EFFICIENT DATA COLLECTION WITH HRW FOR MOBILE MONITORING APPLICATIONS ON A LARGE SCALE: CLUSTERING TREE ALGORITHM-BASED APPROACH

[#1]**Mr.VANGAPALLI RAVITEJA,** *Assistant Professor*
[#2]**Mr.SADULA SANKEERTH,** *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT
The focus of this paper The Hybrid RFID and WSN system (HRW) streamlines data collection by fusing the conventional RFID technology with the WSN. Smart nodes in HRW combine a radio frequency identification tag, a reader for such tags, and a portable sensor. As a result, the first node to reach an RFID reader can instantly transmit the sensing data of all other nodes through the tags they've collected. Information gathered by RFID readers is transmitted to servers in the back where it may be processed and managed. Its many applications include accelerating the placement process, increasing tag storage capacity, decreasing transmission times, and lowering costs.

Index Terms – Radio frequency identification (RFID), wirelesssensor networks (WSNs), distributed hash tables (DHTs), datarouting.
DOI Number: 10.48047/nq.2021.19.11.NQ21266 **NeuroQuantology 2021; 19(11): 614-618**

1. INTRODUCTION

RFID and wireless sensor networks (WSNs) are useful tools for managing supply chains and keeping tabs on a wide variety of other topics, from health and the environment to corporate operations. Physical or environmental factors, such as temperature or noise levels, are typically the focus of WSN monitoring.

In order to exchange information, RFID tags and RFID readers use radio waves to communicate with one another. Using radio frequency identification (RFID) technology, objects may be uniquely identified, which facilitates monitoring and management.

Only in direct transmission mode can the reader exchange data with the tag when the tag is in range. When a reader encounters multiple identities at once, they will jostle with one another to get access to the channels used to transmit data.

Human Resources Workflow (HRW) creation can be of assistance here. The mobile monitoring solution for large-scale use is effective, inexpensive, and provides real-time monitoring of any target.

2. HYBRID SMARTNODES

Reduced-function sensor

This sensor is unique in that it lacks a transmission function found in most others. Hosts, which detect things like pressure and temperature, are just one source of data used by the system to understand its environment and sensations.

RFIDtag

Like other RFID storage devices, it functions as a standard packet memory buffer. Information like a product's name and characteristics are stored in the RFID tag during production.

Reduced-function RFID reader(RFRR)

Information can be transferred across different smart terminals using this method. Using RFRR, a smart node can access the tags of other nodes and relay that data to its own tag.

3. PROACTIVE DATA TRANSMISSION

Figure 1 depicts the standard RFID layout, whereas Figure 2 demonstrates the HRW system architecture. Both structures are essentially hierarchical in nature. Fast backbone connections allow RFID scanners to communicate with the backend infrastructure. The back-end architecture makes it simpler to offer APIs for applications like hospital information systems. Many item hosts transmit information to RFID readers at the ground level. Information transmission is handled differently by the two systems.

As shown in Figure 1, RFID readers can only pick up data from tags belonging to nodes (hosts) that are in their immediate vicinity during a broadcast. Channel interference, as discussed in Section 1, makes data transmission and collection difficult and slow when the direct transmission option is chosen.

The nodes depicted in Figure 2 are intelligent nodes, capable of exchanging and duplicating tag data through wireless RF channels.

When an RFID reader is close enough to a tag, the reader will pick up the tag's signal. Data from tags outside of an RFID reader's broadcast range can be obtained using a multi-hop transmission mode. HRW will be able to gather information more rapidly and effectively using this strategy. Smart node A uses RFRR technology to add a timestamp to the data it collects before storing it in its tag.

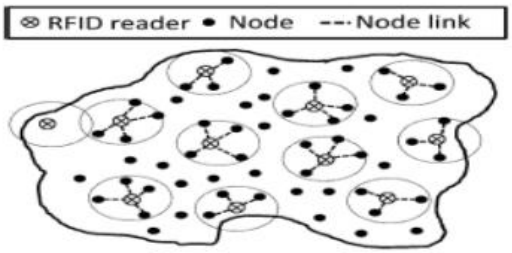


Fig.1.Traditional RFID architecture

The time that node i spent copying data from node j is represented by the notation tij.

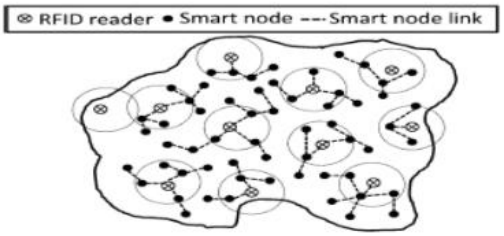


Fig.2.HRW architecture.

