An Intruder Avoidance Vulnerable Path Adjustment Protocol for Wireless Mobile Sensor Networks

Kuei-Ping Shih†, Chun-Chih Li†, and Yen-Da Chen*

†Department of Computer Science & Information Engineering, Tamkang University, Tamshui 251, Taipei, Taiwan
*Department of Computer Information & Network Engineering, Lunghwa University of Science and Technology
Email: †kpshih@mail.tku.edu.tw, *ydchen@wireless.cs.tku.edu.tw

Abstract—**The paper proposes a protocol to adjust the vulnerable path by using mobile sensor networks. The objective of vulnerable adjustment is to protect some important areas, named TBP (to-be-protected) areas in the paper, from being attacked. In the paper, Voronoi diagram is utilized to find a vulnerable path, which is a path that an intruder may pass through. While the vulnerable path passes over a TBP area, a backward tracing and critical sets selection schemes are used to move the fewest number of sensors such that the vulnerable path can be changed and the new vulnerable path will not pass over the TBP area. Moreover, a moving schemes is proposed to decide where mobile sensors shall move. Since sensor movement is the major resource of energy consumption, thus, in order not to cause much movement, the proposed mechanism can move the fewest number of sensors with the shortest distance. Simulation results also verify the advantages of the proposed mechanism.**

I. Introduction

A wireless sensor networks (WSNs) is an auto-configured network consisted of numbers of small-size, low-cost, and low-power devices with sensing, processing, and wireless transmission capabilities, named *sensors*, deployed in an area of interest, called sensing field, in an ad hoc or prearranged fashion. The purposes of WSNs include sensing, monitoring, or tracking environmental events, which have been widely used in battlefield surveillance, environmental monitoring, biological detection, home automation, industrial diagnostics, and so on [1].

These different applications also bring new challenges to WSNs. One of the fundamental and important challenges is the quality of surveillance provided to the sensing field, which is also known as the coverage problem in WSNs. Many different aspects of coverage problems have been investigated in the literature to support different quality of surveillance of the sensing field, which includes the area coverage [2], [3], point coverage [4], [5], barrier coverage [6], [7], and path coverage [8], [9], [10], [11] problems, etc. The major difference between these coverage problems is the targets on which the coverage problem focuses.

In recently years, some of the researches [8], [9], [11], [12], [13], [10] discussed the coverage problem in the scenario which has two opposite roles. One is a defender and the other is an intruder, which are respectively located at the left side and right side of the scenario. From the intruder's viewpoint, the intruder wants to cross the sensing area safely without being detected. On the contrary, in order to detect the movement of the intruder, the defender deploys a lot of mobile sensors on the sensing field where the intruder might pass. Based on the scenario, many previous researches focused on looking for a path which has the weakest sensed capability in the sensing field. Moreover, some works[9], [11], [10] try to deploy addition sensors to enhance the sensing capability for the weakest sensed path in the sensing field. However, it is difficult to deploy addition sensors in some scenarios, such as battlefield or forest. Nevertheless, deploying mobile sensors in WSNs is a feasible way. Mobile sensors can be used to enhance the path with the weakest sensed capability.

Different from the traditional coverage problem, this paper addresses a different kind of coverage problem via moving sensors to protect some important areas, which is termed *area protection problem* in this paper. The paper considers the area protection problem via collaborative movements of mobile sensors for mobile sensor networks to protect some important areas. The scenario of the area protection problem is stated as follows. Suppose there exists several to-be-protected areas, denoted TBP areas, in a sensing field. Numbers of mobile sensors are randomly deployed in the sensing field to protect these TBP areas from being intruded or attacked. The intruder comes from one side of the sensing field and is crossing the sensing field to the opposite side. The intruder will greedily take the least-discovered route to pass through. The path that the intruder passes through is called a vulnerable path. The area protection problem is to figure out how the mobile sensors move such that the vulnerable path will not pass through any of the TBP areas.

