Maximizing the Lifetime of Layered Defense in Wireless Sensor Networks

Cheng-Ta Lee[a, b], Frank Yeong-Sung Lin[a], and Yu-Shun Wang[a]
Department of Information Management
National Taiwan University[a]
Lan Yang Institute of Technology[b]
{d90001, yslin, d98002}@im.ntu.edu.tw

***Abstract* —In this paper, we focus on efficient layered defense strategies for wireless sensor networks of grouping capabilities. We try to find the maximum *K* groups of sensors for layered defense subject to defense rate, early warning rate, battery capacity, intruder behaviors, and defender strategies constraints. The mechanism can prolong the system lifetime and provide lead time alarms. The problem is modeled as a generic mathematical programming problem. A novel three-phase solution approach, which well combines mathematical programming and simulation techniques, is proposed. The experimental results showed that the proposed efficient layered defense strategies algorithm (ELDSA) gets applicability and effectiveness in the layered defense for grouping capabilities.**

I. INTRODUCTION

In the past few years, from either practical or theoretical domain, the application and technique development of wireless sensor networks (WSNs) are important research issues [1], [2]. Some interesting applications for WSNs have been investigated, e.g., surveillance, object positioning, object tracking, intrusion detection, anti-terror, and health care. In addition, under some applied circumstances, we need to detect the objects that intrude the safeguard area [6]-[9], eg., the commander must be notified when the enemies enter the safeguard area in order to take necessary action. Besides, intrusion detection of enemies is also required to record whether the objects enter monitored area for further notification and following track.

In layered defense security, the layered defense is used to describe a security system using multiple rings and policies to safeguard core field of the WSNs against multiple threats including enemies attack and other security considerations.

In this paper, we focus on the sensor grouping problem to support layered defense service. First, we try to find out the sensors nodes to cover the monitoring region for layered defense and early warning rate. Second, we will describe the behavior of intruder. Third, we want to describe the defender strategies. Forth, we want to find the maximum *K* groups of sensors for layered defense in sensor networks. This mechanism can prolong the system lifetime.

The problem is modeled as a generic mathematical programming problem, and a novel three-phase solution approach, which well combines mathematical programming and simulation techniques, is proposed. In first phase, the "initial solution phase", we propose an efficient heuristic algorithm for initial solution. In second phase, the "objective function evaluation phase", we propose efficient and effective simulations are conducted to evaluate the effectiveness of the current defense policy. In third phase, the "add-and-drop phase", we use add-and-drop algorithm to improve and satisfy the defender strategies. From computational experiments in WSNs, applicability and effectiveness of the proposed framework and algorithm are clearly demonstrated.

In the prior studies [6]-[10], In [6], W. Yun, W. Xiaodong, X. Bin, W. Demin, and D.P. Agrawal analyzes the intrusion detection problem in both homogeneous and heterogeneous WSNs. The work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application requirements. In [7], [8], G. Li, J. He, and Y. Fu propose a distributed group-based intrusion detection scheme that meets all the above requirements by partitioning the sensor networks into many groups. The group-based intrusion detection scheme can save power consumption. In [10], P.L. Chiu and F.Y.S. Lin construct the sensor network such that it includes *K* mutually exclusive sets (number *K* is given). These sets are called covers. The covers are disjoint covers. The method can find out the nodes of group and prolong the system lifetime.

In this paper, we introduce the concept of check point and the check points can assist to reach defender policy. Besides, check points can save energy consumption because the concept can check redundant nodes more efficiently for arbitrary topology. Furthermore, we find the maximum *K* sets of sensors to support layered defense service on monitoring region. These sets can be joint or disjoint sets. Each of them, is called a group, can provide to satisfy defender policy in monitoring region. Each group is activated in turn to monitor the monitoring regions. Generally, the power consumption for inactive sensors can be neglected, and the system lifetime can be effectively prolonged up to *K* times. We present a mathematical model to describe the optimization problem and a heuristic-based algorithm is proposed to solve the problem.

To the best of our knowledge, this work is the first effort to model the layered defense in wireless sensor networks.

