International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Enhancing Throughput using Coverage Protocol and Secure Data Assemblage in Wireless Sensor Networks

Kantharaju .H.C[#1], Dr. K.N. Narasimha Murthy[#2], Dr. M. Ramakrishna[#3]
[#1]*Assistant Professor, Department of CSE, Vemana Institute of Technology, Bengaluru, KA, India*
[#2]*Professor, Faculty of Engineering, Christ University, Bengaluru, KA, India*
[#1]*Professor, Department of CSE, Vemana Institute of Technology, Bengaluru, KA, India*

Abstract *- Power consumption is one of the fundamental concerns in wireless sensor networks. In this case, some protocols are needed to schedule activation and deactivation of nodes while keeping the coverage and connectivity quality. The protocols maintaining the area covered are often referred to as coverage protocols while connectivity protocols guarantee the communication quality between nodes. Many previous works use unrealistic assumptions on sensing capacities and wireless communications in designing coverage and connectivity protocols. Therefore, considering most of the existing techniques where energy optimization and security are provided in separate protocols, we design a new protocol with novel security provision with data assemblage for the communicating data along with the energy optimization. Energy conservation has to be achieved by managing the WSNs using hierarchical topology. Each cluster head node needs to predict the energy expenditure for the next cluster operation of the cluster. In this paper, we use probabilistic models to develop coverage and connectivity protocols and we propose a more realistic measure of connectivity.*

Keywords *- Wireless Sensor Network, Secure Energy Optimization, Data Integrity Assurance, CWA Mechanism Secure Data Assemblage.*

I. INTRODUCTION

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it is a challenge to provide security in WSNs. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries [1]. To provide secure communications for the WSNs, all messages have to be encrypted and authenticated. Security attacks on information flow can be widespread. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. An opponent can use natural impairments to modify information and also render the information unavailable. Security requirements in WSNs are similar to those of wireless ad hoc networks due to their similarities. WSNs have the general security requirements of availability, integrity, authentication, confidentiality and non-repudiation. These security requirements can be provided by distribution mechanism with the requirements of scalability, efficiency key connectivity and resilience. Scalability is the ability to support large sensor nodes in the networks. Key distribution mechanism must support large network, and must be flexible against substantial increase in the size of the network even after deployment. Efficiency is the consideration of storage processing and communications limitations on sensor nodes. Key connectivity is the probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a WSN to perform its intended functionality.

II. LITERATURE SURVEY

H. Zhang et al. [2] have presented the sensing range is assumed to be a uniform disk of radius r_s. The disk sensing model assumes that if an event happens at a distance less than or equal to r_s from the sensor location, the sensor will deterministically detect this event. On the other hand, an event occurring at a distance $r_s + ^2$ ($^2 > 0$) cannot be detected at all, even for very small ^{2} values. In this case, the area is covered if any arbitrary point in the area has a sensor within the range of r_s. The disk sensing model is appealing, because it makes coverage maintenance protocols, less complicated to design and analyze. It also makes analytical and asymptotic analysis, tractable. However, it is unlikely that ncing signals drop abruptly from high, full-strength values to zero, as the disk model assumes. This implies that there might be a chance to detect an event occurring at distances greater than r_s. By ignoring this extra sensing capacity, the fully utilize the sensing capacity of sensors, which may lead to: (i) deploying more sensors than needed and thus incurring higher cost, (ii) activating redundant sensors which increases interference and wastes energy, and ultimately (iii) decreasing the lifetime of the sensor network.

Y. Zou et al. [3] have presented Probabilistic sensing models capture the behavior of sensors more realistically than the deterministic disk model. For example, through experimental study of passive infrared (PIR) sensors, the authors of show that the sensing range is better modeled by a continuous probability distribution, which is a normal distribution in the case of PIR sensors. The authors of use an exponential sensing model, where the sensing capacity degrades according to an exponential distribution after a certain threshold, Whereas the authors of propose a polynomial function to model the probabilistic nature of the sensing range Furthermore, the authors of assume sensing range can be modeled as layers of concentric disks with increasing diameters, and each layer has a fixed probability of sensing. A probabilistic sensing model is more realistic because the phenomenon being sensed, sensor design, and environmental conditions are all stochastic in nature. For instance, noise and interference in the environment can be modeled by stochastic processes. Sensors manufactured by the same factory are not deterministically identical in their behavior rather, sensor characteristics are usually modeled using statistical distributions.

