Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 604747, 9 pages
doi:10.1155/2008/604747

Research Article

Performance-Effective and Low-Complexity Redundant Reader Detection in Wireless RFID Networks

Ching-Hsien Hsu,[1] Yi-Min Chen,[1] and Heau-Jo Kang[2]

[1] *Department of Computer Science and Information Engineering, Chung Hua University, Hsinchu 300, Taiwan*
[2] *Division of Computer Engineering, Mokwon University, Daejeon 302-318, South Korea*

Correspondence should be addressed to Ching-Hsien Hsu, robertchh@gmail.com

Received 2 January 2008; Accepted 13 April 2008

Recommended by Jong Hyuk Park

The problems of redundant RFID reader detection and coverage have instigated researchers to propose different optimization heuristics due to the rapid advance of technologies in large-scale RFID systems. In this paper, we present a layered elimination optimization (LEO) which is an algorithm-independent technique aims to detect maximum amount of redundant readers that could be safely removed or turned off with preserving original RFID network coverage. A significant improvement of the LEO scheme is that amount of "write-to-tag" operations could be largely reduced during the redundant reader identification phase. Moreover, LEO is a distributed approach which does not need to collect global information for centralizing control, leading to no communications or synchronizations among RFID readers. To evaluate the performance of the proposed techniques, we have implemented the LEO technique along with other methods. Both theoretical analysis and experimental results show that the LEO is reliable, effective, and efficient. The proposed techniques can provide reliable performance with detecting higher redundancy and has lower algorithm overheads.

1. INTRODUCTION

Radio frequency identifier (RFID) system is an automatic technology aids machines or computers to identify objects, record metadata, or control individual target through radio waves. The RFID system is composed by two components, tags, and readers. An RFID tag is comprised of integrated circuit with an antenna for storing information and communication, respectively. An RFID reader is capable of reading the information stored at tags located in its sensing range. The electronics in the RFID reader use an outside power resource to generate signal to drive the reader antenna and turn into radio wave. The radio wave will be received by RFID tag which will reflect the energy in the way of signaling its identification and other related information. In matured RFID systems, the reader RF can also instruct the memory to be read or written from which the tag contained.

Many applications, such as supply chain automation, identification of products at check-out points, security, and access control, have been developed to take the primary function of RFID systems. Advantages of RFID technologies, such as price efficiency, fast deployment, reusable, and accuracy of stock management also broaden the scope of applications of RFID systems. Advanced characteristics of recent RFID readers, like size miniaturization and capabilities of Wi-Fi or cellular also motivate the development of large scale RFID systems.

In recent RFID technologies, it is motivated that an RFID system can be integrated with wireless sensor network by interfacing RFID tags with external sensing capabilities, such as light, temperature, or shock sensors, forming a hybrid infrastructure that combines advantages of both techniques, such as accurate identification, monitoring of objects, and efficient deployment. Similar to wireless sensor network, RFID tags can be deployed in an ad hoc fashion instead of preinstalled statically. In such way, it will be necessary to install readers in appropriated distance to each other. Otherwise, readers would be interfered with each other from the simultaneous operations. The interference could be caused when the frequency band is shared with other potential users. As an RFID reader is designed to accept the tiny signal reflected from a tag, it will be particularly

influenced to any relatively powerful transmissions from other readers that happen at the same time. Therefore, efficient methods for detecting redundant readers are of great importance for the development of wireless RFID networks.

While the problem of determining coverage redundancy has been studied in wireless sensor networks [1], it differs from the redundant RFID reader elimination problem which was proved as NP-hard problem [2]. In this paper, we propose a randomized and decentralized technique, termed as *layered elimination optimization* (*LEO*), to detect the maximum number of redundant readers that can be safely turned off with preserving the origin network coverage in an RFID network. Advantages of such optimization are twofold; lifetime of wireless RFID network could be extended and reader collisions could be alleviated.

To evaluate performance of the proposed techniques, we have implemented the proposed *LEO* algorithm along with other methods. The experimental results demonstrate that *LEO* provides superior performance in terms of larger number of redundant readers detected. Both theoretical analysis and performance results show that *LEO* has lower algorithm overheads, that is, number of "write-to-tag" operations issued by RFID readers. The performance results also show that *LEO* is suitable in arbitrary RFID network topology and applicable to large-scale RFID environment in practice.

The rest of this paper is organized as follows. In Section 2, a brief survey of related work will be presented. Section 3 introduces the reader collision problem and redundant reader problem. The layered elimination optimization for redundant reader minimization will be discussed in Section 4. Performance analysis and simulation comparisons will be given in Section 5. Finally, in Section 6, some concluding remarks are made.

2. RELATED WORK

Many research results have been proposed in literature. Security- and privacy-related literatures [3–5] focused on methods of preserving and protecting privacy of RFID tags; the RFID reader collision avoidance and hidden terminal problems were first addressed in [6] aiming to enhance accuracy of RFID systems; the energy saving and coverage problem were extensively studied [1, 7–9] in order to improve lifetime of wireless topology network. Since this study is related to reader collision and coverage problem, we will not describe details of security and privacy issues in this section.

