RFIDサプライチェーンにおいて必要な ダミータグ数を低減する安全な鍵配送方式

研究背景

・サプライチェーンはRFIDにより効率化され在庫管理等が容易に

・RFIDの長い通信距離が悪用され配送中に情報が抜き取られる恐れ
→偽造につながるため対策が必要

・RFIDタグにアクセス制限をかけその鍵を安全に配送する方式が検討されてきた

従来研究[1]

・Shamirの秘密分散[2]を用いて鍵をshareに分けタグに書き込み（shareを一定個数以上入手した受取側は鍵を復元可能）

→ダミータグには偽のshareを書き込み(このshareを含むと鍵は復元不可能)

→ダミータグの区別がつかない攻撃者は鍵の復元が困難

図1 従来方式の例

[1] K. Toyoda and I. Sasase, in IEEE International Conference on RFID, 2015.
[2] A. Shamir, Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

提案方式

・商品数が少ない場合必要なダミータグ数が膨大になることに着目

→商品数が一定以下の時追加の商品タグを用意し正規のshareを割当

→見かけ上の商品数が増加することでダミータグ数が低減

図2 提案方式の例

特性評価

・商品数に応じた用意するタグ数（ダミータグ+追加の商品タグ）を評価

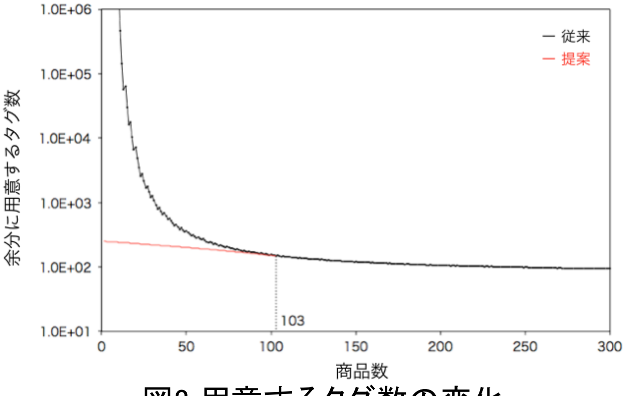


図3 用意するタグ数の変化

・商品数103未満の時に提案方式が適用され商品数10の時90%以上低減

業績 Tatsuaki Sato, Kentaroh Toyoda and Iwao Sasase, "Practical Key Distribution Scheme with Less Dummy Tags in RFID-enabled Supply Chains," The 22nd Asia-Pacific Conference on Communications (APCC 2016), Yogjakarta, Indonesia, August 25-27, 2016.

お問合せ先 sato@sasase.ics.keio.ac.jp

Relocation of Mobile Sensor Nodes with Battery Aware Threshold Distance Algorithm in Wireless Sensor Networks

This paper has been published and received as the best paper award in Regional Conference on Computer and Information Engineering (RCCIE) 2016, October 2016, Yangon Myanmar.

Abstract

Energy efficient relocation method of mobile sensor nodes is presented to improve the network lifetime and sensing coverage holes by using the threshold distance and the residual energy calculation.

System Model

Location aware static and mobile sensors are randomly deployed in the initialization step. We assume that there is no disturbance in the movement of mobile sensor nodes. The wireless sensor network (WSN) area is divided by multiple square grids known to the control station. The variable transmission power is used to communicate with the control station.

Conventional Method

The sensor relocation method by the direct movement approach[1] is presented. This method moves the most redundant sensor directly to the target coverage hole area. However, moving a sensor may create new holes in the left place. To heal this new hole, more sensors are necessary to be moved. Moving the mobile sensor node directly to the destination is a probable answer. However, it may take longer time to complete the coverage healing process in the WSN, since many sensors are sequentially involved in the relocation process. Therefore, coverage hole healing algorithm should provide not only the total distance movements but also the faster relocation time with reduced complexity in the WSN. The scheme in [1] is not energy and time efficient because of the longer distance and time-consuming relocation process in WSNs. In [2], an optimal relocation algorithm for WSN nodes is presented by using genetic method. This method finds the minimum travelled distance for each mobile sensor node. After finding the target position for each mobile node, all mobile sensor nodes will move to the desired position by using shortest distance to achieve the maximum coverage in the WSN. One main issue of this algorithm is that it requires large amount of computation to achieve the minimum travelled distance for each mobile node.

Proposed Method

The best positions for each mobile nodes are calculated. The best position is the grid with the highest weight value to avoid the overlap placement of sensor nodes for maximum sensing coverage.

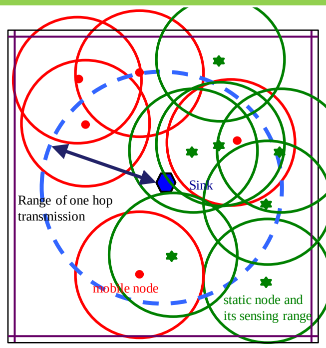


Fig. 1. The layout of WSN with randomly deployed.

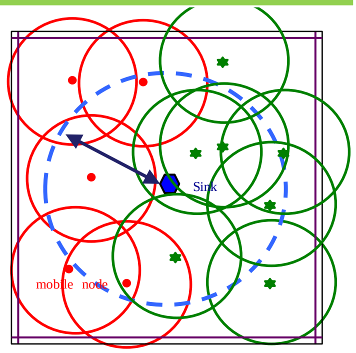


Fig. 2. The optimal new positions relocated by mobile sensor nodes.