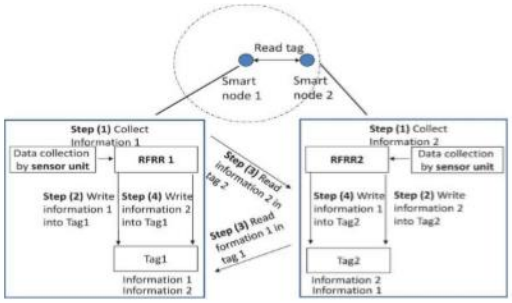


Fig3 Replication process of two smart nodes

When the two nodes next communicate, Node i will ignore any information from Node j that has a timestamp before tij. For example, smart node 3's node 4 may have a timestamp of 11230337, indicating that it was 3:37 a.m. on November 23. When nodes 3 and 4 reconnect, node 3 decides to disregard any replication data with a timestamp earlier than 11230337. By not storing unnecessary information, intelligent nodes reduce the quantity of data that must be transmitted.

4. CLUSTER-BASED DATA TRANSMISSION

Two superior algorithms that work well with this framework are the cluster-member based algorithm and
the cluster-head algorithm. In order for these algorithms to function, the smart nodes must be divided up
into a number of different virtual clusters, each of which is led by a certain individual. The members of the cluster make copies of each other's identification data using the cluster-based technique. An RFID reader can collect data from all the nodes in a virtual cluster by reading a single member's combined tag data when that member approaches the reader.
When using a cluster head-based system, all nodes in the cluster must submit an identical duplicate of their identifying data to the node with the most votes. When the cluster head of a virtual cluster approaches an RFID reader, data from all of the nodes in the virtual cluster is retrieved. This more efficient technique considerably lessens channel congestion, quickens data flows between nodes, and facilitates the elimination of superfluous data inside a cluster. This technique excels at tracking herd-moving subjects (such zebras, animals, and people).

5. COMMUNICATION SECURITY MECHANISMS

Using HRW to relay information over a network of nodes increases the rate of transmission. Some people still have reservations about this approach because they fear for their personal security and anonymity. Since low-cost RFID nodes are easily modified and typically located in a public area, they can be easily compromised. Whoever accomplished this now has complete control over the compromised nodes and can use them to steal sensitive data or even bring the entire system to a halt. In this section, we will examine two potential security vulnerabilities caused by node intrusion attacks: tampering with data and sending just certain data.

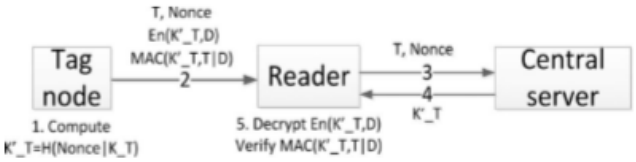


Fig4Procedure for secure data reading and verification.

6. DATA PRIVACY AND DATA MANIPULATION

Before transferring the actual data, the reader communicates the ID N and N to the main computer. The server locates KN, calculates the temporary key K0N, and securely transmits KN to the client. The data DN is tested against the MAC after the reader decrypts it using K0N it obtained from EnK0N. The reader can be confident that the dataset is authentic and the MAC is genuine if it confirms with the MAC obtained from the intelligent node. If not, an adversarial node will replace the EnK0N; DN with a new one.
To avoid detection, an attacker may use an old message repeat attack, in which they replace a newly received message from a node with an earlier message from the same node. Nonce numbers that have already been recorded are easily located when the N and Nonce are delivered to the centralized server. The standard message repeat attack has been identified.

7. DATA SELECTIVE FOR WARDING

The selected cluster head's responsibility in the cluster-head-based transmission technique is to relay the tag data of all cluster members to the reader. A malicious cluster head can selectively discard unneeded data while still delivering necessary information to the correct recipient. These vulnerabilities go undetected because an RFID reader may be unaware of all the smart nodes in a cluster.
To prevent the selective forwarding attack, we can employ the cluster-member based data transmission protocol. Each node in the cluster stores the information of every other node in the cluster according to this protocol. It would be possible for a reader to verify the accuracy of the cluster chief's data by comparing it to that provided by other members of the cluster.

8. EVALUATION ON DATA TRANSMISSION

Use R for 14-meter and 40-meter lengths. Both methods benefit from a marginal reduction in packet-transit time as networks expand in size. If additional nodes are added to a given area but the total number of transmissions remains constant, the result will be a higher node density. As a result, source nodes can more quickly locate other nodes or cluster leaders to transmit their packets to.