Research efforts for collision avoidance have been well presented in literature. Frequency division multiple access (FDMA), code division multiple access (CDMA), time division multiple access (TDMA), and carrier sense multiple access (CSMA) are four basic access methods to categorize MAC-layer protocols [10]. FDMA is functioned via frequency assignment in which the communication is applied in form of many-to-one. Since RFID tags without a frequency tuning circuitry, reader selection is not allowed during communication. Therefore, the addition of such a tuning circuitry will increase the cost of the RFID tags and deployment of RFID systems. CDMA uses spectrum modulation techniques that based on pseudorandom codes for data transmission. It is more complicated and computation intensive due to additional circuitry to the tags which also bring up the cost of tags. TDMA uses time slot for ensuring that messages do not collide. Because there is only one code transmitted during each slot, it allows readers to communicate using different time slot that successfully avoid the collision. To accommodate better read rate in dynamic RFID system, time slot should be reshuffled adaptively. CSMA enables individual data transmission by detecting whether the medium is busy. For hidden terminal problems in RFID networks, the interference of signals of two different readers may still happen due to each of the reader is not in the other's sensing range. Thus, CSMA is not able to avoid collisions caused by a hidden terminal in wireless RFID networks.

Standard collision avoidance protocols like RTS-CTS [11] cannot be directly applied in RFID systems due to the reason, in traditional wireless networks, the CTS are sent back to the sender. Similar situation in RFID system, when a reader broadcasts an RTS, all tags in the read range need to send back CTS to the reader. It then requires another collision avoidance mechanism for CTS, and it will make the protocol more complicated.

Techniques for resolving RFID reader collision problems are usually proposed as reader anticollision techniques or tag anticollision solutions. The *Colorwave* [12] is a scheduling-based approach prevents RFID readers from simultaneously transmitting signal to an RFID tag. The *Colorwave* is used as a distributed anticollision system based on TDMA in RFID network. *Pulse* protocol [13] is referred as beacon broadcast and CSMA mechanism [14]. Readers periodically in separated control channels send a "beacon" during communication with tags. The *contend_back-off* and the *delay_before_beaconing* in the protocol are similar in wireless networks. If the reader receives a beacon, the residual back-off timer will be stored and kept till the next coming chance. This process is expected to achieve the fairness among all readers. A coverage-based RFID reader anticollision mechanism was proposed in [15]. Kim et al. presented a localized clustering coverage protocol for solving reader collision problems occurring among homogeneous RFID readers. HiQ [16], an online learning algorithm, is used to find dynamic solutions to the reader collision problem in RFID systems. The focus of the HiQ algorithm contains two parts: first, HiQ is used to allocate resources to maximize the number of readers communicating at a single time period; second, HiQ is used to minimize the number of collisions among readers' communication. In [17, 18], Cha and Kim proposed two ALOHA-based algorithms with a tag estimation method (TEM) for speedup object identification in RFID systems.

The problem of coverage in wireless sensor networks [19] has been also variety studied. Jiang and Dou [20] presented a decentralized and localized density control algorithm that prolongs network lifetime by keeping a minimal number of sensors in active mode while not scarifying any sensing coverage. Tian and Georganas [1] proposed techniques

for detecting redundant sensors whose coverage area is overlapped with others. In addition, Tanaka and Sasase [21] propose two distributed interference avoidance algorithms based on the detect-and-abort principle for multichannel readers which can effectively mitigate the reader-to-tag interference as well as the reader-to-reader interference. In [8], Ye et al. presented an energy-conserving protocol to extend lifetime of wireless sensor network. The concept of working set was applied in their approach to alternatively turn sensors off and on. A similar research is also presented by Carle and Simplot-Ryl [22]. A centralized algorithm was proposed in [7] for organizing sensor network in disjoint subsets of sensors, in order to maximize efficient use of batteries. On the contrary, Zhang and Hou [9] proposed a grid-based distributed algorithm for maintaining coverage and connectivity. Focusing on RFID system, Carbunar et al. [2] proposed an approximation algorithm for extending lifetime of wireless RFID reader network. Preserving network coverage and eliminating redundancy in a network, energy efficiency could be improved. Probabilistic analysis and experimental results report that the *RRE* heuristic is effective in arbitrary topology. A recent work [23] has been proposed for addressing both redundancy and coverage detection in sensor network. One of the drawbacks of the RRE algorithm is that each RFID reader needs to write its tag count (number of covered tags) and reader ID onto all its covered tags. This could lead higher transmission overheads and incur higher complexity of write-to-tag operation. In this paper, we propose an efficient redundant reader elimination method, termed as *LEO*, which can improve the shortcoming of the *RRE* algorithm.

3. PRELIMINARIES

A reader is redundant if all its covered tags are also covered by at least one of the other readers. Figure 1 shows an RFID network contains three readers, R_1–R_3, and five tags, T_1–T_5. Reader R_2 is referred as redundant reader because the three tags it covers, that is, T_2, T_3, and T_4, are also covered by other readers in the same network. Therefore, reader R_2 can be safely removed without loss of covered tags. Advantages of removing redundant readers are twofold. First, because of the limited battery associated with wireless RFID readers, it can extend the lifetime of overall wireless RFID network if the redundant readers are turned off alternatively. Second, the reader-to-reader interference could be alleviated by eliminating redundant readers. Consequently, reader collisions could be dispelled with the monitoring accuracy of RFID network which can also be improved.

A naïve method to detect reader redundancy is to have all readers broadcast a query message to all its covered tags simultaneously. Because RFID tags will reply queries by signaling its id, therefore, if a reader receives no reply, it means that it is a redundant reader. This is either because the reader covers no tag in its covered range, or because tags are not able to reply due to reader collisions.

