Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2013) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

2013 International Workshop on Communications and Sensor Networks (ComSense-2013)

A trust-based probabilistic coverage algorithm for wireless sensor networks

Zahra Taghikhaki*, Nirvana Meratnia, Paul J.M. Havinga

Pervasive Systems Group, University of Twente, Enschede, Netherlands

Abstract

Sensing coverage is a fundamental issue for many applications in wireless sensor networks. Due to sensors resource limitations, inherent uncertainties associated with their measurements, and the harsh and dynamic environment in which they are deployed, having a QoS-aware coverage scheme is a must. In this paper, we propose a Trust-based Probabilistic Coverage algorithm, which leverages the trust concept to tackle the uncertainties introduced by the nodes and the environment, in which they operate. We formulate this problem as an Integer Linear Programming (ILP) problem, which is able to always guarantee the required QoS despite uncertainties introduced by node and/or environment. In consideration of the limitation of ILP, we also put forward a greedy heuristic algorithm to achieve almost the same ILP results without suffering from complexities imposed by ILP. We examine our heuristic with different input parameters and compare it with the ILP approach. Simulation results are presented to verify our approaches.

Keywords: Coverage; Wireless Sensor Networks; Probabilistic; Optimization; Reliable; Trust.

1. Introduction

Wireless sensor networks (WSN) have attracted much attention in recent years due to their potential use in a wide range of applications. As energy is the most challenging issues in WSNs, various techniques have been utilized over years by WSNs to minimize energy consumption. These techniques range from (i) scheduling the sensor nodes to alternate between active and sleep mode, (ii) adjusting the transmission/sensing range of the sensor nodes, (iii) designing energy-efficient networking and processing protocols. Due to the fact that communication has the highest share in energy consumption, as pointed out in [1] the best method to save more energy is to turn off as many sensor nodes as possible and for as long as possible while the system still functions well. There has been a growing interest in studying large scale WSNs, in which a large number of sensor nodes are densely (high up to 20 nodes/m3 [2][3]) deployed in an area. One of the challenging issues in such networks is determining a schedule based on which sensor nodes must be kept active to efficiently cover the entire monitoring area. By efficiently coverage we mean ensuring long system lifetime as well as maintaining sufficient sensing coverage and reliability. In case of having dense deployment, it is quite possible that more than one node is able to cover a critical region. This can, in turn, lead to higher data accuracy and system reliability. In this case, finding a way to rotate the role of active nodes among all nodes without sacrificing system reliability can result in more energy conservation.

The aforementioned issues put forward coverage problem which is a fundamental concern in WSNs. The coverage problem usually aims to prolong network lifetime by distributing sensor nodes into a number of sets so that each

* Corresponding author. Tel.: +31- 53- 489- 4117

E-mail address: z.taghikhaki@utwente.nl

sensor node is in the sensing range of at least one of the set members. By doing so, mutually exclusive sets of sensor nodes are activated in sequence. This will bring about less spatial density for the active nodes compared with when all nodes are active. As a consequence of having a fewer nodes active in each time slot, interferences at the MAC layer will be reduced, which in turn leads to prolonging network lifetime. Coverage can also be considered as a QoS parameter for WSNs to show how well a network can monitor the critical regions [4].

The problem of guarantying the coverage while meeting application requirements is usually formulated as a combinatorial optimization problem usually solved using Integer Linear Programming (ILP) [5][6]. There are many studies on coverage problem, which aim to prolong network lifetime while fulfilling the requested mission. The main concern addressed in those studies is energy conservation. Therefore, less attention has been paid so far to the QoS support within these algorithms. Since sensor nodes are usually inexpensive hardware components, they are highly vulnerable and may malfunction or fail. Non-malicious behavior- such as the malfunctioning of radios/sensors or even imperfect environments- can result in generation of false data which could have detrimental effects on the overall performance of the network.

In this paper, we address the coverage problem to maximize the network lifetime of a WSN deployed to continuously monitor the critical regions without sacrificing system reliability. One should note that we use the terms reliable and confident interchangeably. The rest of this paper is organized as follows. First we briefly discuss state of the art and problem statement. Then we present the assumption and models used. Thereafter, a detailed description of our approach will be provided, which will be followed by performance evaluation. Finally we draw some conclusions and future works.

