ZKG INTERNATIONAL ISSN: 2366-1313

STREAMLINING HRW DATA COLLECTION FOR EXTENSIVE MOBILE MONITORING APPLICATIONS THROUGH THE IMPLEMENTATION OF A CLUSTERING TREE ALGORITHM

[#1]Dr. T.Veeranna, Associate Professor,
[#2]J. Raja Kala, Assistant Professor,
[#3]Ch. Siva Prakash, Assistant Professor,
Department of Computer Science and Engineering,
SAI SPURTHI INSTITUTE OF TECHNOLOGY, SATHUPALLY, KHAMMAM.

ABSTRACT: This study report is largely concerned with By integrating RFID technology and wireless sensor networks (WSNs), the Hybrid Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) (HRW) system captures the most data possible. The intelligent nodes of the hierarchical routing wireless (HRW) system are made up of three key components: an RFID tag, a portable sensor, and a reader intended to read and interpret RFID tags. As a result, the first node to communicate with an RFID reader can immediately transfer all of the sensory data gathered from other nodes via the tags gathered by those nodes. RFID readers communicate data to backend servers, where it is managed and processed. This technology is useful in a variety of ways, including faster tag insertion, increased store capacity, shorter transfer times, and cost savings.

Index Terms – Radio frequency identification (RFID), wireless sensor networks (WSNs), distributed hash tables (DHTs), data routing.

1. INTRODUCTION

RFID technology and wireless sensor networks, or WSNs, are useful for supply chain management and monitoring a range of elements such as health, the environment, and business processes. WSN tracking typically focuses on tangible or environmental characteristics such as noise levels or temperature.

RFID tags and RFID readers connect using radio waves to send and receive data. Radio frequency identification (RFID) technology can be used to give objects unique names, making monitoring and control easier.

Only when the tag is in direct transmission mode and the reader is within range can it be read. When you provide someone with numerous identities at the same time, they must compete for access to data-carrying channels of communication.

When this happens, the Human Resources Workflow (HRW) plan can come in handy. For many years, this mobile surveillance equipment has proven to be effective, inexpensive, and capable of keeping a watch on any target in real-time.This sensor is distinct in that it lacks a communication function, which other sensors have.

2. HYBRID SMART NODES

Reduced-function sensor

The hosts are the system's only source of information for detecting objects and assessing its surroundings. Their talents allow them to sense a wide range of variables, including temperature and pressure.

RFID tag

As a typical packet memory buffer, this device performs similarly to other RFID storage devices. RFID tags are used in the production process to store critical information such as the product's name and attributes. **Reduced-function RFID reader (RFRR)**

ISSN: 2366-1313

Data can be communicated between intelligent computers using this way. A smart node can receive data from tags on other nodes and relay it to its own tag using RFRR (Radio Frequency Relay) technology.

3. PROACTIVE DATA TRANSMISSION

Figure 2 shows how the HRW device is put together, whereas Figure 1 shows how RFID is commonly configured. Both structures can be thought of as having a hierarchical structure. Because of the availability of fast backbone connections, RFID scanners and the backend architecture can communicate without trouble. Back-end design simplifies and accelerates the provision of application programming interfaces (APIs) for a wide range of applications, including hospital information systems. Several item hosts allow data to be transferred to RFID readers hidden underneath. The two systems exhibit two separate approaches to information management.

Figure 1 shows that during a broadcast, RFID readers can only retrieve data from tags that are attached to nodes (hosts) in close vicinity. The problem of channel interference, as we addressed in Section 1, makes it more difficult to send and receive data quickly and efficiently utilizing the direct transfer method.

The nodes in Figure 2 are referred to as intelligent since they can exchange identification data and communicate with one another over radio frequency channels.

When a tag is in close contact to an RFID reader, the reader detects and records the signal transmitted by the tag. When using a multi-hop transmission mode, you can get data from tags that are not within the broadcast range of an RFID reader. This procedure will allow HRW to learn more rapidly and effectively. Using RFRR technology, smart node A adds a timestamp to the data it receives before storing it in its tag.

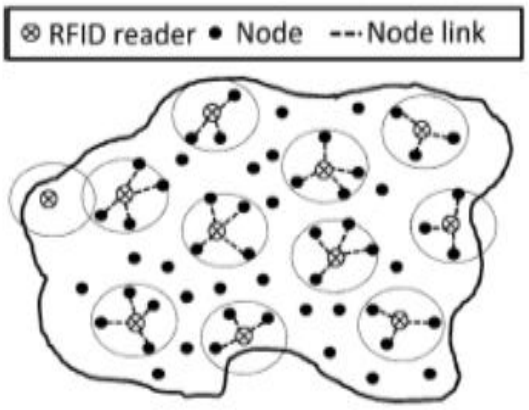

Fig. 1. The traditional method of Radio Frequency Identification (RFID)

The value tij represents the amount of time required to transport data from node j to node i.