In the paper, a vulnerable path adjustment protocol is proposed to alter a vulnerable path such that the intruder will not pass through the TBP areas. As far as we know, vulnerable path adjustment protocol is a new protocol in wireless mobile sensor networks and this paper is the first one to solve the vulnerable path adjustment problem. A vulnerable path can be altered by mobile sensors. However, sensors movement is energy-consuming. Therefore, efficient and effective movement needs to be well-managed. The problem to alter the vulnerable path can be divided into two subproblems. The first subproblem is to figure out where to alter the vulnerable

978-1-4244-5228-6/09/$26.00 ©2009 IEEE

path and the second one is to find which sensors need to move and where these sensors shall move. According to the characteristics of the intruder's movement, an altering point is found to alter the vulnerable path such that vulnerable path not to pass through the TBP areas. As a result, the new locations where mobile sensors shall move can be calculated. Simulation results show that the proposed mechanism can prevent the intruder from passing through the TBP areas. Moreover, the number of mobile sensors to be moved is the fewest and the network lifetime can be prolonged as well.

The rest of this paper is organized as follows. The background knowledge used in the paper is introduced in Section II. The vulnerable path which the intruder passes on can be figured out by using Voronoi diagram. Therefore, Section III presents the proposed protocol to alter the vulnerable path such that the intruder will not pass through the TBP areas, where the altering point as well as a moving scheme is proposed as well. Simulation results to verify the proposed mechanism are illustrated in Section IV. The concluding remarks are made in Section V.

II. Preliminaries

There are n sensors are deployed by the defender to detect the movement of the intruder. Let the sensors which deployed by the defender be the set $S = \{s_0, s_1, ..., s_{n-1}, s_n\}$. According to the detection probability model, the sensing ability decrease with the increasing of distance to target. The sensing ability can be formulated as Eq. (1). The $d(s_i, p)$ represents the Euclidean distance between the sensor s_i and any points p. The positive constants λ and k are sensor technology-dependent parameters. In other word, the farther away the target locates, the harder sensor can detect. For arbitrary p in the sensing field, there exists a least one sensor which closest to the point p.

$$S(s_i, p) = \frac{\lambda}{(d(s_i, p))^k}, s_i \in S \tag{1}$$

From intruder's viewpoint, the intruder wants to seek the path which has the lowest probability being sensed. However, it is difficult for the defender to estimate intruder path due to the large number of sensors are deployed in the sensing field. In order to reduce the complexity of the looking for the intruder path, the scene is simplified into only two sensors in the network at first. If the intruder wants to look for a safest path in such scene, it has to look for the path which far away both of the sensors in the scene. The perpendicular bisector of the sensors has the same distance to the both of the sensors in the scene. The intruder has lowest probability to been detected by the both of the sensors because of the distance from sensor to any points on the edge is maximized. The scene which has the number of sensors can be analyzed by using same way. Drawing the perpendicular bisector of any adjacent sensor on the scene is used to analyze the intruder path. This kind of graph is called the Voronoi diagram in the graph theory and used to analyze the intruder path.

The Voronoi diagram has been used and studied in many domains. The Voronoi diagram is used to analyze the intruder path in this paper. The Voronoi diagram partitions the sensing field into a set of convex polygons such that all points inside a polygon are closest to only one sensor. A Voronoi diagram is shown as Fig. 1. The perpendicular bisectors of two sensors are called Voronoi edges which are the lines in Fig. 1. Let the Voronoi edge set of two adjacent sensors be the VE. And the intersection points of voronoi edge are called voronoi vertices which are the star points in the Fig. 1. Let the Voronoi vertices set be the VV. The Voronoi diagram which consists of sensors in the sensing field can be expressed as the $VG = (VV, VE)$.