2. Related work

Sensor coverage algorithms aim to have each critical or interested region of the deployment area in the sensing range of at least one node. According to the type of field to be monitored, the coverage problem can be formulated as an area coverage [7], in which all points in the deployment area are required to be covered by one or at least k sensor node, or as a target/critical regions [8] coverage, in which each critical region requires to be covered by one or at least k sensor nodes. Coverage problem has also been formulated in other fields, such as Art Gallery Problem (AGP), Ocean coverage, and coverage in robotic systems. The AGP [9] aims to determine the minimum number of guards and their placement, necessary to cover an art gallery interior such that every point is seen by at least one guard. In WSN context, guards are sensor nodes. Many studies in sensing coverage [8][10][11] aim to extend lifetime by distributing sensor nodes into disjoint sets such that every set completely covers all targets. Then, these disjoint sets are activated successively such that at any moment in time only one set is active. As all targets are monitored by every sensor set, the goal of these approaches is to determine a maximum number of disjoint sets, so that the time interval between two activations for any given sensor is longer. Some of existing studies aim at maximizing coverage utilizing mobility of sensors. The work presented in [12] is a computational geometry based approach, [13] [14] are potential field based approaches, and [15] is an incremental deployment scheme. In [16], authors studied the performance of the network with *n* mobile nodes which move randomly over the area. Authors show that node mobility increases capacity of the network. Coverage problem has also been considered in the field of multi-robot exploration. In [13] an incremental deployment algorithm is used in which sensor nodes are deployed one by one in an adaptive fashion. Each new deployment of a sensor is based on the sensed information from sensors deployed earlier. The first sensor is placed randomly. A drawback of this approach is that it is computationally expensive. Coverage models can be binary or probabilistic. In a binary coverage model, a node can monitor a critical region with the highest confidence level if the critical region is located in its sensing range. In a probabilistic coverage model, however, it is possible that a critical region cannot be monitored by a sensor node even if it is located within its sensing range. This is because the coverage model is assumed to be probabilistic. This non-deterministic behavior is introduced by the uncertainties associated with the (i) sensor node such as quality of the sensors, processing unit, sensing algorithm and (ii) environmental parameters such as obstacles, background noise: magnetic field of the earth, weather: temperature, humidity, rainy, windy [17].

3. Our contribution

As shown above, a large number of studies have been done in the literature [3][4][5][6], however, most of them focus on the binary coverage model while we are looking into the probabilistic coverage model, because in reality the detection of a target is not deterministic. Although some studies [17][18] address the probabilistic models, they mostly focus on the distance between sensor node and target as the only parameter which affects sensing quality.

Different from these approaches, we make our probabilistic coverage more general and consider other parameters which may affect sensing quality. Moreover, erroneous data generated by faulty sensor nodes must be protected from being transferred for ensuring effective use of bandwidth and energy utilization. To this end, we leverage trust model in order to quantify the confidence level of each node. Also, given a network where the confidence coefficient of the nodes may change during their lifetimes, discovering all such disjoint sets at the beginning as of [8][10][11] is useless. Therefore, before calculating another feasible set whose node should be activated for the next time interval, we do calculate and consider the confidence level of the nodes. Doing so may bring quite different coverage set than that of other approaches suggest. Finally, although mobility of sensors in [12][13][14][15][16] may increase capacity of the network, however, these protocols have the same assumption that all nodes should be able to re-adjust their positions in the region. Different from these approaches, we consider static sensor nodes that do not have this privileged to move after deployment. More specifically, the main contributions of this paper are:

1. Proposing a trust-based probabilistic scheme for maximizing network lifetime for the coverage problem while taking QoS parameters into account.
2. Proposing a greedy heuristic scheme to achieve the same ILP result without suffering from computational complexity that ILP usually offers to solve large-size instances.

4. Problem statement

We address the critical coverage problem while adhering to the required QoS parameters using trust models. Due to sensors resource limitations, inherent uncertainties associated with their measurements, and the harsh and dynamic environment they are deployed in, having a QoS-aware coverage scheme is a must. Many WSN applications require different observation quality for different regions. The more sensitive the critical areas, the higher the data quality must be. This requires having different number of active nodes in different regions, as more sensitive regions require higher number and density of nodes to provide more redundant and consequently higher quality data.

Given an already deployed WSN, the problem at hand is to define a schedule to activate nodes in such a way that (i) network lifetime is maximized, (ii) each critical region is monitored at least by one node, (iii) quality of data gathered from each critical region should meet a given confidence level. To address this problem, we organize sensor nodes into a number of disjoint feasible sets so that each of them is able to monitor all critical regions with a certain probability. This means that the policy of distributing sensor nodes into these sets should be done in such a way that network lifetime is maximized while the QoS requirements are met. Different from other approaches that define all these sets at the beginning, we opt to find each set whenever the nodes of the current feasible set are about to die. The reason for doing so is because of network dynamicity, which changes during system lifetime. Using fresh information about network state and individual node's lifetime can help defining more robust and efficient feasible set.

5. Assumption and models used

5.1. Assumptions

We make the following assumptions regarding the WSN:

- The WSN consists of n nodes uniformly, randomly and redundantly deployed in a square field. A number of regions in the field are required to be continuously monitored with a certain confidence.
- Sensor nodes should send their measurements to a base station for central processing.
- The coverage of each sensor is modeled as a circle whose center represents the sensor while the radius represents the sensing range of the sensor.
- Sensor nodes have the same initial energy. With no loss of generality, we assume that according to the initial energy each sensor node can be active for one time unit. Therefore, the network lifetime becomes 1 if all nodes are active simultaneously, otherwise the lifetime is represented by the number of *FsbSet* (defined in section 6.2) which could be made. The larger such number, the longer lifetime.
- Sensor nodes can alternate between active/sleep mode according to their appearance in the Coverage Set (CS).
- As connectivity is not a concern of this study, sensor nodes are assumed to talk directly with the neighboring nodes as sensor's communication distance is assumed to be longer than twice of its sensing range.