M. Hefeeda et al. [4] have presented the k-coverage problem in wireless sensor networks, and provide an overview of our solution. Our problem is to select a minimal subset of nodes for activation to ensure that all sensor locations are k-covered by the set of activated nodes. The k-coverage Problem can formally be stated as follows. Problem 1 (k-Coverage Problem) Given n already-deployed sensors in a target area, and a desired coverage degree $k \geq 1$, select a minimal subset of sensors to cover all sensor locations such that every location is within the sensing range of at least k different sensors. It is assumed that the sensing range of each sensor is a disk with radius r, and sensor deployment can follow any distribution. The above k-coverage problem is proved to be NP-hard by reduction from the minimum dominating set. The proof idea is to model the network as a graph where there is an edge between any two nodes if they are within the sensing range of each other. M. Hefeeda et al. [5] have proposed a probabilistic coverage protocol (denoted by PCP) that considers probabilistic sensing models. We design PCP keeping in mind that no single sensing or communication model (probabilistic or not) will accurately model all types of sensors in all environments. It is expected that different sensor types will require different sensing and communication models. Even for the same sensor type, these models may need to be changed in different environments or when the technology changes. Designing, implementing, and testing a different coverage protocol for each model is indeed an extremely costly process, if at all possible. To address this challenging task, we design our protocol with limited dependence on the sensing and communication models. In particular, our protocol requires the computation of a single parameter from the adopted models, while everything else remains the same. Camtepe et al. [6] have presented a novel deterministic and hybrid approaches based on Combinatorial Design for deciding how many and which keys to assign to each key-chain before the sensor network deployment. Ren et al. [7] have presented a multifunctional key management framework assures both node-to-sink and node-to-node authentication along the report forwarding routes. The authors have came up with a location-aware end-to-end security framework in which secret keys are bound to geographic locations and each node stores a few keys based on its own location. Le et al. [8] have presented an energy efficient access control scheme based on Elliptic Curve Cryptography (ECC) to overcome these problems and more importantly to provide dominant energy efficiency. Maarouf et al. [9] have proposed a reputation system based solution for trust-aware routing, which implements a new monitoring strategy called an efficient monitoring procedure in a reputation system which is a probabilistic and distributed monitoring methodology that tries to reduce the monitoring activities per node while maintaining the ability to detect attacks at a satisfactory level. Yu et al. [10] have presented Constrained Random Perturbation-based pairwise key establishment (CARPY) scheme and its variant, a CARPY+ scheme, for WSNs. It is the first non-interactive key establishment scheme with great resilience to a large number of node compromises designed for WSNs.

Gu et al. [11] have designed an end to end secure communication protocol in randomly deployed WSNs. Specifically, the protocol is based on a methodology called differentiated key pre-distribution. He et al. [12] have proposed a distributed and DoS-resistant code dissemination protocol named DiCode. The work has also reported the evaluation results of DiCode in a network of resource limited sensor nodes, which shows the efficiency of the protocol in practice. Jokhio et al. [13] have proposed the novel Sensor node Capture Attack Detection and Defence (SCADD) protocol that provides a cost effective solution against the node compromise and capture attacks in WSNs, enhancing the overall WSN security for security sensitive applications. Alomair et al. [14] have provided a statistical framework based on binary hypothesis testing for modeling, analyzing, and evaluating statistical source anonymity in wireless sensor networks. The authors have introduced the notion of interval indistinguishability to model source location privacy.

III.EXISTING SYSTEM

- Probabilistic Coverage Protocol (CCANS) is implemented in terms of the number of activated sensors, network lifetime and energy consumption.
- Deterministic Coverage Protocols such as (OGDC, CCP) are implemented for maintaining the connectivity.

