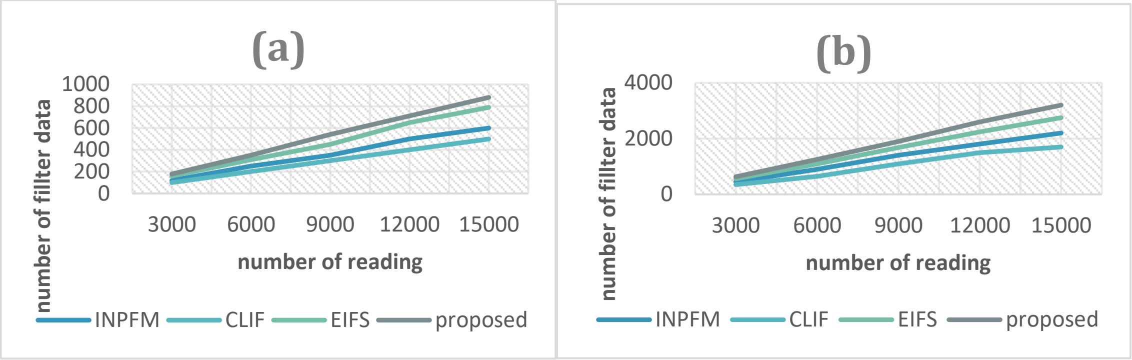


Figure 11. Amount of data filtered (a) 10% replication. (b) 35% replication.

5.3) Comparative Analysis of Processing Time

In the proposed method, the external-filtering function is the only function that is repeated after every three steps. This function takes only O(1) time. Therefore, the processing time of the suggested method will be very short.

Figure 12 compares the processing times of the schemes for filtering duplicate readings. The number of readings is increased from 20,000 to 100,000. In this experiment, the size of the array is set to the highest number of readings as in the previous experiment.

As can be seen, the proposed scheme consumed filtering less time than other schemes (INPFM, CLIF, and EIFS)

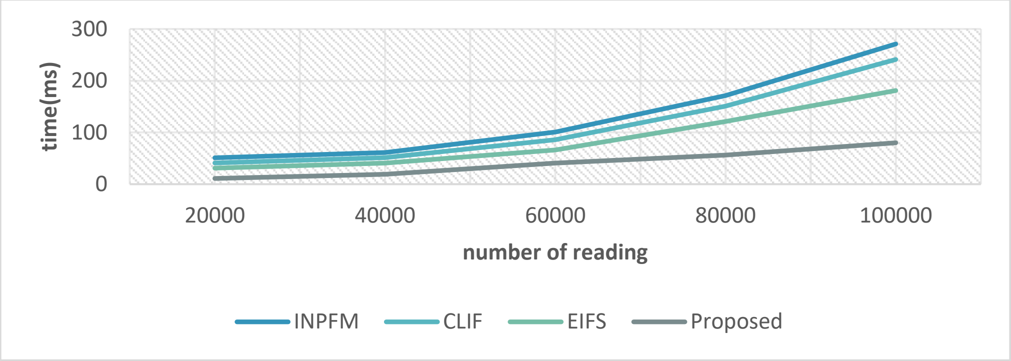


Figure 12. Comparison of processing time for filtering duplicate readings.

5.4) Comparative Analysis of Communication Cost

The comparison of the communication cost has been done by calculating the number of relays required to send information by the nodes to the sink node. The number of relays is obtained from the following equation:

Number of Relays = $\underline{\sum_{i=1}^{Ncl} Ni\ Ri}$

Ri : The number of relays required to send information from the i-th cluster to the sink node.

Ni : The number of nodes in the i-th cluster

N_{CL} : Number of clusters

Due to the fact that in the proposed plan, larger clusters are placed near the sink using Hoffman's algorithm, the number of relays required to transmit information is less than the EILS, CLIF, INPFM methods, as shown in Figure 13.

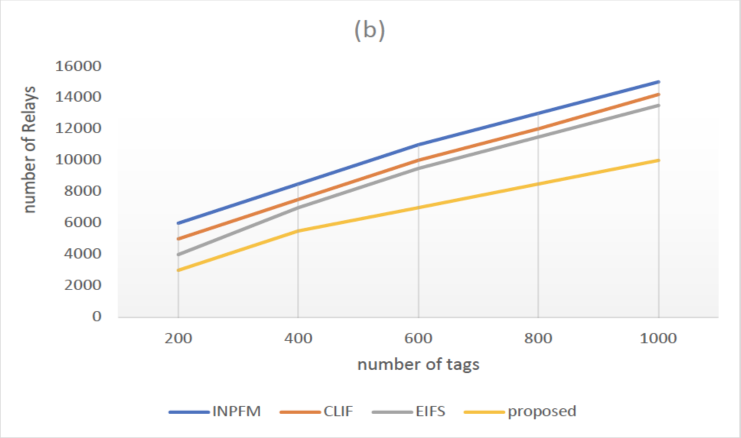


Figure 13. Comparison of relays of the proposed algorithm with other methods

6. CONCLUSION

In this article, after describing the general characteristics of RFID and WSN networks, four classical methods of combining RFID and WSN were described. Some of the challenges of combined RFID and WSN networks are: authentication, real-time performance, energy consumption, data filtering, and data cleaning. Among the above challenges, data filtering and energy consumption is more important. Many algorithms proposed about solving data filtering problem. In this paper, three algorithms: INPFM, CLIF, and EIFS were investigated.