5.2. Models used

Each sensor node may suffer from node or area imperfections which could affect the quality of information received by the base station. We use a two-state Markov model of node transitions between a "healthy" and "faulty" state in order to model node failure. Apart from node failure, the area or network conditions may introduce some new challenges for quality of data received by the base station. Therefore, it is possible that the sensed data of one node is changed during the packet transmission because of area or channel imperfections. To avoid this situation, selecting active nodes at locations nearby those areas experiencing favorable conditions are more effective. We utilize the Gilbert–Elliott two-state Markov model [19] on the packet level to model dynamic channel conditions which can be affected by the environmental factors. We also assume a probabilistic coverage model where the coverage quality varies exponentially with the distance between a node and a given critical region [17], as shown in Equation 5.

Utilizing these three aforementioned models gives us an insight about the confidence level that each node and the environment around the given node can provide for each critical region.

6. Our protocol

Given an already densely deployed WSN, sensor nodes regularly send their opinions about their neighbors in terms of availability and sensing quality to the base station. Even asleep sensor nodes are required to do so, which implies that they have to wake up, scan their neighborhood, and inform the base station about their opinion. This enables the base station to have a comprehensive view of state, in which all nodes are. Upon receiving this information by the base station, it quantifies the confidence level of each node as will be explained in Section 6.1. Thereafter, base station utilizes either our ILP algorithm or our greedy heuristic scheme to build the Feasible Set (*FsbSet).* Finally, the base station informs sensor nodes belonging to the *FsbSet* to keep themselves ON and to monitor their nearby critical region for the next time interval. We organize the network activities into several rounds. This means that the base station runs our algorithms at intervals of a round time unit. Each round, as shown in Fig 1, starts with a set-up phase followed by a sensing phase. In the set-up phase, the base station has to decide the set of nodes, which should be kept active in the sensing phase. In what follows, we focus on the algorithms the base station uses in the set-up phase.

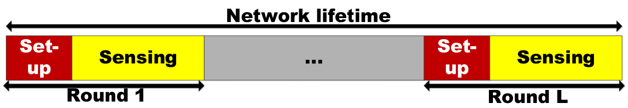

Fig.1. Network activities organization

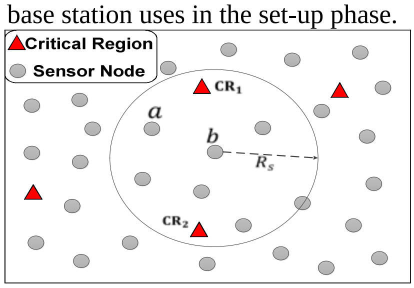

Fig.2. An example of nodes and CR deployment

6.1. Calculating node's confidence level

In this subsection we explain how to calculate the confidence of each node which is required by the base station to judge about a node's appropriateness to act as an active node. In this paper we address three parameters which introduce uncertainty in the sensed values. These three values are 1) the distance between a critical region and a sensor node, 2) the condition of the area in which sensor nodes are deployed, and 3) the reliable state of the sensor node itself (in processing/sensing units).

Usually, sensing ability of a node is directly dependent on the distance between the given node and a critical region. We assume sensor ability decreases if distance from critical regions increases. As the sensor nodes and critical regions are stationary, the first aforementioned parameter is always unchanged for a given pair of node and critical region. We address this parameter using Equation 5. The second and third parameters are not fixed and may change with the physical conditions that network or nodes experience. We assess quality of nodes measurements using functional reputation and trust concepts [23]. Reputation and trust concepts are being recently used in WSNs to diminish the impact of malicious/faulty nodes and links. Having history of the nodes' activities and area/links' states can give useful information about their situations, based on which a proper policy can be made to achieve the desired performance. To evaluate the trust, we select Bayesian formulation and to represent reputation we utilize BETA distribution function of the sensor node's previous actions.

Each sensor node a should act as a referee node. It should calculate the sensing reputation $\rho_{a,b}^{Sensing}$ and availability reputation $\rho_{a,b}^{availability}$ of a given neighbor node b using BETA distribution function, as explained in [20], and send both reputation values for that neighbor b to the base station. All sensor nodes have to wake up in some predefined times and monitor their region to detect the misbehavior of their neighbors and quantify their observation as reputation values of those nodes[21]. It is worth mentioning that the misbehaviors seen from the neighbors could be caused either by those neighbors' misbehavior/failure or by the imperfect/noisy environment nearby those neighbors.