A. CCANS AND OGDC, CCP

The probabilistic coverage protocol (CCANS), proposed in terms of the number of activated sensors, network lifetime, and energy consumption. The idea of CCANS is to start all nodes in active mode, then iteratively deactivate nodes that are not needed for coverage. A token is circulated among nodes in the network in a certain manner. The node holding the token calculates the coverage on the grid points around it. If coverage is achieved at these points, it broadcasts a notification to its neighbors, passes the token to another node, and deactivates itself.

All redundant nodes are deactivated when the token visits each node in the network. We make CCANS check only for coverage and not for connectivity. Several distributed coverage protocols have been pro-posed for the disk model, including For example, OGDC tries to minimize the overlap between the sensing circles of activated sensors, while CCP deactivates redundant sensors by checking that all intersection points of sensing circles are covered. CCP can provide coverage with degrees higher than 1 as well. Sensors in PEAS probe their neighbors to decide whether to be in active or sleep mode. The coverage algorithms solve a variation of the set k-cover problem, where sensors are partitioned into k covers and individual covers are iteratively activated to achieve 1-coverage of the monitored area. The authors propose three node scheduling schemes that estimate the distance to the nearest neighbor, number of neighbors, or the probability of a node being off duty and use one of these metrics to put some sensors in sleep mode. The coverage algorithm tries to find uncovered spots and activate sensors in these areas using information from nearby active sensors.

B. DIFFICULTIES IN EXISTING SYSTEM

In sensor network applications are ensuring area coverage and maintaining the connectivity of the network. Selecting the minimum number of sensors to activate to achieve coverage as NP hard problem

- ✓ Random node failure
- ✓ Imperfect time synchronization
- ✓ Location in accuracy

IV. PROPOSED SYSTEM

Probabilistic coverage protocol [4] works with the common disk sensing model as well as probabilistic sensing models with minimum changes. One model does not fit all sensor types Pcp is designed with limited dependence on sensing model can be used with various sensor types. We consider the more general k-coverage ($k \geq 1$) problem where each point should be within the sensing range of k or more sensors. Covering each point by multiple sensors is desired for many applications, because it provides redundancy fault tolerance-coverage is necessary for the proper functioning of other applications, such as intrusion detection, data gathering, and object tracking. To illustrate, consider an intrusion detection system in military applications, where k-coverage is essential to identify intruding objects of different sizes. A tank, for instance, is detected by many sensors, while a soldier is detected by only a few. A high degree of coverage makes the classification more precise.

A. SYSTEM ARCHITECTURE

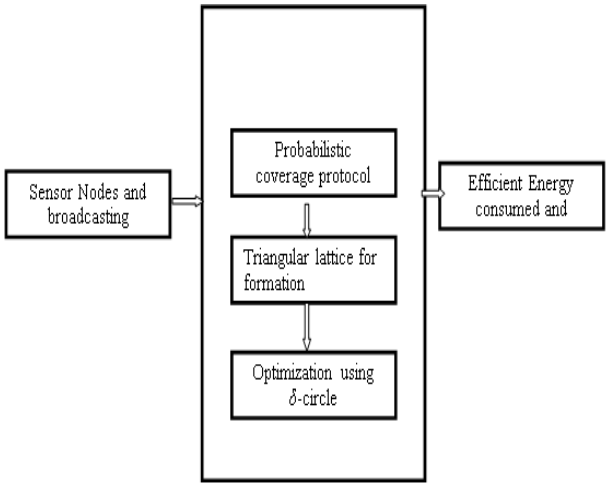

Fig. 4.1. System Architecture

The probabilistic coverage protocol (CCANS), proposed in terms of the number of activated sensors, network lifetime, and energy consumption. The idea of CCANS is to start all nodes in active mode, then iteratively deactivate nodes that are not needed for coverage. A token is circulated among nodes in the network in a certain manner. The node holding the token calculates the coverage on the grid points around it. If coverage is achieved at these points, it broadcasts a notification to its neighbors, passes the token to another node, and deactivates itself. All redundant nodes are deactivated when the token visits each node in the network. We make CCANS check only for coverage and not for connectivity.