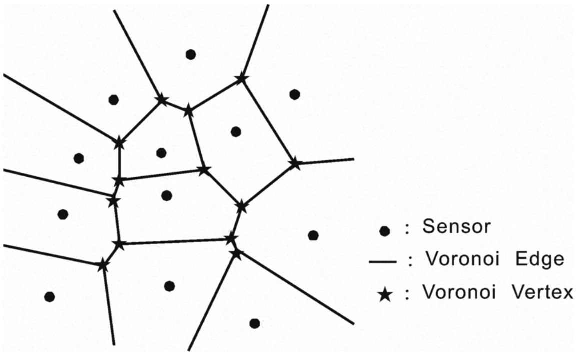

Fig. 1. The Voronoi diagram consists of Voronoi vertices and Voronoi edges.

In order to quantify the sensing ability on Voronoi edge, the weight value is designed to quantify the sensing ability. According to the detection probability model in Eq. (1), the sensing ability is inversely proportional with the distance to the closest sensor. The weight value of a Voronoi edge is defined as the shortest distance from the sensor to the Voronoi edge which can be expressed as following.

$Weight(VE_i) = min(p, S)$, for all $p \in VE_i, VE_i \in VE$

The larger value on weight means the weaker in the sensing ability. In other words, the intruder has to choose the larger weight Voronoi edge as the vulnerable path to prevent the detecting by the sensors. However, the intruder is supposed decides the vulnerable path which has lowest probability being detected by the local information. The intruder does the decision at the every Voronoi vertices which the intruder passed. Most important of all, the intruder has to cross the area which deployed the sensors. The direction of intruder is supposed always toward the destination. In other word, the Voronoi edges which back away to the destination will not be chosen as the intruder path. In summary, this paper has two basic assumptions on intruder path on flowing.

- The intruder always chooses the vulnerable path at every Voronoi vertices which met by the intruder. The intruder chooses the larger weight Voronoi edge as vulnerable among the Voronoi edges which the intruder can choose.
- The intruder never chooses the Voronoi edge which back away to the destination as the vulnerable path.

The defender deploys number of sensor to detect the movement of the in the sensing field. Moreover, there exist some areas which do not want to be crossed by the intruder. Those areas is called TBP area and notated as the VA. Each TBP area is composed of a set of Voronoi edges and Voronoi vertices. The TBP area VA can be expressed as the

$VA = (VV_{VA}, VE_{VA})$. Once the intruder path pass through the VA, defender has to alter the intruder path by moving some of the sensors in the sensing field.

III. Vulnerable Path Adjustment Protocol

As the discussion in the previous section, the defender has to alter the intruder path if and only if the TBP area is passed through by the intruder path. Therefore, the TBP area protection problem can be divided into two sub-problems. One is to finger out which sensors should be selected to alter the vulnerable path. The other is to decide where sensors should be moved to in order to alter the vulnerable path with minimal energy consumption. First, how to select the sensor to move will be described. Following, the moving scheme to alter the vulnerable path is going to introduce.

A. Overview

The multiple TBP areas are supposed in the sensing area. The defender has to prevent the intruder passing through the TBP area. Once the intruder path passes through one of the TBP area, the defender has to activate the mechanism and move the sensors such that the intruder path not to pass TBP area. However, it is difficult to consider all the TBP areas at the same time. In order to simplify the area protection problem, the sensing area is divided into several subarea which like Fig. 2. Each sub-area only has one TBP area. The whole problem is simplified into only a TBP area in each subarea. The proposed mechanism activates once the TBP areas in a sub-area passed through by the intruder. The defender chooses a set of mobile sensors in the sub-area to move and alter the vulnerable path. If the intruder will not pass the TBP area in any sub-area, the intruder path does not pass any TBP area in the sensing field.