There are drawbacks of the above method to detect reader redundancy. Firstly, time synchronization among readers is required. Second, network coverage may be

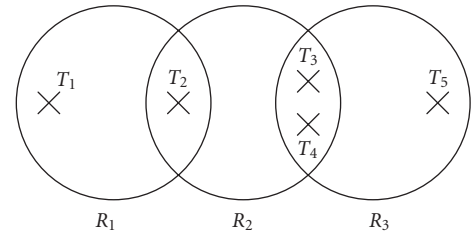


Figure 1: Example of wireless RFID network with redundant reader.

destroyed and resulting additional tags uncovered if all redundant readers are turned off. The second situation can be explained by taking the same network topology shown in Figure 1. We assume the same readers, R_1–R_3, and only four tags, T_1–T_4, existence in the RFID network. According to the above description, readers R_2 and R_3 will receive no tag reply and treat itself a redundant reader (tags T_2, T_3, and T_4 are unable to reply queries from readers because readers R_1 and R_2 collide at tag T_2, and readers R_2 and R_3 collide at tags T_3 and T_4). Therefore, if readers R_2 and R_3 are both turned off, it will result in that tags T_3 and T_4 will be uncovered.

The following statements clarify our network model, research assumptions, and characteristics of *LEO*.

(i) There is no restriction in the RFID network model. An RFID system could be of arbitrary topology with unlimited number of RFID readers and tags.

(ii) RFID Tags are passive and the associated memory is writable.

(iii) Reader collision problem is assumed avoided before running redundant reader identification.

(iv) The proposed *LEO* is a distributed scheme, need not to collect global network information for centralizing control, leading no communications and no need of time synchronization between RFID readers. Each reader performs redundancy check locally.

4. THE LAYERED ELIMINATION OPTIMIZATION

As mentioned previously, *LEO* has advantages in practice, such as it is designed for arbitrary RFID network topology; there is no communication between RFID readers, and there is no need to perform time synchronization. The only assumption in *LEO* implementation is that reader collisions are avoided before running *LEO*. Since there are many previous published papers on contention-free transmissions of RFID readers that can avoid collisions caused by hidden terminal, we discuss the phase of collision avoidance in this study.

To verify beneficial of the proposed *LEO* technique, we briefly review the redundant reader elimination (*RRE*) algorithm. To simplify the presentation, we depict the operation of redundant reader identification in the *RRE* algorithm as an interaction flow shown in Figure 2(a).

The concept of *RRE* algorithm is to record "*tag count*", number of tags a reader covers, into RFID tags' memory.

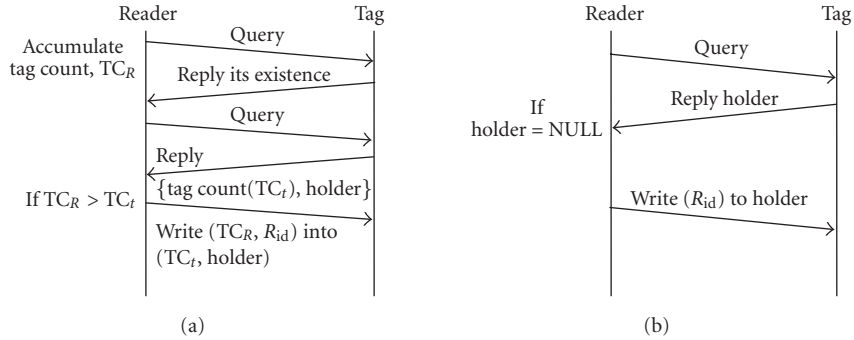


Figure 2: Interaction of redundant reader identification (a) *RRE* algorithm, (b) *LEO* algorithm.

Only the reader has maximum *tag count* could be holder of the corresponding RFID tag. Therefore, at the beginning, an RFID reader (R_i) will send a query for accumulating number of tags in its vicinity. Then, it queries all of these tags for their holder (i.e., the reader who wrote maximum *tag count* onto the tag). If *tag count* of the holder is smaller than R_i's *tag count*, R_i writes its *tag count* onto the tag and records its id to tag's holder. Oppositely, reader R_j will be regarded as redundant if holders of all its covered tags are not R_j and their origin tag counts are larger than R_i's tag count. In such way, each tag will be written at least two data, "*tag count*" and "*holder*". Furthermore, the "*tag count*" and "*holder*" of a tag might be updated by a later query RFID reader if the reader *tag count* is larger than previous value.

The layered eliminate optimization simplifies the above method. An RFID reader only writes reader id into a tag. Once a tag is written by another reader, the later query RFID reader will not overwrite the tag. Therefore, the total number of write operations is at most equal to the number of RFID tags in the RFID network (it is possible for tags not covered by any reader in a given RFID network. In such situation, the total number of write-to-tag operations is less than amount of tags in the network).

Figure 2(b) shows the operations of redundant reader identification in *LEO* algorithm. The term "layered" represents the relationship between early query RFID readers with the later query ones. Relatively, for later query reader, it will have higher probability to be redundancy.

Referring to the operations of *LEO* outlined in Figure 2(b), an RFID reader (R_i) broadcasts a query message to tags in its vicinity asking tags' holder. Once tag replies its holder, there are two possibilities, holder = "NULL" or holder = "R_k", where R_k is one of the readers in the RFID network. If holder = "NULL", R_i writes its id onto the tag holder. If holder = "R_k" and $R_k \neq R_i$, R_i skips the reply. Therefore, an RFID reader will be regarded as redundant if it receives tag replies which are all nonNULL.