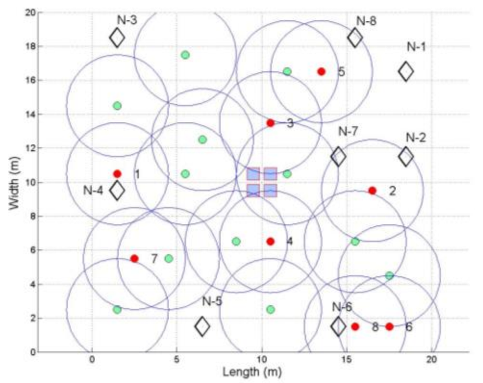


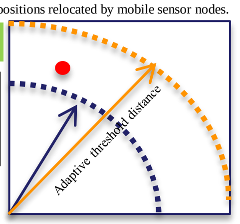
Fig 3. Layout of the sensor network with the optimal new position deployment.

Adaptive threshold distance is used in the relocation process of mobile sensor nodes.

Maximum handling nodes=2; Number of remaining nodes > maximum handling nodes

For 3 mobile nodes case, Permutation of 3 mobile nodes 3! = 6

Few remaining mobile nodes => Few permutation => Less complexity



N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	
×	2	×	1	×	8	3	5	remaining mobile nodes-4,6,7
N-1	N-2	N-3	N-4	N-5	N-6	N-7	N-8	
5	2	×	1	7	8	3	×	remaining mobile nodes-4,6

Energy Consumption
Movement>> Communication>> Sensing
Therefore: Emphasize on movement

Reference:
[1]. G. Wang, G. Cao, T. La Porta, and W. Zhang, "A Bidding Protocol for Deploying Mobile Sensors", IEEE Conference on Network Protocols ICNP, pp. 315-324, November 2003.
[2]. Y. Qu and S. V.Geogakopoulos, "Relocation of Wireless Sensor Network Nodes Using a Genetic Algorithm", IEEE Wireless and Microwave Technology Conference (WAMICON), April 2011.

Simulation Results

Table1. Simulation Parameters

WSN area (width X length)	20m X 20m	100m X 100m
Number of static sensor nodes	16	500
Number of mobile sensor nodes	8	100
Maximum handling nodes M_{max}	2 and 8	2 and 8
Starting threshold distance D_{thr}	4.5m	4.5m
Energy consumption of mobile node	27.96J/m	27.96J/m
Sensing radius	3m	3m

Table.2 . Comparison of calculation time for relocation of hole healing case for each method.

Calculation time for each method (seconds)	(%) Percentage of hole area w.r.t WSN area							
	2.1%	4.2%	6.4%	8.9%	11.6%	14.5%	17.5%	20%
Method in [16]	0.0015	0.0021	0.0024	0.0027	0.001	0.003	0.003	0.003
Method in [17]	1.9534	2.0096	2.0097	2.0099	2.011	2.015	2.017	2.017
Proposed M_{max} =8	0.00142	0.00144	0.00159	0.0016	0.0017	0.00176	0.00189	0.0019
Proposed M_{max} =2	0.00133	0.00135	0.00138	0.0015	0.0016	0.00166	0.0017	0.00178

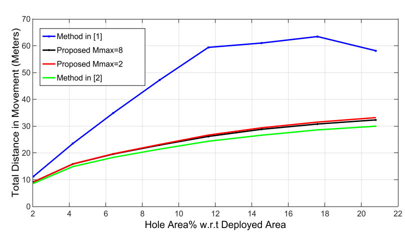


Fig.4 Comparison of total distance movement in 400 sq-meters area.

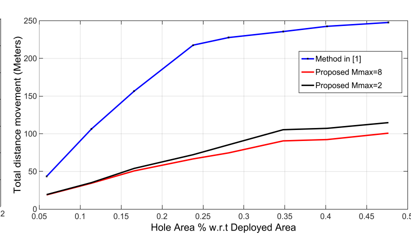


Fig.5 Comparison of total distance movement in 10000 sq-meters area.

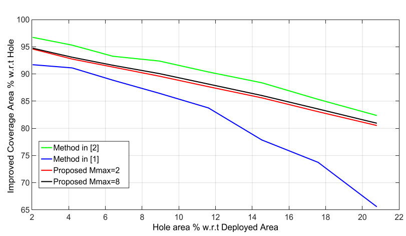


Fig.6 Comparison of coverage improvement in 400 sq-meters area.

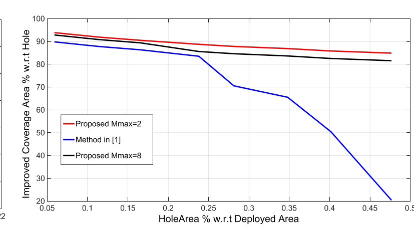


Fig.7 Comparison of coverage improvement in 10000 sq-meters area.

研究者名 **Aye Mon Htun, Maung Sann Maw and Iwao Sasase**
Department of Information and Computer Science, Keio University

お問合せ先 ayemon@sasase.ics.keio.ac.jp, sannmaw@ieee.org, sasase@ics.keio.ac.jp