The basic idea of the altering vulnerable path is that let the intruder path alter at any of the Voronoi vertices on the vulnerable path. However, the intruder still follows the greedy rules to choose the intruder path. The intruder still has probability to pass the TBP area. At this time, the defender has to choose another set of sensors to move and the additional energy cost is made. This problem is called re-entry problem in the paper. In order to minimal the moving cost as possible, the entry vertices searching mechanism is proposed to select the candidate Voronoi vertices which can the altering the intruder path without re-entry problem. Based on the analysis of the Voronoi edge, the weight-based moving schema is proposed to decide where the sensor has to move. Final, a set of moving sensors is chosen to move and alter the intruder path.

B. Entry Vertices Searching Mechanism

In order to choose the candidate to alter Voronoi vertices without the re-entry problem, the Entry Vertices Searching The definition of the entry Voronoi vertex is defined as follow.

Definition 1: The Voronoi vertex becomes an entry Voronoi vertex if and only if the Voronoi vertex leads the intruder path passed the TBP area.

For example, the VV_1 in the Fig. 3 is one of the Voronoi vertices on the intruder path which passes the TBP area. According to the intruder path selection rules, the intruder selects the Voronoi edge which passes the TBP area at VV_1. In other word, the Voronoi vertex VV_1 which leads the path passing through the TBP area and the VV_1 is called an entry Voronoi vertex. Once the intruder does the intruder path selection at the entry Voronoi vertex, the intruder path will be leaded to pass the TBP area. However, the defender has to prevent the intruder does the path selection at those entry Voronoi vertices. The entry Voronoi vertices searching mechanism is designed to looking for the all entry Voronoi vertices in a sub-area.

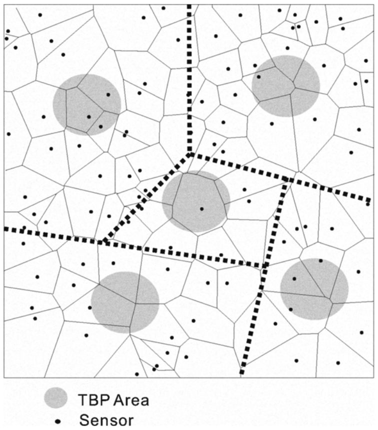

Fig. 2. The sensing area is divided into several sub-area and each sub-area only has a TBP area.

The basic idea of entry Voronoi vertices searching mechanism is based on the backward tracing and the intruder path analysis. By using backward tracing, the all possible path which leads the path choosing the TBP area can be found out. Moreover, the entry Voronoi vertices also can be found out. The detail of the Voronoi vertices searching mechanism describes as follow. The entry Voronoi vertices searching algorithm starts the searching from the Voronoi edges which enter the TBP area. However, some of the Voronoi edge impossible passes through the TBP area due to the constraints on vulnerable path selection rules and it can be ignored. For example, $VE_1, VE_2, VE_3, VE_4, VE_5$ are the Voronoi edges which enter the TBP area. However, the intruder will not choose the Voronoi edge which goes back away to destination so that the Voronoi edges VE_3, VE_4, VE_5 will be excluded and the backward tracing starts from the VE_1, VE_2. If the intruder passes through the TBP area by passing the Voronoi edge VE_1, it means the intruder has to do the choices at the Voronoi vertex VV_1 and the intruder has to chose the VE_1 as the path at the VV_1. According to the intruder path selection rule, the intruder chooses the Voronoi edge which has the largest weight among all the onward Voronoi edges at VV_1. Once the Voronoi edge VE_1 has the largest weight among all the onward Voronoi edges, the intruder must pass through the TBP area. The Voronoi vertex VV_1 is one of the entry Voronoi vertices in the sensors. The intruder path will pass the TBP area because of the intruder arrives the entry Voronoi vertex. It is necessary to prevent the intruder to arrive the entry Voronoi vertices. After the determine the Voronoi vertex VV_1 is entry

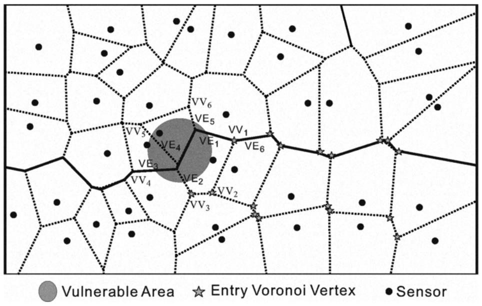

Fig. 3. An Example of Entry Voronoi Vertices.