B. DISTRIBUTED K-COVERAGE ALGORITHM (DRKC)

We propose approximation algorithm for Probabilistic Coverage Protocol is distributed Randomized K-Coverage (DRKC)

DRKC Sender

```
1. while (true) {
2. /* initialize parameters */
3. weight = 1, totalWeight = n, netSize = 1;
4. curCoverage = 0, state = TEMP;
```


5. while (netSize ≤ n) {
6. / activate neighbors to achieve k coverage */*
7. if (netSize × (weight/totalWeight) > rand()) {
8. state = ACTIVE;
9. reqCoverage = k − curCoverage;
10. Pa = reqCoverage/(neighborSize − curCoverage);
11. broadcast an ACTIVATE message containing Pa and reqCoverage to neighbors;
}
13. wait for NOTIFY messages;
14. / verify k-Coverage */*
15. if (curCoverage ≥ k) { break; }
16. / update variables for next iteration */*
17. if (1/(n − netSize) > rand()) { weight = weight × 2; }
18. netSize = netSize × 2;
19. totalWeight = totalWeight + totalWeight/n;
20. }
21. if (state 6= ACTIVE) { state = SLEEP; }
22. wait until end of round;
23.}

DRKC Receiver
/* upon receiving a message msg */

1. if (msg.type == ACTIVATE and msg.Pa > rand()) } / chosen to be active */*
2. / wait random time to reduce collision */*
3. send a NOTIFY message to msg.source after int rand(0, msg.reqCoverage) × Tm sec;
4. state = ACTIVE;
5. }
6. update (neighborSize, curCoverage); / based on msg.source */*

V. EXPERIMENTAL RESULTS & DISCUSSION

We have implemented our PCP protocol in NS-2 and in our own packet-level simulator in C++.]. Some results from the NS-2 implementation with reasonable network sizes (up to 1,000 nodes) are presented. Most results, however, are based on our own simulator because it supports much larger networks, which we need to rigorously evaluate our protocol. We use the following parameters in the experiments, unless otherwise specified. We uniformly at random deploy 20,000 sensors over a 1 km $_3$ 1 km area. We use two sensing models: The disk sensing model with a sensing range of r_s ¼ 15 m and the exponential sensing model with sensing capacity decay factor $_3$ ¼ 0:05, and we set r_s ¼ 15 m as the threshold value below which sensing is achieved with probability 1. We employ the energy model in which is based on the Mote hardware specifications. In this model, the node power consumption in transmission, reception, idle, and sleep modes is 60, 12, 12, and 0.03 mW, respectively. The initial energy of a node is assumed to be 60 Joules, which allows a node to operate for about 5,000 seconds in reception/idle modes. When we compare various coverage protocols, we assume that the wireless communication channel has a bandwidth of 40 Kbps. Since the message sizes in all protocols are almost the same, we assume that the average message size is 34 bytes, which is the same size used in [4]. We ignore the propagation delay because it is negligible for the 1 km $_3$ 1 km area considered in the simulation. This results is a message transmission time $_{3m}$ ¼ 6:8 ms. We repeat each experiment 10 times with different seeds and report the averages in all of our results. We also report the minimum and maximum values if they do not clutter the figures.