In the proposed method, an architecture for combining RFID and WSN was presented. In this architecture, the clustering method is used to send information and the Hoffmann algorithm is used to reduce energy consumption in sending information. Two algorithms were presented to remove redundant data. Finally, it was shown by simulation that the proposed method filters more redundant data than the evaluated algorithms and reduce energy consumption. It also takes less time, because it takes only O (1) time.

REFERENCES

1. Yarinezhad, R., 2019.” Reducing delay and prolonging the lifetime of wireless sensor network using efficient routing protocol based on mobile sink and virtual infrastructure.” Ad Hoc Netw. 84, 42–55.
2. Yetgin, H., Cheung, K.T.K., El-Hajjar, M., Hanzo, L.H., 2017. “A survey of network life- time maximization techniques in wireless sensor networks. “IEEE Commun. Surv. Tutor. 19 (2), 828–854.
3. Jain, S., 2019. MLBC:” multi-objective Load Balancing Clustering technique in Wireless Sensor Networks. “ Appl. Soft Comput. 74, 66–89.
4. Das, R., and Harrop, 2014-2024 , RFID forecasts, players and opportunities
5. Fei Yuan et al, 2014, “Data density correlation degree clustering method for data aggregation in WSN”, IEEE sensors journal, vol 14, April 2014
6. Ashwini w. Nagpukar. Siddhant k. Jaiawal, 2015, 'An Overliew of WSN and RFID Network Integration", IEEE S Spnsored Second Internal Conferee On Electronics and Communication Systems (Ieecs 2015).
7. Ganjar Alfian et al, 2017,” Integration of RFID, wireless sensor network, and data mining in an e-pedigree food traceability system”, journal of food engineering 212(2017) 65-75
8. Z. Zhao, 2014. “A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem,” Journal of Medical Systems, vol. 38, no. 5, pp. 1–7,
9. C. Jin, C. Xu, X. Zhang, and J. Zhao, 2015, “A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography,” Journal of Medical Systems, vol. 39, no. 3, pp. 1–8,.
10. John Wiley & Sons, 2016, RFID and Network Automation in the food industry, published.
11. Z. Zhang and Q. Qi, 2014. “An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryp- tography,” Journal of Medical Systems, vol. 38, no. 5, pp. 1–7,
12. Barjesh Kochar and Rajender Chhillar, 2012, “An Effective Data Warehousing System for RFID Using Novel Data Cleaning, Data Transformation and Loading Techniques”, The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.
13. Kapoor, G., and Piramuthu, s. (2012), Single RFID tag ownership transfer protocols. IEEE Transactions on Systems, Man, and Cybernetics-c 42(2), 167-173.
14. Myo Min Aung, Yoon Seek Chang and Jang-Un Won, 2012,'"Enterging RFID /USN Application and Challenge”, In International Journal of RFID Security and Cryplography (LIRFIDSC), Mar-Dec 2012
15. Ali Kashif Bashir, Se-Jung Lim, *2011,”* Energy Efficient In-network RFID Data Filtering Scheme in Wireless Sensor Networks”
16. Sarma, S.E. 2009, Towards the five- cent tag. Technical report MIT.AUTOID- WH-006, MIT Auto-ID Center: New NY, USA 2001. Available online: http://www.autoidcenter. Org/research/MIT-AUTOID-WH-006-pdf (accessed on ganuary)
17. Choi, W.; Park, M.S. January 2007, In-network Phased Filtering Mechanism for a Large-Scale RFID Inventory Application. In Proceedings of the 4th International Conference on IT & Applications (ICITA), Harbin, China, January 2007; pp. 401-405.
18. Dong-Sub Kim, Ali Kashif, UIC 2008,” Energy Efficient In-Network Phase RFID Data filtering scheme”
19. Sundaresan, S Doss, R., Piramuthu, S.: and Zhou, W. L. 2014, A robust grouping proof protocol tot RID EP C I di tags. IEEE transactions on information ‘Forensics and security 9(6), 2014
20. Li wang Li Da Xu, 2014, Data cleaning for RFID and WSN Integration. IEEE Transactions Vol.10, No 1. Februry 2014.
21. Zhang, 2009, RFID and Networks AU7777_c018
22. Sundaresan, St, Doss, R., Piramuthu, S., and Zhou, W. L, (2015), Sccurc ownersgip- passivc RFID environment with individnal-owncer privacy. Computer, (2015)
23. X. Wang, Y. Ji, and B. Zhao, 2014. “An approximate duplicate- elimination in RFID data streams based on d-left time bloom filter,” in Web Technologies and Applications, vol. 8709 of Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp.413–424, Springer, Basel, Switzerland, 2014.
24. Mahia Samani, 2011, “A new routing algorithm to reduce consumed energy in wireless sensor”, Third International Conference on Computational Intelligence, Communication Systems and Network