Voronoi vertex, the Voronoi edges which connects to the entry Voronoi vertex, VV_1, VE_6, also needs to determine whether the Voronoi vertex is entry Voronoi vertex or not.

The entry Voronoi vertex set searching mechanism is used to search the entry Voronoi vertices. However, the entry Voronoi vertices only means that once the intruder arrives one of the entry Voronoi vertices the intruder path will pass through the TBP area. The suitable altering Voronoi vertices which lead the intruder path altering are going to be discussed. A straightforward idea of altering the intruder path is that altering the intruder path at any of Voronoi vertices on the intruder problem. However, the re-entry problem will occur if altering the intruder path at unsuitable Voronoi vertices. For example, the intruder path can be altered at VV_1 in the Fig. 3. However, the intruder still arrive another entry Voronoi vertex no matter what direction the intruder path altering. To deal this problem, the altering Voronoi vertex should be chosen carefully.

In order to pick suitable Voronoi vertices to alter the intruder path, the entry Voronoi vertices is divided into two types. One is the alterable entry Voronoi vertex and another is the non-alterable entry Voronoi vertex. The alterable entry Voronoi vertex means that the intruder path can be alter at this Voronoi vertex without generating the re-entry problem. The characteristic of this type of entry Voronoi vertex is that the entry Voronoi vertex has a least one Voronoi edge connecting to the Voronoi vertex which is not the entry Voronoi vertex. For example, the VV_6 in the Fig. 4 has a Voronoi edge connecting to the non-entry Voronoi vertex. The Voronoi vertex VV_6 belongs the alterable entry Voronoi vertex. Relatively, the non-alterable entry Voronoi vertex means that the Voronoi edges of entry Voronoi vertex connect to entry Voronoi vertex. The results of entry Voronoi vertices dividing is shown in. It is easy to see that the intruder path can be altered at the alterable entry Voronoi vertex. It is useless to alter the intruder path at non-alterable entry Voronoi vertex. The non-alterable entry Voronoi vertex has to cooperate with non-alterable entry Voronoi vertex. Once the intruder path alters at the non-alterable entry Voronoi vertex, it has to cooperate with a non-entry Voronoi vertex on the following path. Due to the Voronoi vertex VV_7 is non-alterable entry Voronoi vertex, it has to cooperate with a non-entry Voronoi vertex on the following path. In this example, the intruder path has been altered successfully after altering the intruder path at VV_7, VV_2. By these rules, the suitable set of altering path can be found out.

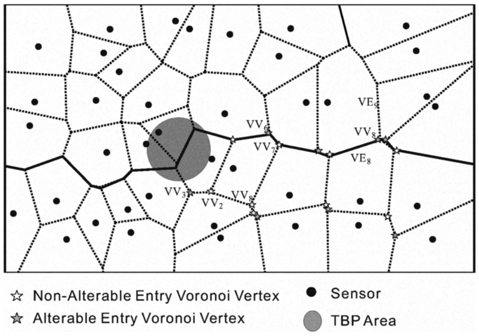
VE7
VV6
VV7
VV8
VE8
VV3
VV2
VV4
☆ Non-Alterable Entry Voronoi Vertex
★ Alterable Entry Voronoi Vertex
● Sensor
TBP Area

Fig. 4. An Example of the Alterable and Non-alterable Entry Voronoi Vertices.

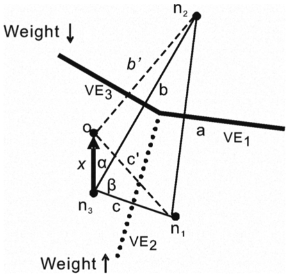

Fig. 5. An Example of Weight-Based Moving Scheme.