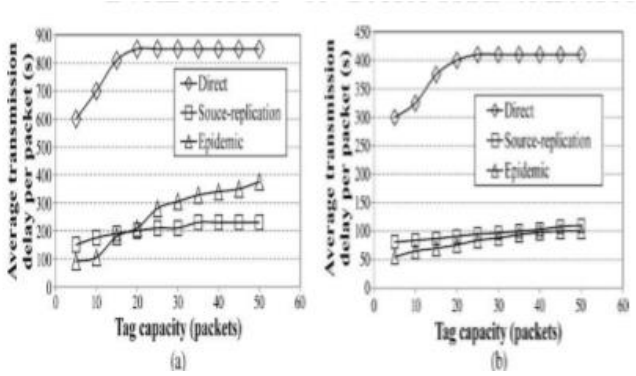
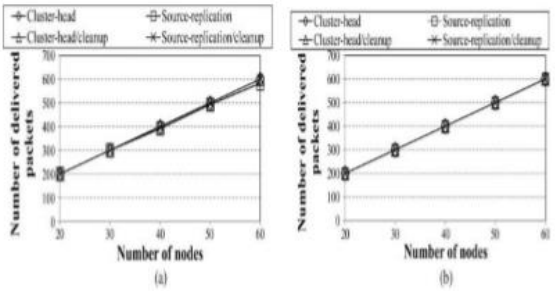


Fig5 Transmission delay versus tag capacity.(a) Range¼20m.(b)Range¼40 m.

In HRW, we used both an epidemic spread and a source-replication spread. The data carried by a node is replicated and sent to other nodes within a specified number of hops as the epidemic progresses. TTL stands for "time to live" in this context. The initial time-to-live setting is 6. A source node will only allow a certain number of receivers to receive its packets during times of source duplication. Typically, this figure is 10. hese methods were compared to the conventional "direct" mode of transmission in RFID systems. Until it is physically close to an RFID reader, a node can transmit information directly by storing it on its tag. When one of the duplicates presents itself at an RFID scanner, the package is considered delivered. In the test, we simply counted the first occurrence of each packet.

9. EVALUATION ON CLUSTER-BASED DATA TRANSMISSION

Figure 6 depicts the typical delay in data transfer at two different distances, 14 20 m and 14 40 m. Readers are not included in this calculation because it is based on the size of the network. Both methods benefit from a marginal reduction in packet-transit time as networks expand in size. If the number of nodes in a given area increases but the quantity of messages remains constant, the result will be a higher node density. This improves the likelihood that source nodes will locate other nodes or cluster heads to transmit their packets to, which in turn accelerates the transfer rate.



1. Fig.6 Comparison of the delivery capacity versus network size.(a) Range¼ 20m.(b)Range¼ 40m.

2.

10. CONCLUSION

The HRW system merges the multi-hop transmision mode of WSNs with the direction transmission mechanism of RFID systems. As a result, mobile monitoring applications can get the low-cost, high-performance, real-time monitoring they need, while also benefiting from improved data gathering efficiency. The HRW system is comprised of hybrid smart nodes and RFID readers. Numerous simulations and data-driven experiments demonstrate that HRW outperforms conventional RFID in terms of installation price, data throughput, transmission time, and tag requirements. Additional safety measures, including testing and approval, should be taken before HRW is utilized in the actual world.

REFERENCES

1. R. Clauberg, ‘‘RFID and Sensor Networks,’’ in Proc. RFID Workshop,St. Gallen,Switzerland,Sept.2004.
2. L. Zhang and Z. Wang, ‘‘Integration of RFID into Wireless SensorNetworks: Architectures, Opportunities and Challenging Problems,’’ inProc. Grid Coop.Compute. Workshops,2006,pp.433-469.
3. H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, ‘‘Taxonomy and Challenges of the Integration of RFID and Wireless Sensor Networks,’’IEEE Netw., vol.22,no.6,pp.26-35,Nov./Dec. 2008.

4. J.Y.Daniel, J.H.Holleman, R. Prasad, J.R. Smith, and B.P.Otis, ‘‘Neural WISP: A Wirelessly Powered Neural Interface with 1-mRange, ’’IEEE Trans.Biomed.Circuits Syst., vol.3, no.6, pp.379-387,Dec. 2009.
5. A.P.Sample,D.J.Yeager, and J.R.Smith,‘‘A Capacitive Touch Interface for Passive RFID Tags,’’ in Proc. IEEE Int’l Conf. RFID,2009,pp.103-109.
6. Z.Li,H.Shen, and B.Alsaify,‘‘Integrating RFID with Wireless Sensor Networks for Inhabitant, Environment and Health Monitoring,’’ inProc.ICPADS,2008,pp.639-646.
7. T. Lez and D. Kim, ‘‘Wireless Sensor Networks and Rfid Integration for Context Aware Services,’’ Auto-ID Labs, Cambridge, MA, USA,Tech. Rep.,2007.