Basically, if a sensor node execute a false active/sleep schedule or does not respond to hello messages or the hello message is not received by the referee node a due to environmental conditions, the reputation value of that node b in terms of availability ($\rho_{a,b}^{availability}$) is decreased. In the other hand, if the measurement of a sensor node significantly differs from its one-hop neighbors, the reputation value of that node in terms of sensing may be reduced. We use the Jaccard similarity as our similarity function. These obtained $\rho_{a,b}^{Sensing}$ and $\rho_{a,b}^{availability}$ should be sent to the base station after a certain period of time denoted by τ. base station is responsible to determine the best active nodes for the next round according to these reputation values. In this way after receiving the information from each sensor node, the base station must obtain a consensus on the neighbors' viewpoint of every node about its observation quality for a given critical region. To this end, base station first employs Equation 1 and Equation 2 to calculate global sensing reputation denoted by $\gamma_{b}^{sensing}$ for a given node b as well as global availability reputation denoted by $\gamma_{b,c}^{availability}$ for a given node b about the critical region c.

$$\gamma_{b,c}^{availability} = \frac{\sum_{a\in Nei(b)} dist(a,c)^{-1} \times \rho_{a,b}^{availability}}{\sum_{a\in Nei(b)} dist(a,c)^{-1}} \quad (1)$$

$$\gamma_{b}^{sensing} = \frac{\sum_{a\in Nei(b)} \rho_{a,b}^{sensing}}{|Nei(b)|} \quad (2)$$

Where $Nei(b)$ denotes the neighbor nodes of b. In calculating $\gamma_{b,c}^{availability}$, the base station considers the reverse distance of $a \in Nei(b)$, to the given CR c as a weight of a's vote about the b's availability for CR c. This implies that closer nodes to a CR could have better insight about that CR and hence, their opinion could be considered with a higher value. Thereafter, BS combines weighted global sensing reputation and weighted global availability reputation to obtain the total reputation $\gamma_{b,c}^{total}$ of node b for CR c as equation 3:

$$\gamma_{b,c}^{total} = \omega_{sn} \times \gamma_{b}^{sensing} + \omega_{av} \times \gamma_{b,c}^{availability} \quad (3)$$

We introduce two weights ω_{sn} and ω_{av} for global sensing reputation and global availability reputation in order to prioritize them if needed. The main reason behind considering the distance factor in calculating $\gamma^{availability}$(Equation 1) is that each sensor node may experience different environmental conditions in different directions. For example in Fig 2, if $dist(b, CR_1) = dist(b, CR_2)$, it is still likely that the quality of observing these two CRs by b would be different. This difference is caused by the different situations experienced by b in these two directions.

Base station can obtain more consistent local view about b using the information provided by the b's two-hops neighbors, through b's one-hop neighbors who have already explored their one-hop neighbors as well. By doing so in the K^{th} effort, the base station can utilize the information of the k hops neighborhood of b to make system more robust against false ratings.

6.2. Integer linear programming

In this section we formulate maximizing network lifetime for the coverage problem while guaranteeing quality and reliability requirements for each critical region as an Integer Linear Programming. First we define a Feasible Set (*FsbSet*), which is a set of sensor nodes selected in such a way that critical regions are covered at least by one of the nodes of such set. An appropriate or minimal *FsbSet* is denoted by a decision binary vector *x*, where Sn_j is included in the set if $x_j = 1$, otherwise $x_j = 0$. The optimization problem is stated as follows. Given:

- A set of n sensor nodes, $SS = \{Sn_1, Sn_2, \dots, Sn_n\}$)
- A set of m critical regions, $CRS = \{CR_1, CR_2, \dots, CR_m\}$
- A vector RCL each element of which represents the confidence level required by each CR, $RCL = [Rc_1 Rc_2 .. Rc_m]$
- A matrix $SCL_{m\times n}$ consists of $\gamma_{j,i}^{total}$ for a given critical region i and a given sensor node j.
- A matrix $Rm_{m\times n}$ which makes a relation between SS and CRS as equation 4 where R_s represents the sensing range and *dist* shows the Euclidean distance.

$$Rm_{i,j} = \begin{cases} 1 & if\ dist(Sn_j, CR_i) \le R_s \\ 0 & otherwise \end{cases} \quad (4)$$

The above binary sensor model assumes that sensor measurements have no associated uncertainty, while in reality, sensor measurements are imprecise and should be represented in probabilistic form. To this end, the above binary Relationship matrix can be replaced with Equation 5 to represent the impact of the distance on the sensing quality:

$$Rm_{i,j} = \begin{cases} e^{-\beta \times dist(Sn_j, CR_i)} & if\ dist(Sn_j, CR_i) \le R_s \\ 0 & otherwise \end{cases} \quad (5)$$

Where β is a parameter related to the physical characteristics of the sensing device, which can be obtained from field experiments. The probabilities $P_{j,i}^{obs}$ that Sn_j could observe CR_i. Actually, apart from the impact that the distance between a sensor node and a critical region may have on the sensing quality, malfunctioning of sensor nodes or changing environmental conditions may influence the sensing and coverage quality as well. To address these parameters, we already introduced $SCL_{i,j}$ above. Also, $P_{j,i}^{obs}$ is the probability that Sn_j could observe CR_i and is a combination of $Rm_{i,j}$ and $SCL_{i,j}$ as follows:

$$P_{j,i}^{obs} = Rm_{i,j} \times SCL_{i,j} \qquad CR_i \in CRS, Sn_j \in SS \quad (6)$$