C. Vulnerable Path Altering Scheme

The suitable Voronoi vertices sets to alter the intruder path is chosen in previous section. However,it has not yet to explanation that how to alter the intruder path at a selected Voronoi vertices by moving the sensors.

If the defender wants to alter the intruder path at the selected Voronoi vertex, the intruder has to do different choices at the selected Voronoi vertex. According to the vulnerable path selection rules, the intruder do the choices at the voronoi vertex and the intruder always choose the Voronoi edge which has largest weight among the all Voronoi edges as the vulnerable path. The main idea of the weight-based moving scheme is that decrease the weight on the Voronoi edge which the defender wants to be passed by the intruder and increase the weight on the Voronoi edge which the defender does not want to be passed by the intruder. Taking VV_6 in Fig. 4 for example, the defender has to increase the weight on the Voronoi edge VE_7 and decrease the weight on the Voronoi edge VE_6. Once the weight on the Voronoi edge VE_7 is bigger than the weight on the Voronoi edge VE_6, the intruder do the different choices at the VV_6. The intruder choices the upside Voronoi edge as the vulnerable path and the vunerable path will not pass the TBP area.

In order to change the weight on the Voronoi edge, the defender has to move the sensor to close the Voronoi edge where passed by the intruder and away the Voronoi edges where not to passed by the intruder. The intruder chooses the sensors which both can increase the weight on the one Voronoi edge and decrease the weight on another Voronoi edge. For example in the Fig. 4, the defender chooses the $s1$ to move due to the movement of the $s1$ causes the affection on the both Voronoi edge. After the sensors move to the new location, the weight value should be changed. For easy explanation, Fig. 5 is used to explain the following calculation. In the example, the intruder path represents as boldface line and denotes as VE_3. The dot line represents the path which the defender wants to alter to and denotes as the VE_2. The Delaunay triangulation is used to calculate the new location of the sensor. The Delaunay triangle is composed of three edges which are the perpendicular bisectors of the VE_1, VE_2, VE_3. The edges of the Delaunay triangle are denotes as the a, b, c. The length of the a, b, c are represented as $l(a), l(b), l(c)$. The angle between b and c is β. After the sensor moved to new location o, the new Delaunay triangle is composed of three edges which are b' and c'. According to Law of Cosines, the new length of the (b') and $w(c')$ can be formulated as follows.

$$l(b')^2 = l(b)^2 + x^2 - 2l(b)x\cos\alpha \tag{2}$$

$$l(c')^2 = l(c)^2 + x^2 - 2l(c)x\cos(\alpha+\beta) \tag{3}$$

The main idea of the weight-based moving scheme is that let the weight of the Voronoi edge which defender wants to be passed by the intruder bigger than the weight of the Voronoi edge which defender does not want to be passed by the intruder. The relation between $l(b')$ and $l(c')$ can be derived based on Eq. (2). The relation between the moving distance and the moving direction has been formulated. The minimal moving distance can be found if the moving direction has been chosen. However, the defender wants to use minimal moving distance to change the weight on Voronoi edge. The differential is used to find the shortest moving distance and best angle. After calculated first order derivative, the angle which causes the maximal or minimal moving distance can be found by solving the first order derivative. In order to verify the limit value is minimal or maximal, it is necessary to derive the second order derivative to show the minimal existed. The result of second order shows derivative always positive, it means that the angle derived from first order derivative has the minimal moving distance. The best angle which causes shortest moving distance can be calculated by the first order derivative.Moreover, the minimal moving distance X can be calculated. The final results are shown in the Eqs. (4) and (5).