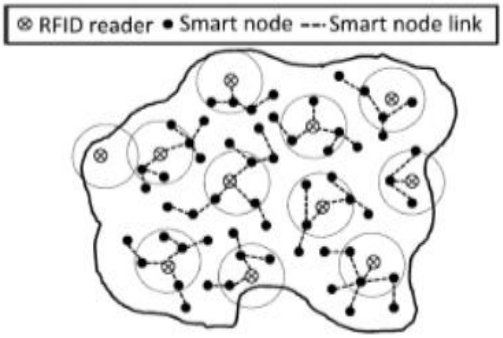

Fig. 2. People are talking about the HRW design industry.

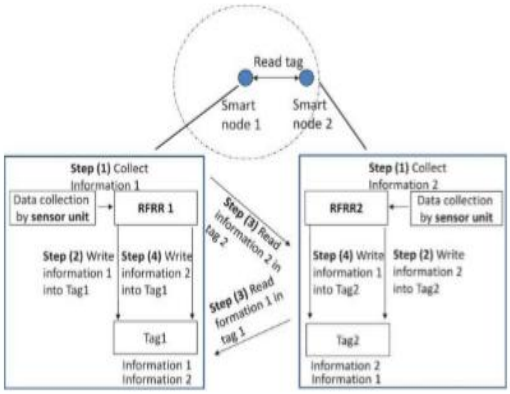

Fig 3 The process by which two intelligent nodes duplicate themselves.

Node I will not utilize data from Node j with a timestamp before tij when the two nodes connect again. Node 4 of smart node 3 may, for example, have a timestamp of 11230337, indicating that it is November 23 at 3:37 a.m. Node 3 is responsible for disregarding any replication data with a timestamp earlier than 11230337 once nodes 3

ISSN: 2366-1313

and 4 are reconnected. By rejecting unneeded information, smart nodes lower the amount of data that must be transferred.

4. CLUSTER-BASED DATA TRANSMISSION

The framework works with the well-known cluster-head methodology as well as the cluster-member-based method. To ensure that these methods work as intended, the smart nodes must be separated into several virtual clusters, each with its own leader. The cluster members use a cluster-oriented technique to replicate each other's identity information. When a member approaches an RFID reader, the reader can read the member's tag's combined tag data. This collects information from all virtual cluster nodes. In a cluster head-based system, every node must submit an exact copy of their own personal information to the node with the most votes. When the virtual cluster's cluster head makes contact with an RFID reader, data from each node in the virtual cluster is received. This strategy boosts speed by drastically lowering channel congestion, accelerating data transmission between nodes, and making it easier to remove unneeded data from a cluster. This is a good method for tracking individual and group movements, including zebras and other animals.

5. COMMUNICATION SECURITY MECHANISMS

Using Hybrid Routing and Wavelength (HRW) speeds up data transmission over a network of connected nodes. There are still those who are concerned about their safety and privacy as a result of this activity. Because they are cheap and easy to modify, inexpensive RFID nodes, which are commonly located in public places, are easily exploited. The individual who executed this operation successfully now has complete control over the hacked devices. This implies they have the ability to steal important data or disrupt the entire system. This section describes two security flaws that could arise as a result of node attack attempts: data modification and sending only a subset of data.

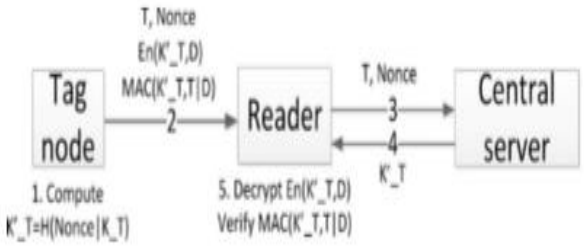

Fig 4 This ensures that data is read and verified without jeopardizing its privacy or integrity.

6. DATA PRIVACY AND DATA MANIPULATION

The reader communicates with the main computer by entering the identifying numbers N and N, which are then followed by the transfer of factual data. The server is in charge of locating KN, executing the calculations required to obtain the ephemeral key K0N, and securely delivering KN to the client. The reader decrypts the data DN using the key K0N obtained during the encryption method EnK0N. The data DN is then checked against the Message Authentication Code (MAC). The dataset is real and legitimate if the MAC (Message Authentication Code) matches the MAC (Message Authentication Code) retrieved from the intelligent node. If this criterion is not met, a malicious node will replace the EnK0N; DN with a new one.

An attacker may use an old message repetition attack to escape detection, which involves replacing a new message with an older message from the same node. It is simple to recover previously recorded nonce numbers when the N value and the nonce are communicated to the central computer. Standard message repeat attacks are generally known and accepted.

