An Efficient Data Collection with HRW for Large Scale Mobile Monitoring Applications using clustering tree algorithm

P.Steffy Graf
Department of Communication Systems, PSN College of Engineering and Technology, Tirunelveli

T.Rajesh
Asst. Professor, Department of ECE, PSN College of Engineering and Technology, Tirunelveli

Abstract – In this concise, A hybrid RFID and WSN system (HRW) that integrates the traditional RFID system and WSN system for efficient data collection. HRW has hybrid smart nodes that combine the function of RFID tags, the reduced function of RFID readers, and wireless sensors. Therefore, nodes can read each other's sensed data in tags, and all data can be quickly transmitted to an RFID reader through the node that first reaches it. The RFID readers transmit the collected data to the back-end servers for data processing and management. It is used to improve efficiency, cost of deployment, transmission delay and capability, and tag capacity requirement.

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

1. INTRODUCTION

Frequency Identification (RFID) and wireless sensor networks (WSNs) are two of the most important systems widely used in many monitoring applications such as environmental and health monitoring and enterprise supply chains. WSNs are mainly used for monitoring physical or environmental condition, collecting environmental data such as temperature, sound.

RFID is a technology that uses radio waves to transfer data between RFID tags and RFID readers (readers in short). RFID can be implemented on the objects to be identified, improving the efficiency of individual object tracking and management.

RFID tag data usually is collected using direct transmission mode, in which an RFID reader communicates with a tag only when the tag moves into its transmission range. If many tags move to a reader at the same time, they will contend to access the channels for information transmission.

To overcome this problem, we can implemented a HRW. It has low economic cost, high performance and real-time individual monitoring in large-scale mobile monitoring applications.

2. HYBRID SMART NODES

2.1. Reduced-function sensor

Unlike the normal sensors, this sensor does not have transmission function. It collects the environmental data and the sensed data (e.g., pressure, temperature) from hosts.

2.2. RFID tag

As the normal RFID tags, it serves as traditional packet memory buffer for information storage. The RFID information such as identity and properties is configured into the RFID tag during the production stage.

2.3. Reduced-function RFID reader (RFRR)

It is used for the data transmission between smart nodes. A smart node uses RFRR to read other smart nodes' tags and write the information into its own tag.

3. PROACTIVE DATA TRANSMISSION

Fig. 1 shows the traditional RFID architecture, and Fig. 2 shows the architecture of the HRW system. Both architectures are hierarchical. The upper layer is composed of RFID readers connected to the back-end infrastructure with high-speed backbone cables. The back-end infrastructure connects to the applications (e.g., database in a hospital). The lower layer is formed by a considerable number of object hosts that transmit data to RFID readers. The difference between these two architectures is the transmission mode.

In Fig. 1, only the nodes (hosts) in the transmission range of RFID readers can send their tag information to the RFID readers. As explained in Section 1, this direct transmission mode would lead to channel contention and hence low successful transmission rate and slow data collection.

In Fig. 2, the nodes are smart nodes that can exchange and replicate tag information with each other using wireless RF channels.

Each RFID reader reads tags within its transmission range. Since the data can be transmitted to the RFID reader using a multi-hop transmission mode, each RFID reader can also receive the information in tags outside of its transmission range. In this way, HRW can quickly collect data and expedite the data collection. After smart node A collects the sensed data, it appends the sensed data with a timestamp and stores the data in its tag through RFRR.

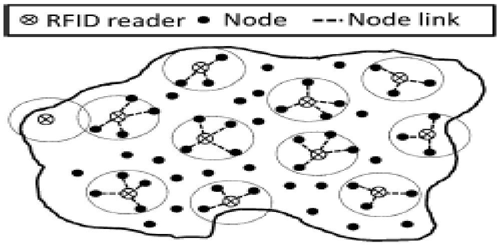

Fig. 1. Traditional RFID architecture

When node i replicates node j's data, node i also records the timestamp of the replication time denoted by tij.