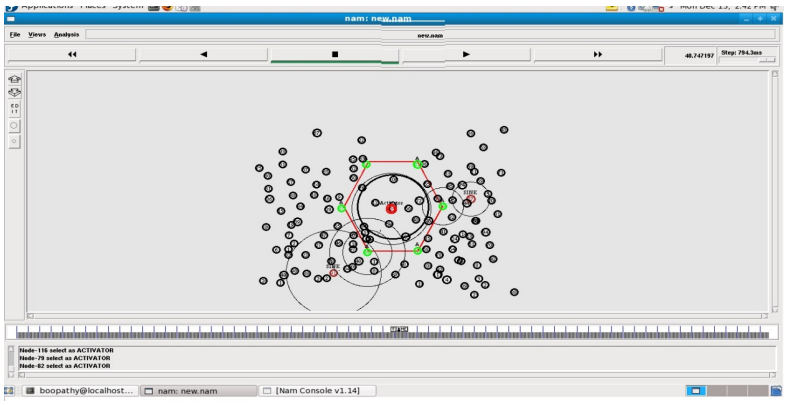

Fig 5.1 nodes activation process in PCP. Activated

Note that the simulated sensor network in each experiment replica has 20,000 nodes, and the measured statistics are collected from all of them. Therefore, we believe that combining the data from 10 different replicas and each with 20,000 nodes yields statistically significant results (we did not see large variances in our results). Finally, we mention that in most experiments, each single replica took several hours of running time on a decent multicore Linux server. Furthermore, processing the huge traces created in these large-scale experiments consumed many CPU hours. Nodes try to form a triangular lattice over the area. The above figure shows that PCP is to activate a subset of deployed sensors to construct an approximate triangular lattice on top of the area to be covered. PCP starts by activating any sensor in the area, which we refer to as an activator. This sensor activates six other sensors located at vertices of the hexagon centered at that sensor. Each activated sensor, in turn, activates other sensors at vertices of its own hexagon.

Fig 5.2 Energy Consumption

The figure shows that as SMAC activates more nodes and exchanges more messages than PCP, we show that our protocol distributes the load uniformly across all deployed nodes. This is critical in order to keep nodes alive for the longest possible period, and thus to prolong the network lifetime and achieve more reliable coverage.

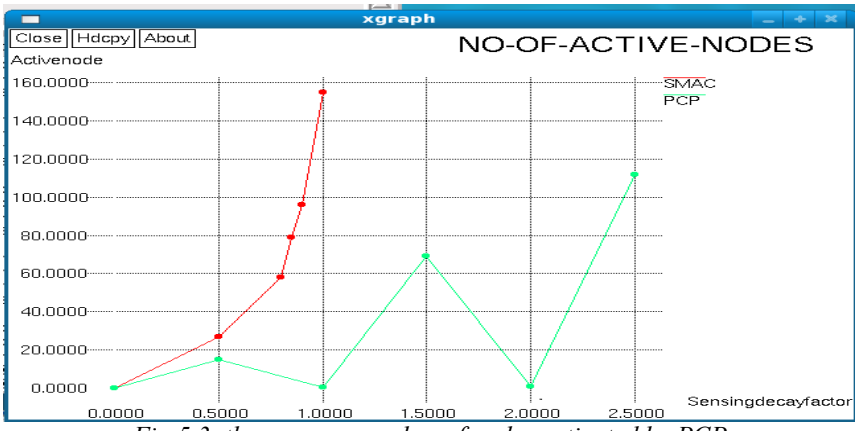

Fig 5.3. the average number of nodes activated by PCP

We plot in the average number of nodes activated by PCP and different values of the sensing decay factor and the coverage threshold. As the figure shows, PCP activates a much smaller number of nodes, while ensuring the same level of probabilistic coverage. This is significant because it indicates that the sensor network could last much longer using our protocol.

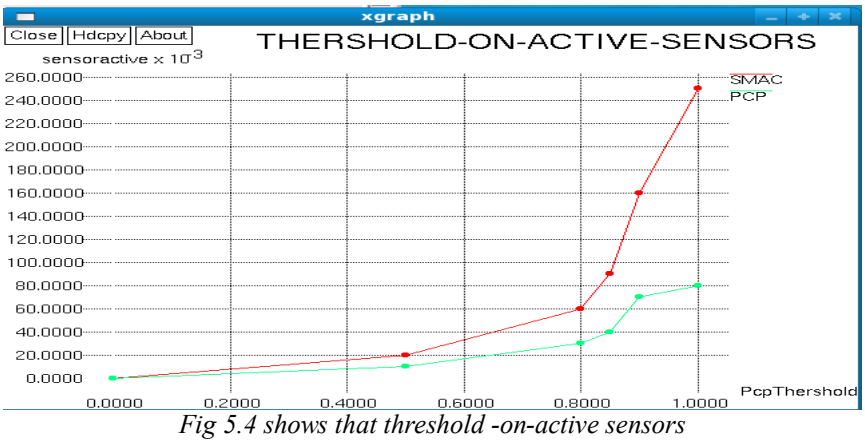

Fig 5.4 shows that threshold -on-active sensors

We conduct an experiment to assess the potential savings in number of active nodes fig shows the results for different values for the sensing decay factor. The fig indicates that saving of up to 30 percent in number of active nodes can be achieved, which means less energy consumed and ultimately longer lifetime for the sensor network.