7. DATA SELECTIVE FORWARDING

The selected cluster head is responsible for providing the identifying data of each cluster member to the reader in the cluster-head-based transmission mechanism. A bad cluster head can choose which information to leave out while still

ISSN: 2366-1313

ensuring that important information reaches the appropriate receiver. This means that these flaws may have gone undetected because an RFID reader may not have been aware of all smart nodes in a cluster.

The use of the cluster-member-based data transmission protocol reduces the danger of selective forwarding. Each cluster node is responsible for keeping information on the other cluster nodes, according to these principles. Comparing the data provided by the cluster chief to the data provided by other cluster members may assist confirm the accuracy of the chief's data. The computer language R can be used to configure lengths of 14 and 40 meters. Packet-transfer speeds improve in both directions as networks grow. Adding nodes to a given area increases the number of nodes there while keeping the total number of messages constant. This allows source nodes to easily identify and send messages to other nodes or cluster controllers.

8. EVALUATION ON DATA TRANSMISSION

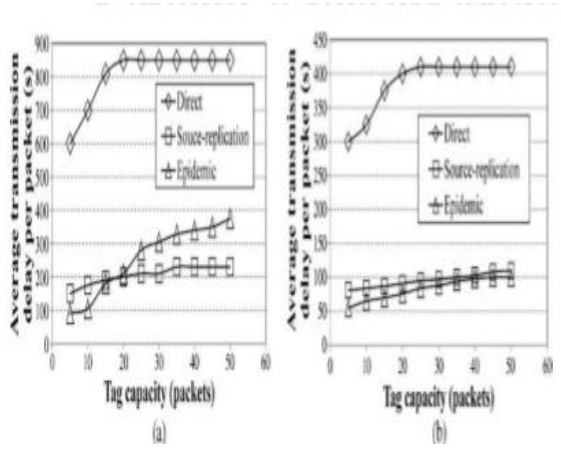

Fig 5 The graph contrasts tag capacity with communication latency. The length is twenty meters. b) The measurement is 40 meters.

Based on the study setting, we used both an epidemic spread model and a source-replication spread model in our research. A node's data is replicated and transmitted to other nodes in a predetermined number of steps. This is the method by which the sickness spreads. TTL now stands for time to live. The default value for the time-to-live argument is 6. Multiple receivers could receive packets from the same source point at the same time. Typically, the value of this number is ten. Radio frequency identification (RFID) systems, in contrast to these tactics, use a direct form of communication. Tags can retain data until they come into contact with an RFID reader, allowing data to be sent between nodes. When an RFID scanner detects one of the duplicates, the box is considered delivered. Throughout the experiment, a simple tally of how frequently each package appeared for the first time was kept.

9. EVALUATION ON CLUSTER-BASED DATA TRANSMISSION

Figure 6 demonstrates the typical lag that occurs when data is transferred over 14 and 40 meter distances. Because of the network's size, this estimate excludes readers. Packet-transfer speeds improve in both directions as networks grow. An increase in node density occurs when the number of nodes in a specific area grows while the quantity of messages transmitted remains constant. This increases the chances of source nodes being able to send packets to other nodes or cluster leaders. This will speed up data transfer.

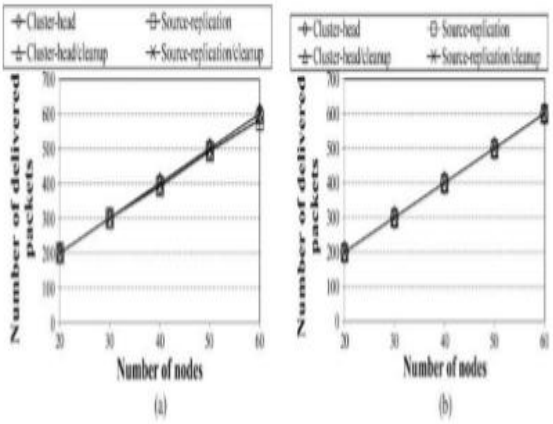

Fig. 6 The goal of this research is to find out how delivery capacity varies with network size. Twenty meters equals one-fourth of the total distance. This distance is approximately twenty-four meters.

10. CONCLUSION

ISSN: 2366-1313

The direction transmission mechanism of RFID systems is merged with the multi-hop transmission method of Wireless Sensor Networks (WSN) in the HRW system. This means that real-time tracking capabilities that are both cheap and useful can be added to mobile monitoring apps, increasing the utility of data collection. HRW is made up of a hybrid intelligent node and an RFID reader. Numerous simulations and data-driven studies show that HRW surpasses the majority of RFID systems in areas such as installation cost, data throughput, transmission time, and tag requirements. HRW must go through additional safety tests before it can be utilized in the real world, including extensive testing and severe approval procedures.

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 Sensor Networks: Architectures, Opportunities and Challenging Problems,’’ in Proc. 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, ‘‘NeuralWISP: A Wirelessly Powered Neural Interface with 1-m Range,’’ 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,’’ in Proc. 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.