Objective: Minimizing the bellow function

$$\sum_{j=1}^{n} x_j \quad (7)$$

Subject to

$$x_j \times \sum_{j=1}^{n} P_{j,i}^{obs} > 0 \quad for\ all\ CR_i \in CRS \quad (8)$$

$$P_{Cvr}(i) \geq RCL_i \quad for\ all\ CR_i \in CRS \quad (9)$$

$$x_j \in \{0,1\} \ for\ all\ Sn_j \in SS \quad (10)$$

As it is quite possible that one critical region is covered by more than one active sensor, the probability of monitoring that critical region must be calculated precisely. Usually, when probability of two simultaneous events is calculated while these events are not mutually exclusive, additive law of probability [22] is used. This means that the probability of observing a critical region *C* with two sensor nodes *A* and *B* is calculated as follows:

$$P_{Cvr}(C) = P_{A,C}^{obs} + P_{B,C}^{obs} - P_{A,C}^{obs} \times P_{B,C}^{obs} \quad (11)$$

Where $P_{Cvr}(C)$ is the probability that critical region *C* is covered by any active sensor node.

In case of having more than two nodes observing one critical region, the additive law probability becomes complex. To overcome this issue, we examine the problem from the unobserved probability perspective and calculate the cumulative coverage probability as:

$$P_{Cvr}(CR) = 1 - \prod_{j \in NS_{CR}} (1 - P_{j,CR}^{obs}) \qquad (12)$$

$$NS_i = \{j | Rm_{i,j} > 0\ and\ Sn_j\ is\ active\}$$

6.3. A greedy heuristic algorithm

Recently, there has been a growing interest in studying large-scale WSNs. Such a network consists of a large number of sensors which are densely deployed in a certain area. Basically, it is possible to compute the optimal solution by extensive search for small network sizes (small values of *n* and *m*). However, the complexity of computing the optimal solution in terms of computation grows exponentially with the size of the network. Therefore, an efficient heuristic solution approach needs to be developed.

In consideration of the limitation of ILP for large networks, as described previously, we put forward a greedy heuristic, which aims to achieve the ILP result without exploring all combinations of sensors.

Our algorithm adds sensor nodes to the *FsbSet* in a greedy way according to the P^{obs} that nodes offer for different critical regions. After finding this set, all sensor nodes belonging to *FsbSet* are removed from the available sensor nodes set. The sensor nodes from the *FsbSet* switch to activate mode and the rest would be in sleep mode. Whenever, the current active nodes are about to die, the base station has to define another *FsbSet* using the up-to-date state of the nodes and network. To this end, the base station runs our greedy algorithm (Fig 3) from the beginning with the new values for *C* matrix to discover a new *FsbSet* (if any). Finally, the network will die if the base station is unable to define *FsbSet* anymore using the available sensor nodes. In what follows, we present and then elaborate on our greedy heuristic algorithm. This algorithm takes P^{obs} and *RCL* as two key inputs and gives one *FsbSet* for the next time interval. To be able to define *FsbSet*, first we sort the sensor nodes according to the P^{obs} they offer for different critical regions in the descending order. By doing so, in the sorted matrix *C* we will have (Sn_s, $P_{s,h}^{obs}$) pair.

$$C= \begin{array}{c} 1 \\ \vdots \\ m \end{array} \begin{bmatrix} (Sn_l, P_{l,1}^{obs}) & \cdots & (Sn_k, P_{k,1}^{obs}) \\ \vdots & \ddots & \vdots \\ (Sn_r, P_{r,m}^{obs}) & \cdots & (Sn_q, P_{q,m}^{obs}) \end{bmatrix} \quad (13)$$

Then, we select the node who provides the highest $P_{x,y}^{obs}$ and check which critical region(s) is (are) covered by the given node (step 6). If the given critical region(s) has/have not already been covered by any node or its *RCL* has not been satisfied yet, we add that node to the *FsbSet*, otherwise we repeat this step while replacing the node with one who has the next highest $P_{x,y}^{obs}$. As each sensor node may be able to observe more than one critical region, we check whether there is other critical region(s) which can be covered by this node. If so, we mark those critical region(s) as being covered by that specific node with the specific probability extracted from *C* matrix for each critical region (step 7). Then, after adding the node to the *FsbSet*, set, it is removed from *C* matrix. We repeat steps 7 as long as no critical region is remained uncovered. We need to calculate the confidence level that *FsbSet* provides for each critical region (step 9). We use the additive law probability represented by Equation 12 to calculate the confidence level for a critical region, if more than one element of *FsbSet* is observing the given critical region. If the obtained confidence level by the *FsbSet* is less than *RCL* for a critical region, step 7 is repeated as long as all critical regions are covered with their *RCL*. The base station informs sensor nodes about their schedule based on which they should switch between active/ sleep mode for the next time interval.