Let us demonstrate the identification of redundant reader in both *RRE* and *LEO* by taking the example shown in Figure 3. Table 1(a) illustrates the contents of tags' memory modified by each RFID reader when issuing a query/write operation. The appearance of RFID readers is assumed in numerical order, that is, R_1, R_2, and R_3. Reader R_1 firstly

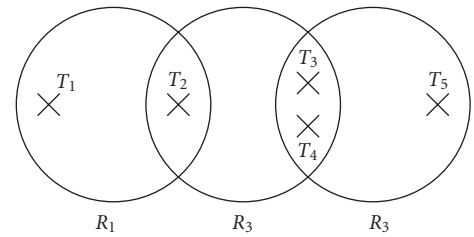


Figure 3: The second example of redundant reader.

writes its *tag count* (TC) = 2 and id into tags T_1 and T_2 (first row of the table). Then, R_2 writes (TC, R_{id}) = (3, R_2) into all its covered tags, T_3, T_4, and T_5. In the following, reader R_3 attempts to write (TC and R_{id}) into its covered tags, T_2, T_3, and T_4. Because tags T_3 and T_4 have the same *tag count* which was written by reader R_2, and T_2's *tag count* of its holder is smaller than R_3's *tag count*, therefore, R_3 will only overwrite (TC, R_{id}) in T_2. Finally, tags T_1–T_5 will be held by readers, R_1, R_3, R_2, R_2, R_2, respectively. That means no redundant reader could be detected.

Consider again the example by using *LEO* redundant reader identification. According to the interaction flow described in Figure 2(b), reader R_1 firstly marks tags T_1 and T_2 as its responsible tags. Then, reader R_2 writes its id as holder of the three tags in its vicinity. Following operations of R_1 and R_2, reader R_3 will not issue write operation to tags T_2, T_3, and T_4 because of their nonnull holder. Consequently, tags are finally held by readers R_1 and R_2 which makes reader R_3 redundant as shown in Table 1(b). This example shows that *LEO* detects one redundant reader which was not detected by the *RRE* algorithm. It is worthy to mention that the different order of queries by RFID readers might have different results. As a result, the *RRE* could be better in other permutation with different order of active RFID readers. We will discuss the performance of miscellaneous comparisons by these two approaches in Section 5.

On the other hand, for safety concerns of the proposed method, recall that *LEO* is an extended approach that based on the *RRE* scheme; it is sufficient to prove that the *LEO* is safe. In a wireless RFID network, the false positive will not happened in either *RRE* or *LEO* techniques, namely, the *LEO*

Table 1: Redundant reader identification for the second example: (a) result of *RRE*, (b) result of *LEO*.

(a)

	T_1	T_2	T_3	T_4	T_5
R_1	$(2, R_1)$	$(2, R_1)$			
R_2			$(3, R_2)$	$(3, R_2)$	$(3, R_2)$
R_3		$(3, R_3)$			
Final	$(2, R_1)$	$(3, R_3)$	$(3, R_2)$	$(3, R_2)$	$(3, R_2)$
Redundant reader			*N/A*		

(b)

	T_1	T_2	T_3	T_4	T_5
R_1	R_1	R_1			
R_2			R_2	R_2	R_2
R_3					
Final	R_1	R_1	R_2	R_2	R_2
Redundant reader			R_3		

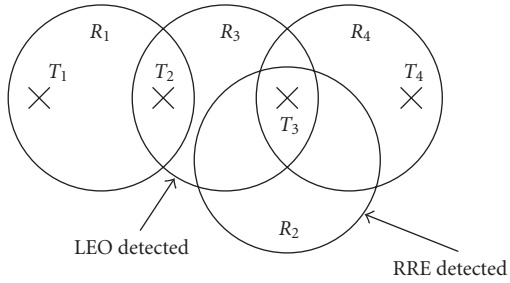


Figure 4: The third example of redundant reader.

will not turn off an RFID reader that covers tags not covered by active readers.

In practice, *LEO* is an algorithm-independent optimization technique. It can be executed either independently (one-phase scheme) or combined with other redundant reader elimination methods (i.e., two phases scheme) to enhance algorithm performance. Let us consider the third example shown in Figure 4 and apply both *LEO* and *RRE* algorithms to demonstrate this feature.

Figures 5(a) and 5(b) show the results after performing *RRE* and *LEO* algorithms, respectively. Both of the two algorithms detected one redundant reader. Exchanging the two algorithms to the reduced RFID networks obtained in Figure 5, that is, executeing *LEO* in Figure 5(a) and executeing *RRE* in Figure 5(b), the resulting network from the second round redundant reader identification performed by *RRE* + *LEO* and *LEO* + *RRE* schemes is shown in Figure 6. The two-phase redundant reader identification detected one more redundant reader in both cases as compare to the single phase scheme. Due to this reason, two-phases scheme is expected to have has superior performance in term of total

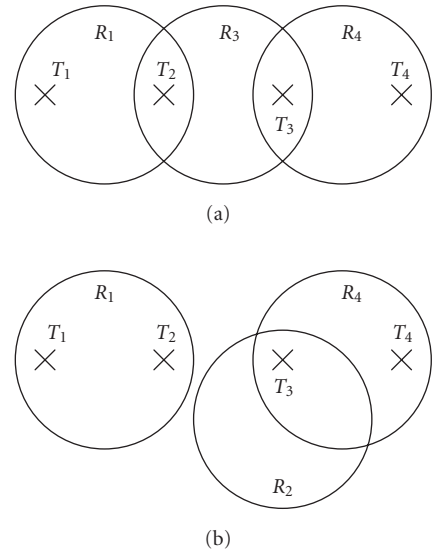


Figure 5: The reduced RFID network after performing (a) *RRE* and (b) *LEO*.