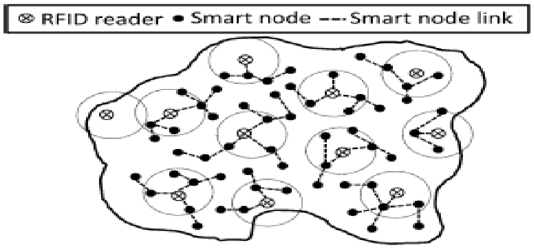

Fig. 2. HRW architecture.

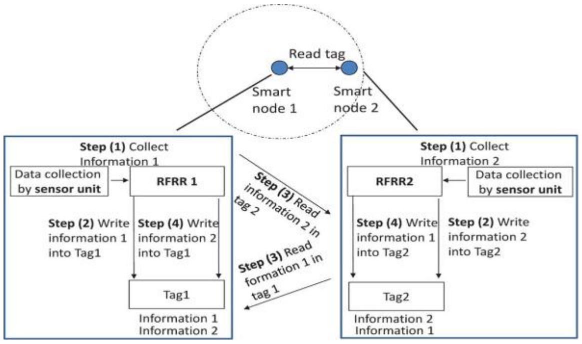
Read tag
Smart node 1
Smart node 2
Step (1) Collect Information 1
Data collection by sensor unit
RFRR 1
Step (2) Write information 1 into Tag1
Step (4) Write information 2 into Tag1
Tag1
Information 1
Information 2
Step (3) Read information 2 in tag 2
Step (3) Read formation 1 in tag 1
Step (1) Collect Information 2
RFRR2
Data collection by sensor unit
Step (4) Write information 1 into Tag2
Step (2) Write information 2 into Tag2
Tag2
Information 2
Information 1

Fig 3 Replication process of two smart nodes

Next time when node i meets node j, node i will not replicate node j's data with timestamps prior to tij. Suppose the timestamp of smart node 3 for node 4 is 11230337, which represents the time 03:37 am, Nov. 23th. When node 3 meets node 4 next time, node 3 ignores the information with timestamp less than 11230337 in the information replication. In this way, smart nodes avoid recording duplicated information, and hence avoid the unnecessary overhead in the transmission.

4. CLUSTER-BASED DATA TRANSMISSION

In this mode, we describe two enhanced algorithms called cluster-member based and cluster-head algorithms, in which smart nodes are clustered to different virtual clusters and each cluster has a cluster head. In the cluster-member based algorithm, cluster members replicate their tag data between each other. When a cluster member of a virtual cluster enters the reading range of an RFID reader, by reading the aggregated tag information from the cluster member, the RFID reader receives all information of nodes in this virtual cluster.

In the cluster head based algorithm, cluster members replicate their tag data to the cluster head. When a cluster head of a virtual cluster reaches an RFID reader, the RFID reader receives all information of nodes in this virtual cluster. This enhanced method greatly reduces channel access congestion, reduces the information exchanges between nodes and makes it easy to erase duplicate information in a cluster. The method is suitable to the applications where monitored objects (e.g., zebras, birds, and people) tend to move in clusters.

5. COMMUNICATION SECURITY MECHANISMS

The multi-hop message transmission mode in HRW improves the communication efficiency. However, such method introduces privacy and security risks. Low-cost RFID nodes are not tamper-resistant and deployed in open environment, thus the attackers can easily physically access and take control of these nodes. The attacker can obtain all the information in the compromised nodes and use the compromised nodes to obtain sensitive information and disrupt system functions. Thus, in this section, we consider two security threats arising from node compromise attacks: data manipulation and data selective forwarding.

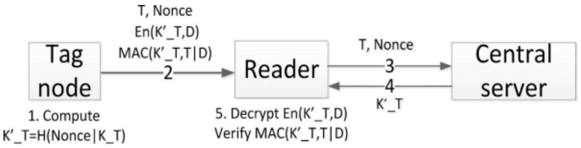

Fig 4 Procedure for secure data reading and verification.

6. DATA PRIVACY AND DATA MANIPULATION

When a reader receives the data, it first sends to the central server the tag ID N and N once. The server finds KN and computes the temporary key K0N, and then securely sends K0N to the reader. After receiving K0N, the reader is able to decrypt the data DN from EnðK0N; DNÞ and then verifies whether MAC is correct. If the recomputed MAC is consistent with the MAC received from the smart node, the reader considers the MAC is correct and the data set is authentic. Otherwise, the EnðK0N; DNÞ is changed by an adversary node.