1. $FsbSet = \{\}$
2. $\textbf{for}\ \forall\, CR \in CRS\ \ CCov(CR) = \{\}$
3. $\textbf{for}\ \forall\, Sn \in SS\ \ SCov(Sn) = \{CR | P^{obs}_{Sn,CR} > 0\}$
4. Descending sort of P^{obs} and make matrix C according to Equation 13
5. ***Repeat***
   6. $[x, y] = \textbf{arg}\ \mathbf{max}_x (P^{obs}_{x,y})$
   7. ***Repeat***
      $if\ (CCov(y) = \{\}\ || P_{Cvr}(y) < RCL(y))$
      $FsbSet = FsbSet \cup \{x\}$
      $\textbf{for}\ \forall\, z \in SCov(x)$
      $CCov(z) = CCov(z) \cup \{x\}$
      $\textbf{for}\ \forall\, P^{obs}_{s,t} \in C$
      $\textbf{if}\ (s == x) P^{obs}_{s,t} = 0$
      $else\ go\ to\ 4\ by\ finding\ the\ next\ best\ x\ using\ \textbf{arg}\ \mathbf{max}_x (P^{obs}_{x,y})$
   8. $\textbf{until}\ ((CCov(CR) \neq \{\}\ for\ \forall CR \in CRS) || (\exists CR\ P^{obs}_{Sn,CR} = 0\ for\ \forall Sn \in SS))$
   9. $\textbf{for}\ \forall CR \in CRS$
      $Use\ Equation\ 12\ to\ calculate\ confidence\ level$
10. $\textbf{until}\ ((P_{Cvr}(CR) \geq RCL_{CR}) || (\exists CR\ P^{obs}_{Sn,CR} = 0\ for\ \forall Sn \in SS))$

Fig.3. Pseudocode of propose greedy algorithm

7. Performance evaluation

The heuristic algorithm we introduced takes P^{obs} and *RCL* as inputs and gives a minimal coverage set as output. However, we could use the same proposed heuristic algorithm with different inputs . In this section we evaluate the performance of our heuristic algorithm when different input parameters are set. Actually, we want to analyze the impact of different factors on the algorithm's performance. Following, we list the name and a short description of the algorithms which are seen in the graphs.

- ILP-BNR: An ILP that utilizes binary coverage model and does not address P^{obs} and *RCL* parameters.
- CNF: Our heuristic algorithm when P^{obs} is taken as an input. It tries to achieve the highest confidence in a greedy way if only one node is allows to observe one critical region.
- CNFRCL: Our heuristic algorithm if P^{obs} and *RCL* are taken as input. Different from CNF, CNFRCL should achieve the requested *RCL* for a given CR even if more than one node has to become active and observe it.
- CNTR: Our heuristic algorithm when contribution of each sensor node (*Cntr*) is considered as an input. The contribution of each node is defined as the number of CR each node has inside its sensing range. The higher sensor node's contribution, the more covered CRs and the higher the chance to be activated for the next time interval.
- CNFTR: Our heuristic algorithm when P^{obs} and *Cntr* are taken as input. We aim to combine these two parameters to see the impact of selecting one node with the highest P^{obs} and *Cntr*. Here, due to lack of *RCL*, only one node allows to observe one CR.
- ILP-PRB: The probabilistic ILP model used in this paper and explained in section 6.2.

We simulate a stationary network with sensor nodes and critical regions which are uniformly randomly distributed in an area of $100m \times 100m$. For the performance evaluation, six sets of experiments are designed and in each set one of the following tunable parameters is changed:

- *n*: number of sensor nodes. By varying this parameter, we analyze the impact of node density on the performance.
- R_s: sensing range.
- m: number of critical region to be covered.
- RCL: maximum confidence level which could be demanded by a critical region.
- CSn:This parameter represents up to what extent a node or area nearby that node could be unreliable.
- k:as explained in last paragraph of section 6.1 the base station uses the opinion of up to *k*-hop neighborhood of a node to judge about the confidence level of the given node.

All points in the following graphs are averaged over 50 trials. Unless otherwise specified, we consider 5 critical regions and 30 sensor nodes, sensing range is set to 35m, RCL is 0. 90 for all critical regions, *CSn* is 0.75, *k*=1, $\omega_s = \omega_a = 1$ and $\beta = 0.5$. We use the optimization toolbox in Matlab to solve the ILP.