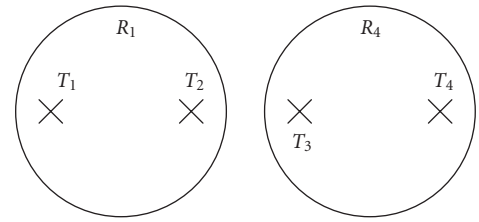


Figure 6: The reduced RFID network after performing *RRE* + *LEO* and *LEO* + *RRE*.

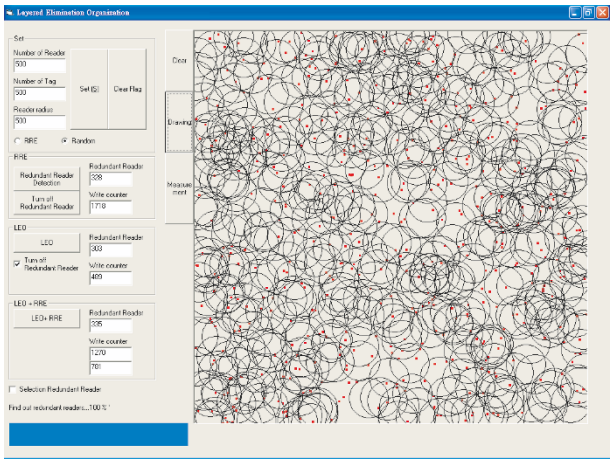
number of redundant readers detected. However, two phases scheme might have higher algorithm overheads because RFID readers will record *tag count* and *reader id* in both phases. As mentioned earlier, *LEO* has lower algorithm overheads (i.e, number of *write-to-tag* operations) than *RRE*. For these two composite approaches, *LEO* + *RRE* and *RRE* + *LEO*, we will recommend using *LEO* + *RRE* in practice. This is because most of redundant readers can be removed by *LEO* in the first phase. In such way, there will have less number of RFID readers in network and expecting lower overheads of the *RRE* algorithm in the second phase. A detailed analysis will be discussed in Section 5 with algorithm overheads comparison.

5. PERFORMANCE EVALUATION AND RESULTS

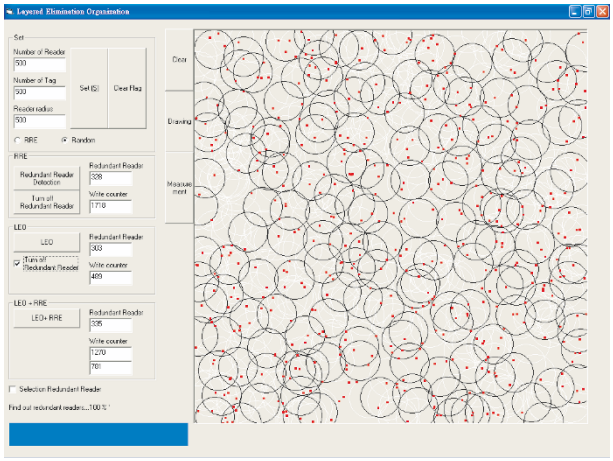
In this section, we first introduce the simulator, a random RFID network generator and explain metrics for performance comparison. Then, we will discuss the results of performance evaluation.

5.1. Simulator and comparison metrics

To evaluate performance of the proposed optimization technique, we have implemented a random RFID network



(a)



(b)

Figure 7: Snapshot of RFID network simulator: (a) a randomly generated RFID network, (b) network topology after redundant readers are removed.

generator to simulate various circumstances. The simulator uses number of readers, number of tags, and reader radius as parameters to produce network topologies with different characteristics. Three optimization approaches, *RRE*, *LEO*, *LEO* + *RRE*, were tested in the experiments. The simulation results will report number of redundant readers detected and number of write operations issued by RFID readers in each algorithm. Figure 7(a) shows snapshot of a randomly (uniform distribution) produced RFID network with 500 readers before redundancy checking. Figure 7(b) shows the snapshot of the network after redundant readers are removed.

As mentioned earlier, the objective of redundant reader problem is to detect maximum number of readers that can be removed safely without changing network coverage. Therefore, we will evaluate the number of redundant readers detected by each algorithm. In addition, we also evaluate algorithm complexities by calculating number of "write-to-tag" operations issued by all RFID readers. In short, the larger the number of redundant readers detected, the lower the number of "write-to-tag" operations issued by RFID readers, and the algorithm is better.

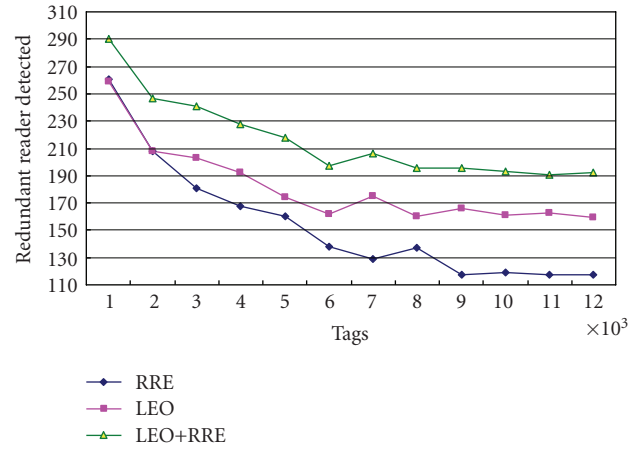


Figure 8: Comparison of redundant reader detected with network area 10000 × 10000, reader radius = 500, and number of reader = 500.