VI. CONCLUSION

In this paper, a fully distributed, probabilistic coverage protocol has been proposed. A key feature of our protocol is that it can be used with different sensing models, with minimal changes. The protocol has been analysed and showed that it converges fast and has a small message complexity. The analytical results are verified using simulations. The k-coverage problem is modelled as a set system for which an optimal hitting set corresponds to an optimal solution for k-coverage. An approximation algorithm has been proposed for computing near-optimal hitting sets efficiently. Simulation results show that the distributed algorithm converges faster and consumes much less energy than previous algorithms. The analysis and design of the coverage protocol can be extended to the probabilistic k-coverage case. K-coverage is needed in several sensor network applications to enhance reliability and accuracy of the network. Using probabilistic sensing models in the k-coverage case is expected to yield even higher savings in the number of activated sensors. Another extension is to consider probabilistic communication models, in addition to the probabilistic sensing models, in the design and operation of the protocol. The simulation demonstrates that PCP is robust, and it can function correctly in presence of random node failures, inaccuracies in node locations, and imperfect time synchronization of nodes.

REFERENCES

[1]. Z. J. Haas, L. Yang, M-L. Liu, Q. Li, and F. Li, "Current Challenges and Approaches in Securing Communications for Sensors and Actuators," Chapter 17 in "The Art of Wireless Sensor Networks," H.M. Ammari (ed.), Springer-Verlag Berlin Heidelberg, 2014, DOI: 10.1007/978-3-642-40009-7_17.
[2]. H. Zhang and J. Hou. Maintaining sensing coverage and connectivity in large sensor networks. Ad Hoc and Sensor Wireless Networks: An International Journal, 1(1-2):89{123, January 2005
[3]. Y. Zou and K. Chakrabarty. A distributed coverage- and connectivity centric technique for selecting active nodes in wireless sensor networks. IEEE Transactions on Computers, 54(8):978{991, August 2005
[4]. M. Hefeeda and M. Bagheri, "Randomized K-Coverage Algorithms for Dense Sensor Networks," Proc. IEEE INFOCOM,pp. 2376-2380, May 2007
[5]. M. Hefeeda and H. Ahmadi. Network connectivity under probabilistic communication models in sensor networks. In Proc. of IEEE International Conference on Mobile Ad-hocand Sensor Systems (MASS'07), Pisa, Italy, October 2007
[6]. Camtepe, S.A., Yener, B., "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 15, No. 2, April 2007.
[7]. Ren, K., Lou, W., Zhang, Y., "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 7, No. 5, May 2008.
[8]. Le, X.H., Lee, S, Butun, I., "An Energy-Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography", Journal of Communications and Networks, Vol. 11, No. 6, December 2009.
[9]. Maarouf, I., Baroudi, U., Naseer, A.R., "Efficient monitoring approach for reputation system based trust-aware routing in wireless sensor networks", IET Communications, 2008, Vol. 3, Iss.5, pp.846-858, October 2008.
[10]. Yu, C.M., Lu, C.S., Kuo, S.Y., "Non-interactive Pairwise Key Establishment for Sensor Networks, IEEE Transactions on Information Forensics and Security", Vol. 5, No. 3, September 2010.
[11]. Gu, W, Dutta, N., Chellappan, S., Bai, X., "Providing End-to-End Secure Communications in Wireless Sensor Networks, IEEE Transactions on Network and Service Management", Vol. 8, No. 3, September 2011.
[12]. He, D., Chen, C., Chan, S., Bu, J., "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 11, No. 5, May 2012.
[13]. Jokhio, S.H., Jokhio, I.A., Kemp, A.H., "Node capture attack detection and defence in wireless sensor networks", IET Wireless Sensor Systems, 2011.
[14]. Alomair, B., Clark, A., Cuellar, J., Poovendran, R., "Toward a Statistical Framework for Source Anonymity in Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013.