In the first experiment, we vary the number of sensor nodes between 20 to 55 with an increment of 5. From Fig 4.a. we observe that with an increase in the network density, the network lifetime shows a linear increase because a critical region can be monitored by more sensors and there is a higher opportunity for a critical region to be in the sensing range of multiple sensors. It is worth mentioning that we consider lifetime to be the duration up to the time when either there exists one critical region that can no longer be monitored by any node or the required QoS cannot anymore be guaranteed. One can see that the network lifetime produced by the ILP algorithm is longer than that of Conf-RCL. This happens because the ILP explores almost all combinations of sensors that satisfy requirements and can provide the optimal solution but ILP pays for this by a long runtime. Thus, Conf-RCL is more scalable for large WSNs. As Conf-RCL and ILP require to satisfy the RCL of the critical regions which in this case is at most 0.9, possibly sometimes more than one node j is asked to observe a CR i if $P_{j,i}^{obs} < RCL_i$. This is the main reason that these two approaches usually present shorter lifetime. Looking at the results of Average Reliability graph in Fig 4.a. helps us to understand this point, as only Conf-RCL and ILP always guarantee the RCL which is set to 0.90.

Although, CONFTR considers this but its performance in terms of provided confidence is still lower than CONF. This is because in CONFTR, $P^{obs} \times Cntr$ is considered as the key parameter based on which the activated nodes will be selected. In this case, it is quite possible that one node with a very high *Cntr* and low P^{obs} comes high on the list of being selected as an active node. Fig 4.b shows the performance of different deployment algorithms when we change the sensing radii of sensors. The longer the sensing range (surveillance range), the more nodes are able to observe multiple critical regions, the more room our approach has to schedule the sensors properly, and therefore the longer the lifetime. However, as the observation probability becomes small when the distance between the sensor nodes and critical regions gets large, the lifetime of Conf-RCL and ILP increase with a small slope compared to other algorithms. Further results which are shown in Fig.4.c are obtained by varying the upper bound of *RCL* parameter. This parameter represents the requirement of the critical regions in terms of confidence level. In case of high *RCL*, more nodes must be involved in monitoring a critical region, which results in a shorter lifetime. In the next experiment whose results are shown in Fig.4.d., we gradually decrease the failure rate of the network to see how our algorithm works on the networks with different failure rates. In other words, we vary the lower bound of the edge probabilities for the used Markov models from 0.1 to 0.8 with an increment of 0.1.

Fig.4.e. shows the impact of number of critical regions on the network lifetime. From the results we see that the lifetime decreases with the number of critical regions, because monitoring more critical region requires more energy consumption. However, after six critical regions the results remain almost unchanged because all critical regions can be covered with the already active nodes. In this experiment the size of the deployment area is fixed and we vary the number of critical regions. Therefore, we could deduce that covering six critical regions in a 100*100 area, it is almost similar to covering the whole deployment area.

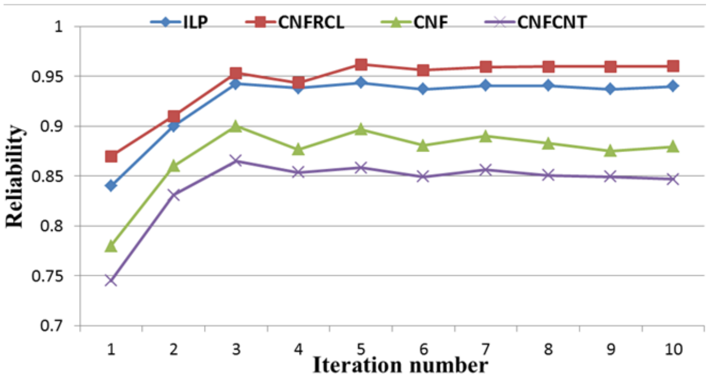

Fig.5. The impact of *k* on Reliability

Finally, in the last experiments we aim to investigate the impact of *k*, which denotes how much neighbors contribute to the global reputation of a node, on the obtained confidence for the trust based approaches. In this way for *k>1*, the reputation values build up more quickly, due to the ability of nodes to learn from each other's mistakes. The higher *k* is, the more consistent the local view is. From Fig.5. it can be seen that when *k>3*, the improvement in the confidence value is not very significant. Therefore, we could set *k* to be 3. Just to have a better insight, table 1 shows the active nodes set at the beginning for different approaches if $n=20$ and $m=4$. The settings which consider confidence as an input parameter needs larger number of nodes to be kept active at a time.

Table.1. Example of Active node set

ILP-BNR	CNF	CNFRCL	CNTR	CNFTR	ILP-PRB
{8,10}	{14,2,7}	{14,2,7,12,6}	{8,6,9}	{14,8,5}	{14,16,18,19}

8. Conclusion

One of the most active research fields in WSNs is coverage problem which is usually interpreted as how well a WSN monitors a field of interest. In this paper we propose a coverage scheme which aims to cover critical areas in an energy efficient and reliable way by mitigating the difficulties introduced by inherent uncertainties associated with sensor nodes and environment, using trust model. Quality of sensed data could be affected by the imperfection environment, faulty sensor/processor units and the distance of each node to the critical areas. Considering these issues, we formulate the coverage problem as an ILP which could provide required QoS despite node/ area imperfections. We also propose a greedy-based heuristic algorithm which tries to achieve the ILP result with much less complexity. In simulation, we change the input parameters of our greedy algorithm to show the impact of different parameters in different situations (different network set-up). According to the simulation results, one can easily judge about the appropriateness of each heuristic in different situation. The simulation results also show the superiority of our proposed approaches in terms of fulfilling required QoS parameters compared with the tradition optimal solutions.