$$\alpha = \arctan(\frac{c\sin\beta}{b - c\cos\beta}) \tag{4}$$

$$x = \frac{b^2 - c^2}{2b\cos(\alpha+\beta)} \tag{5}$$

IV. Performance Evaluation

A lot of simulations has been proceeded to evaluate the performance of the proposed mechanism. The simulator is written by using C++. Due to the proposed mechanism is the first work which using the mobile sensors to alter the intruder path and protect TBP area. A greedy and simple mechanism is used to compare with the proposed mechanism. The greedy mechanism is that moving the sensors which close to the TBP area and direct to the TBP area until the intruder path disappear. The greedy mechanism not only increases the quality of sensing in TBP area but also alters the intruder path. The energy consumption is affected by the two factors, which are node density in the sensing field and size of TBP area. The simulation results compare the energy consumption under different node density and size of TBP area. Sensors are randomly deployed in the sensing field. Each sensor has 5‰ failure probability which causes by the out of energy or hardware broken or etc. Other simulation settings are shown in Table I.

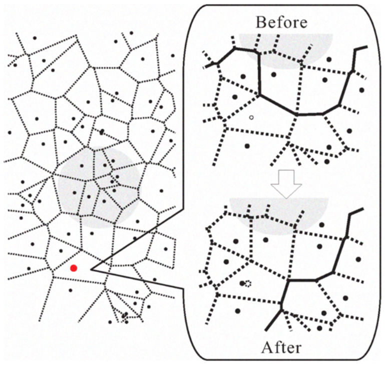

Fig. 6. The Moving Results By Using Vulnerable Path Adjustment Protocol.

TABLE I
Simulation Parameters

Parameter	Value
Simulation area	500 meters × 500 meters
Radius of TBP area	70 meters
Number of sensors	300 meters
Failure Probability	5‰
The initial moving of each sensor	4 unit
The energy on moving per meter	3 unit

First, the correctness of the proposed mechanism is shown in Fig. 6. The 100 mobile sensors are deployed in the 500 meters square sensing field. The proposed Entry Vertices Searching Mechanism is used to locate the Voronoi vertices which leads the intruder path crossing TBP area. The weight-based moving scheme is adopted to move the mobile sensors. The moving result is shown in Fig. 6. The left part of the figure is the scenario which after the moving. The red point means the sensor which needs has to move. The right part of the figure is the zoom in figure which compares the location of sensors before moving and after moving. Due to the weight-based moving scheme increase the weight on the Voronoi edge which is not chosen by the original intruder path, the intruder path would be change the choices at selected Voronoi vertex. In the enlargement part of the figure, it is clear to see that the intruder path has been changed by only moving the short distance. The accurate moving distance which is calculated by the weight-based moving scheme is 0.67 meters.

The proposed mechanism wants to use minimal energy to alter the intruder and protect the TBP area. The simulation results on energy consumption are shown in Fig. 7 and Fig. 8. Fig. 7 shows the energy consumption under different sensor density and TBP area size by using the proposed mechanism. Fig. 7 shows the energy consumption under different sensor

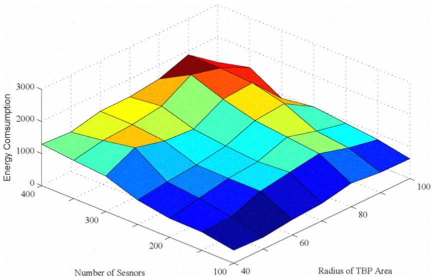

Fig. 7. The Moving Energy Consumption on Vulnerable Path Adjustment Protocol.

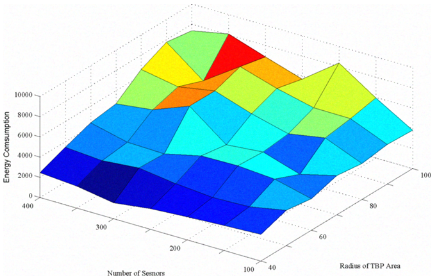

Fig. 8. The Moving Energy Consumption on Greedy Mechanism

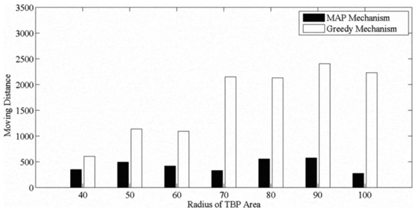

Fig. 9. The Comparison of Moving Distance in 300 Sensors Scenario.