To avoid being detected for changing data, an adversary may launch old message replay attack by replacing a new message from a node with an old message from the node. When a reader forwards the N and Nonce to the central server, the central server can easily detect outdated nonce values which were reported previously. As a result, the old message replay attack can be detected.

7. DATA SELECTIVE FORWARDING

In the cluster-head based transmission algorithm, the cluster head in each cluster is responsible for forwarding the tag data of all cluster members to the reader. A malicious cluster head can drop part of the data and selectively forward the gathered information to the reader. Since an RFID reader may not know all the smart nodes in a head's cluster in advance, it cannot detect such attacks.

To prevent the selective forwarding attack, we can exploit the cluster-member based data transmission algorithm, in which all cluster members hold the data of all other nodes in the cluster. A reader can compare cluster members' reported data with the cluster head's reported data to verify the correctness of the latter.

8. EVALUATION ON DATA TRANSMISSION

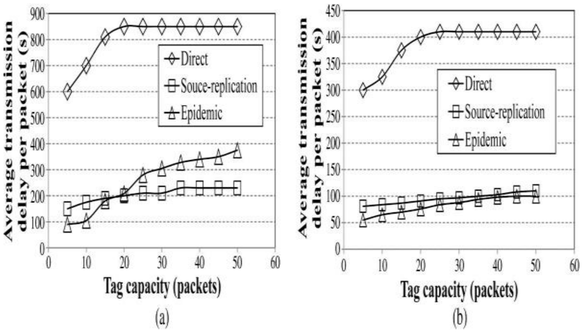

Fig 5 Transmission delay versus tag capacity. (a) Range ¼ 20 m. (b) Range ¼ 40 m.

We used two transmission modes in HRW: epidemic and source-replication. In the epidemic transmission, the packets of nodes are replicated to other nodes within TTL hops, which was set to 6 by default. In the source replication transmission, a source node allows a certain number (10 by default) of nodes to read its packets. We compared these methods with the ''direct'' transmission method in the traditional RFID systems, in which a node keeps its collected information in its tag until it reaches the range of an RFID reader. If one of the copies of a packet arrives at an RFID reader, we consider this packet successfully delivered. We only considered the first delivered replica of a packet in the measurement.

9. EVALUATION ON CLUSTER-BASED DATA TRANSMISSION

Figure 6 shows the comparison results of the average transmission delay versus the network size excluding readers when R ¼ 20 m and R ¼ 40 m, respectively. We see that as the network size increases, the packet transmission delay of both algorithms decreases slightly. The reason is that given the same number of packets, increasing the number of nodes in the same area increases the node density. Therefore, source nodes gain higher probability of meeting other nodes or cluster heads to forward their packets, which reduces the transmission delay.

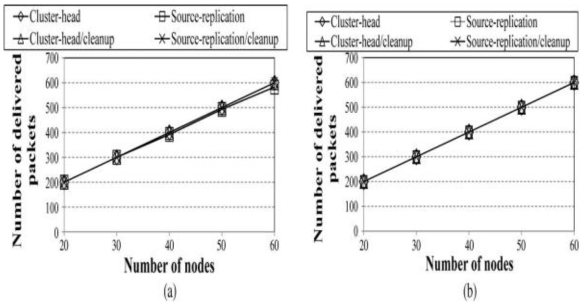

Fig. 6 Comparison of the delivery capacity versus network size. (a) Range ¼ 20 m. (b) Range ¼ 40 m.

10. CONCLUTION

Hybrid RFID and WSN System(HRW) that integrates the multi-hop transmission mode of WSNs and direction transmission mode of RFID systems to improve the efficiency of data collection, hence to meet the requirements of low economic cost, high performance and real-time monitoring in mobile monitoring applications. HRW is composed of RFID readers and hybrid smart nodes. Extensive simulation and trace driven experimental results show that HRW outperforms traditional RFID in terms of the cost of deployment, transmission capacity and delay and tag capacity requirement. It has to be evaluate HRW in a real world tested with more securing mechanisms.

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.