5.2. Experiment results

The first experiment is conducted under a fixed number of RFID readers with an increasing amount of RFID tags. The number of redundant readers detected by different algorithms is reported. Figure 8 shows that the *LEO* performs better than the *RRE* in terms of amount of redundant readers detected under the network configuration with 10000 × 10000 network area, radius of reader's sensing range = 500 and number of readers = 500. However, both techniques detect less number of redundant readers than the composite approach, that is, *LEO* + *RRE*. As mentioned in Section 4, *RRE*+*LEO* scheme is not recommended in practice due to its very high algorithm overheads. Therefore, our experiments only show the results of *LEO* + *RRE*. Observing the results shown in Figure 8, we noticed that when the number of tags is increased, the number of redundant readers is decreased. This is because that a reader may cover new RFID tags in high-density environment while it covers no RFID tag in lower density environment, making such RFID reader nonredundancy in high-density RFID systems.

Figure 9 compares the overheads of different schemes. The overhead is referred as amount of "write-to-tag" operation issued by all RFID readers in order to detect redundancy correctly. We observe that *LEO* < *LEO* + *RRE* < *RRE*. This phenomenon matches our expectation that indicates that *LEO* has least amount of *write* operations and *RRE* performs worst. According to the description in Section 2, we know that an RFID reader needs to write both "tag count" and "reader ID" onto its covered tags in the *RRE* scheme. On the contrary, an RFID reader only needs to write "tag count" in the *LEO* method. As a result, the *LEO* has $\theta(m)$

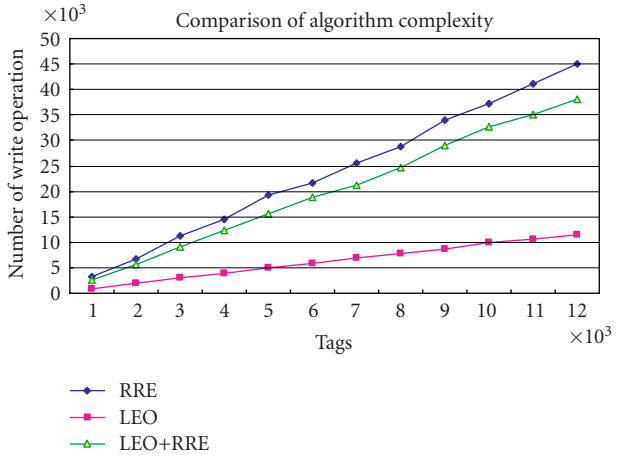


Figure 9: Comparison of number of write operations with network area 10000 × 10000, reader radius = 500, and number of readers = 500.

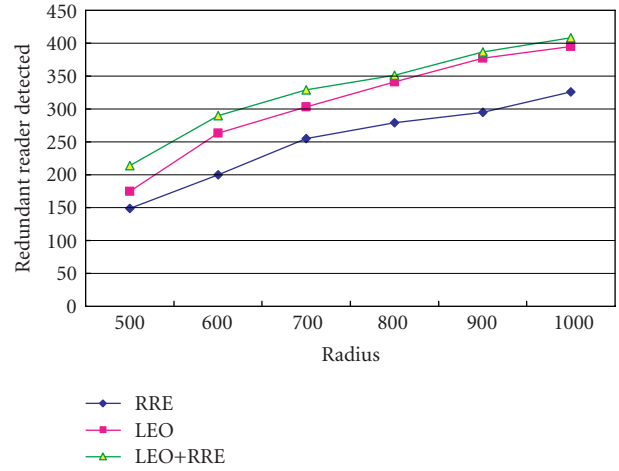


Figure 10: Comparison of redundant reader detected with network area 10000 × 10000, number of tags = 4000, and number of readers = 500.

as upper bound of *write* operation while *RRE* has $\theta(2m)$ as lower bound under the assumption that each tag is covered only by one RFID reader, where m is the number of RFID tags. Moreover, if an RFID tag is covered by r readers in average, the *RRE* will have $\theta(2mr)$ as lower bound of write operation while *LEO* remains $\theta(m)$ as upper bound. Reason for *LEO* + *RRE* has less algorithm overheads than *RRE* is because *LEO* removes most of redundant readers in the first identification phase, the overheads of *RRE* algorithm could be largely reduced in the second phase.

Figure 10 shows the performance comparison of the algorithms by increasing radius of readers' sensing range. As the amount of RFID tag is fixed, when radius of RFID readers' sensing range is increased, the coverage of an RFID reader becomes wider, making RFID readers cover more RFID tags that might be also covered by other RFID readers. This is the main reason for the three methods detect higher redundancy when RFID reader's sensing radius is increased. Furthermore, the *LEO* + *RRE* scheme has best performance in terms of total number of redundant readers detected. Compared with the *LEO* scheme, the improvement of *LEO* + *RRE* is not significant. On the contrary, the *RRE* performs worst in terms of number of redundant readers detected.