density and TBP area size by using the proposed mechanism. Similarly, Fig. 8 shows the energy consumption by using the greedy mechanism. Both of the simulation results shows the energy consumption increase with the sensor density and TPB area size. The proposed mechanism costs energy less than 2000 units on moving in most of case in Fig. 7. However, the greedy mechanism costs energy much than 2000 units on moving in most of case in Fig. 8. It is easy to see the proposed mechanism save much energy on moving than greedy mechanism. In order to analyze more detailedly, the moving distance of scenario which deploys 300 sensors is shown in Fig. 9. The proposed mechanism moving less distance than greedy mechanism due to the proposed mechanism always moving the sensors which costs less energy. Fig. 9 also shows the proposed mechanism does not increase the moving distance violently.

V. Conclusions

Vulnerable path adjustment problem is a popular encountered problem in the sensor networks, such as the military defense, reservation area protection, and so on. The paper proposed a solution to protect some area being attacked and dynamically alter the vulnerable path such that the intruder will not pass through the TBP areas. As far as we know, vulnerable path adjustment is a new problem in sensor networks and this paper is the first one to solve the problem.

According to Voronoi diagram, proposed mechanism can find an altering point on the vulnerable path such that the adjustment of the altering point can prevent the vulnerable path from passing through the TBP areas. As a result, the movement of mobile sensors is able to adjust the altering point. Therefore the fewest number of mobile sensors are figured out to move such that the vulnerable path will not pass through the TBP areas. Moreover, a weight-based moving schema is proposed to alter the vulnerable path. Simulation results show that the proposed mechanism can effectively change the intruder path not to pass through the TBP areas. Moreover, the energy consumption of the proposed protocol is much lower than that of a greedy one.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] B. Carbunar, A. Grama, J. Vitek, and O. Carbunar, "Coverage preserving redundancy elimination in sensor networks," in *Proceedings of the Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2004, pp. 377–386.

[3] K.-P. Shih, Y.-D. Chen, C.-W. Chiang, and B.-J. Liu, "A distributed active sensor selection scheme for wireless sensor networks," in *Proceedings of the IEEE International Symposium on Computers and Communications (ISCC)*, Jun. 2006.

[4] Q. Zhao and M. Gurusamy, "Maximizing network lifetime for connected target coverage in wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Jun. 2006.

[5] K.-P. Shih, H.-C. Chen, C.-M. Chou, and B.-J. Liu, "On target coverage in wireless heterogeneous sensor networks with multiple sensing units," *to appear in Journal of Network and Computer Applications*, 2009.

[6] A. Chen, S. Kumar, and T. H. Lai, "Designing localized algorithms for barrier coverage," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Sep. 2007.

[7] B. Liu, O. Dousse, J. Wang, and A. Saipulla, "Strong barrier coverage of wireless sensor networks," in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, May 2008, pp. 411–419.

[8] S. Megerian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proceedings of the IEEE INFOCOM, the Annual Joint Conference of the IEEE Computer and Communications Societies*, Jun. 2001.

[9] S. Megerian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Worst and best-case coverage in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 84–92, Jan.-Feb. 2005.

[10] S. Zhou, M.-Y. Wu, and W. Shu, "Blocking vulnerable paths of wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, Nov. 2006.

[11] R.-H. Gau and Y.-Y. Peng, "A dual approach for the worst-case-coverage deployment problem in ad-hoc wireless sensor networks," in *Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, Oct. 2007.

[12] S. Megerian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Nov. 2001.

[13] Q. Huang, "Solving an open sensor exposure problem using variational calculus," Technical Report WUCS-03-1, Washington University, Department of Computer Science and Engineer, St, Louis, Missouri, Tech. Rep., 2003.