Acknowledgement

This work is supported by IST FP7 STREP GENESI and the RECONSURVE funded by ITEA2 and Agentschap NL.

Reference

[1] HeidCarle, J., Simplot-Ryl, D. 2004. Energy-efficient area monitoring for sensor networks. IEEE Computer, vol.37, no.2, pp.40,46.
[2] Estrin, D., Govindan, R, Heidemann, J. and Kumar, S.,1999 Next Century Challenges: Scalable Coordination in Sensor Networks. Proc. of ACM MobiCom.
[3] Kahn, J., Katz, R. and Pister, K. 1999. Next Century Challenges: Mobile Networking for Smart Dust, Proc. of ACM MobiCom.
[4] Meguerdichian, S., Koushanfar, F, Potkonjak, M., Srivastava, M.B. 2001. Coverage problems in wireless ad-hoc sensor networks. Proc.s of INFOCOM. pp.1380,1387.
[5] Chakrabarty, K, Iyengar, S., Hairong Q., Eungchun, C. 2002. Grid coverage for surveillance and target location in distributed sensor networks. IEEE Transactions on Computers, vol.51, no.12, pp.1448,1453.
[6] Chakrabarty, K, Iyengar, S., Hairong Q., Eungchun, C. 2001.Coding theory framework for target location in distributed sensor networks. Proc.s of International Conference on Information Technology: Coding and Computing, pp.130,134.
[7] Zongheng, Z., Das, S., Gupta, H. 2004. Connected K-coverage problem in sensor networks. Proc. of. 13th International Conference on Computer Communications and Networks, pp.373,378.
[8] Cardei, M., Thai, M., Yingshu, L., Weili, W. 2005. Energy-efficient target coverage in wireless sensor networks. Proc. of INFOCOM, pp.1976,1984.
[9] O'Rourke, J. 1994. Computational Geometry in Column, Cambridge University Press.
[10] Cardei, M., Jie W., Mingming L., Pervaiz, M. 2005. Maximum network lifetime in wireless sensor networks with adjustable sensing ranges. Proc. of IEEE Conference on Wireless And Mobile Computing, Networking And Communications,pp.438-445.
[11] Cardei, M., MacCallum, D., Cheng, M. X., Min, M., Jia, X., Li, D. and Du, D.-Z. 2002. Wireless Sensor Networks with Energy Efficient Organization. Journal of Interconnection Networks, vol.3, pp. 213-229.
[12] Wang, G., Cao, G., La Porta, T. 2006. Movement-assisted sensor deployment, IEEE Transactions on Mobile Computing, vol.5, pp.640-652.
[13] Howard, A., Mataric, M., and Sukhatme, G. 2002. Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem. Proc. of 6th Symposium on Distributed Autonomous Robotics Systems, pp. 299-308.
[14] Poduri, S., Sukhatme,G. 2004.Constrained coverage for mobile sensor networks. Proc. of Robotics and Automation Conferences. pp.165-171.
[15] Howard, A., Mataric, M., and Sukhatme, G. 2002. An incremental self-deployment algorithm for mobile sensor networks, Special Issue on Intelligent Embedded Systems Autonomous Robots, vol. 13(2), pp. 113–126.
[16] Grossglauser, M., Tse, D. 2001. Mobility increases the capacity of ad-hoc wireless networks, Proc. of IEEE INFOCOM 2001, pp.1360,1369.
[17] Zhang, J., Yan, T., Son, S.H. 2006. Deployment Strategies for Differentiated Detection in Wireless Sensor Networks, Proc. of 3rd IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, pp.316-325.
[18] Dhillon, S.S., Chakrabarty, K. 2003. Sensor placement for effective coverage and surveillance in distributed sensor networks, Wireless Communications and Networking, pp.1609-1614.
[19] Ebert, J., Willig, A. 1999. Gilbert-Elliot Bit Error Model and the Efficient Use in Packet Level Simulation, Technical Report TKN 99-2002, Germany.
[20] Taghikhaki, Z., Meratnia, N., Havinga, P. J M. 2011. Energy-efficient Trust-based aggregation in wireless sensor networks, Proc. of IEEE INFOCOM. pp.584-589.
[21] Ozdemir, S. 2007. Secure and reliable data aggregation for wireless sensor networks. Proc. of 4th conference on Ubiquitous computing system, Japan .
[22] Additive law of probability: www.proofwiki.org/wiki/Addition_Law_of_Probability
[23] Roman, R., Fernandez, M., Lopez, J., Chen, H. 2009. Trust and Reputation Systems for Wireless Sensor Networks. Proc. of On Security and Privacy in Mobile and Wireless Networking. Troubador Publishing Ltd.