Once again, Figure 11 demonstrates the algorithms overheads by estimating the number of write-to-tag operations and has the order, *LEO* < *LEO* + *RRE* < *RRE*, which is similar to the observation we obtained in Figure 9. One thing worthy to mention is that the *LEO* has a constant number (equal to number of tags) of *write* operations even under different reader sensing radius. This is because the number of tags remains fixed in this experiment.

From the above analysis and observation, the *LEO* presents superior performance in both redundancy checking and algorithm overheads. Overall speaking, the *LEO* or *LEO* + *RRE* could be a good choice to handle the redundant reader problem. On the contrary, the *RRE* presents a comprehensive solution that aims to solve reader collision

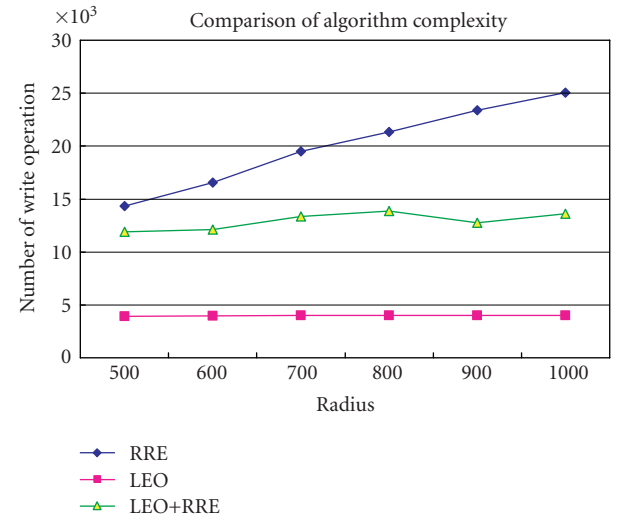


Figure 11: Comparison of number of write operations with network area 10000 × 10000, number of tags = 4000, and number of readers = 500.

problem and reader redundant problem. If one considers handling both collision and redundant problems by using an integrated approach, the *RRE* could be helpful in such need. Otherwise, the *LEO* can be considered as an efficient approach to handle only redundant problem.

Figure 12 shows the accumulated redundant reader detected by *LEO* and *RRE* with multiphase optimization. As shown in Figure 12(a), the *LEO* technique has better performance than the *RRE* scheme at the beginning (i.e., the first and second phases). As the *RRE* scheme could not detect more redundant readers after the third phase, the *LEO* technique has sustained optimization until the 9th or 10th round. It is shown that even some redundant readers cannot be detected in early phases (false negative); they are

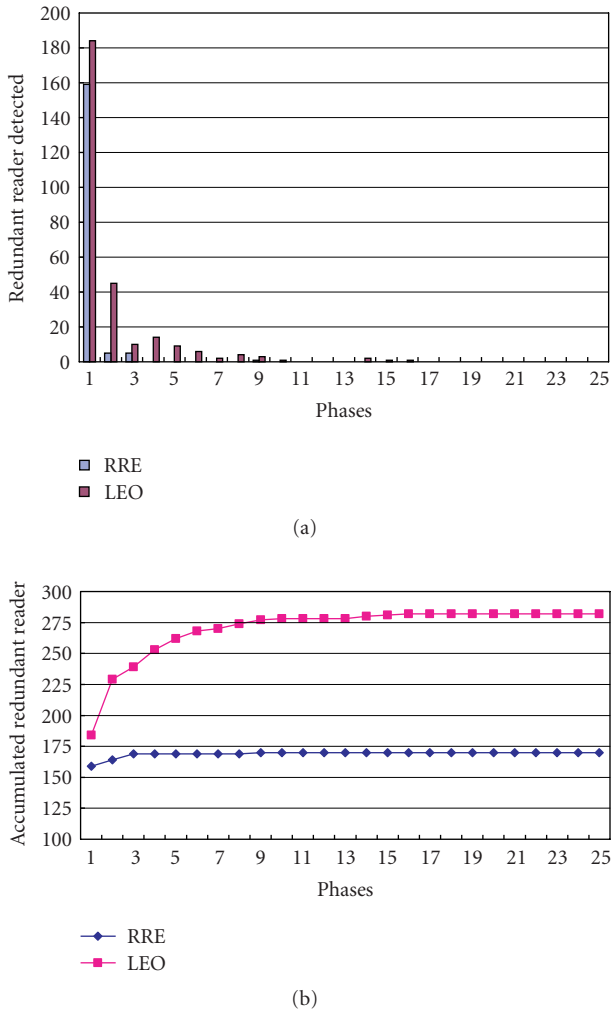


Figure 12: Comparison of number of redundant readers detected (a) and accumulated (b) with network area 10000 × 10000, reader radius = 500, number of tags = 4000, reader = 500.

eventually detected by *LEO* in late phases. From Figure 12(b), the accumulated values of both schemes are reported. Obviously, the *LEO* presents significant optimization results than the RRE scheme.

6. CONCLUSIONS

In this paper, we have presented a distributed optimization technique, *LEO*, for optimizing redundant reader detection problem in wireless RFID network. *LEO* is an algorithm-independent optimization technique which is applicable in arbitrary RFID network topology. A significant improvement of the *LEO* scheme is that the amount of write-to-tag operations could be largely reduced in the redundant reader identification phase. To evaluate the performance of the proposed technique, we have compared the *LEO* method along with the redundant reader elimination scheme as well as other composite methods. The experimental results show that the *LEO* provides superior performance in terms of larger amount of redundant reader detected and lower algorithm overheads. The *LEO* scheme is also verified effective under high density wireless RFID reader network.

ACKNOWLEDGMENT

The work of this paper is supported by National Science Council, Taiwan, under Grant no. NSC96-2218-E-007-007.

REFERENCES

[1] D. Tian and N. D. Georganas, "A coverage-preserving node scheduling scheme for large wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, pp. 32–41, Atlanta, Ga, USA, September 2002.

[2] B. Cărbunar, M. K. Ramanathant, M. Koyutürk, C. Hoffmannt, and A. Grama, "Redundant reader elimination in RFID systems," in *Proceedings of the 2nd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON '05)*, pp. 176–184, Santa Clara, Calif, USA, September 2005.

[3] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pp. 103–111, Washington, DC, USA, October 2003.

[4] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES '02)*, vol. 2523 of *Lecture Notes in Computer Science*, pp. 454–469, Redwood Shores, Calif, USA, August 2002.

[5] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Proceedings of the 1st International Conference on Security in Pervasive Computing*, vol. 2802 of *Lecture Notes in Computer Science*, pp. 201–212, Boppard, Germany, March 2004.

[6] D. W. Engels and S. E. Sarma, "The reader collision problem," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC '02)*, vol. 3, pp. 641–646, Hammamet, Tunisia, October 2002.

[7] S. Slijepcevic and M. Potkonjak, "Power efficient organization of wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '01)*, vol. 2, pp. 472–476, Helsinki, Finland, June 2001.

[8] F. Ye, G. Zhong, J. Cheng, S. Lu, and L. Zhang, "PEAS: a robust energy conserving protocol for long-lived sensor networks," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems (ICDCS '03)*, pp. 28–37, Providence, RI, USA, May 2003.

[9] H. Zhang and J. C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," *Wireless Ad Hoc and Sensor Networks*, vol. 1, no. 1-2, pp. 89–124, 2005.

[10] F. Ye, S.-T. Sheu, T. Chen, and J. Chen, "The impact of RTS threshold on IEEE 802.11 MAC protocol," *Tamkang Journal of Science and Engineering*, vol. 6, no. 1, pp. 57–63, 2003.

[11] J. L. Sobrinho, R. de Haan, and J. M. Brazio, "Why RTS-CTS is not your ideal wireless LAN multiple access protocol," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '05)*, vol. 1, pp. 81–87, New Orleans, La, USA, March 2005.

[12] J. Waldrop, D. W. Engels, and S. E. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem," in *Proceedings of the International Conference on Communications (ICC '03)*, vol. 2, pp. 1206–1210, Anchorage, Alaska, USA, May 2003.

[13] S. M. Birari and S. Iyer, "Mitigating the reader collision problem in RFID networks with mobile readers," in *Proceedings of the 13th IEEE International Conference on Networks jointly held with the 7th IEEE Malaysia International Conference on Communications (ICON '05)*, vol. 1, pp. 463–468, Kuala Lumpur, Malaysia, November 2005.

[14] X. Wang and K. Kar, "Throughput modelling and fairness issues in CSMA/CA based ad-hoc networks," in *Proceedings of the 24th IEEE Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, vol. 1, pp. 23–34, Miami, Fla, USA, March 2005.

[15] J. Kim, S. Kim, D. Kim, W. Lee, and E. Kim, "Low-energy localized clustering: an adaptive cluster radius configuration scheme for topology control in wireless sensor networks," in *Proceedings of the 61st IEEE Vehicular Technology Conference (VTC '05)*, vol. 4, pp. 2546–2550, Stockholm, Sweden, May-June 2005.

[16] J. Ho, D. W. Engels, and S. E. Sarma, "HiQ: a hierarchical Q-learning algorithm to solve the reader collision problem," in *Proceedings of the Internalional Symposium on Applications and the Internet Workshops (SAINT '06)*, pp. 88–91, Phoenix, Ariz, USA, January 2006.

[17] J.-R. Cha and J.-H. Kim, "Novel anti-collision algorithms for fast object identification in RFID system," in *Proceedings of the 11th International Conference on Parallel and Distributed Systems Workshops (ICPADS '05)*, vol. 2, pp. 63–67, Fukuoka, Japan, July 2005.

[18] J.-R. Cha and J.-H. Kim, "Dynamic framed slotted ALOHA algorithms using fast tag estimation method for RFID system," in *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (CCNC '06)*, vol. 2, pp. 768–772, Las Vegas, Nev, USA, January 2006.

[19] M. Cardei and J. Wu, "Coverage in wireless sensor networks," in *Handbook of Sensor Networks*, CRC Press, Boca Raton, Fla, USA, 2004.

[20] J. Jiang and W. Dou, "A coverage-preserving density control algorithm for wireless sensor networks," in *Proceedings of the 3rd International Conference on Ad-Hoc, Mobile, and Wireless Networks (AdHoc-NOW '04)*, pp. 42–55, Vancouver, Canada, July 2004.

[21] Y. Tanaka and I. Sasase, "Interference avoidance algorithms for passive RFID systems using contention-based transmit abortion," *IEICE Transactions on Communications*, vol. E90-B, no. 11, pp. 3170–3180, 2007.

[22] J. Carle and D. Simplot-Ryl, "Energy efficient area monitoring for sensor networks," *Computer*, vol. 37, no. 2, pp. 40–46, 2004.

[23] B. Cărbunar, A. Grama, J. Vitek, and O. Cărbunar, "Redundancy and coverage detection in sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 1, pp. 94–128, 2006.