We formulate the problem as a generic mathematical programming problem where the objective function is the maximization of the system lifetime of layered defense subject to defense rate, early warning rate, battery capacity, intruder behavior, and defender strategies constraints. We construct a heuristic-based algorithm to solve the problem.

The problem is formulated as an optimization-based problem with two different main decision variables: wake up sensor *s* in the round *r* and satisfying defense policies in the round *r*. Wake up sensor *s* in the round *r* is 1 if sensor *s* is awake in the round *r*, and 0 otherwise. Satisfying defense policies in the round *r* is 1 if round *r* is satisfying total defense rate and early warning rate in the round *r*, and 0 otherwise. In the further computational experiments, our proposed layered defense for grouping capabilities algorithm is expected to be efficient and effective in dealing with the optimization problem.

From papers review, we find that this study differs from prior works in several points. First, we consider both the energy conservation and lifetime extending during the sensor deployment phase for layered defense. Second, we present a mathematical model to describe the optimization problem. Third, the relationship between the grouping capabilities of layered defense and the maximum extension of system lifetime is investigated. Fourth, we present a new concept of the check point for deal with the problem.

The rest of this paper is organized as follows. The problem and mathematic model are described in section 2 and 3, respectively. Additionally, the solution procedure is presented in section 4. Furthermore, the computational results are discussed in section 5, and conclusions are presented in section 6.

II. PROBLEM DESCRIPTION

A. Layered Defense for Grouping Capabilities

In this section, we describe the problem and propose the attack and defense scenario with specific assumptions.

Definition 2.1 *Defense rate* (*D*): The number of detected intruders divided by the total number of intruders.

Definition 2.2 *Early warning rate* (*W*): The number of satisfying early warning distance *L* divided by the total number of intruders.

For example, defenders set defense rate=0.9 and early warning rate=0.8. If defenders deploy the topology of sensor to satisfy the condition, then the strategies can prevent 90% intruders and satisfy 80% early warning. Defenders use defense strategies, defense rate and early warning rate, to protect core field. Furthermore, the defense strategies can support object tracking and detection airborne intruders.

We try to find maximum *K* sets of sensors to support layered defense service, as shown in Fig. 1. Each of them, is called a group, can provide satisfying total defense rate and early warning rate of the monitoring region. Each group is activated in turn to monitor the monitoring region. Fig. 2 shows the state transitions of the sensor network. From the network viewpoint, two operation states exist: the sleeping and active states. Only one group sensors are activated in turn to monitor the region, and the other group sensors are sleeping in one time. The system lifetime can be effectively prolonged up to *K* times.

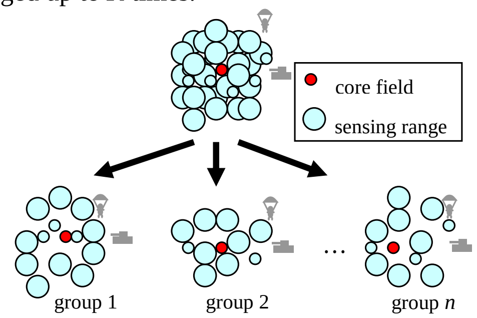

Fig. 1 The layered defense model.

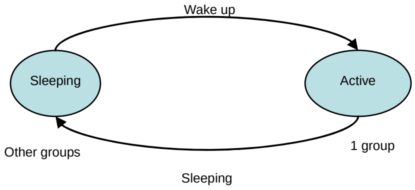

Fig. 2 The state diagram of the sensor network.

Each objective of intruder is to attack the core field in the given sensor network. The defender has perfect knowledge of the sensor network. The defender tries to find the maximum *K* groups of sensors for layered defense subject to defense rate, early warning rate, battery capacity, intruder behavior, and defender strategies constraints. However, the intruders are not aware that the defender has deployed topology in the sensor network; in other words, their knowledge of the network is imperfect. In addition, we assume that each intruder only has information about the core field location.

B. Behaviors of Intruders

1. *Motion model of intruders*: The mobility pattern uses the Gauss-Markov motion model [3].
2. *Intrusive angle*: An intrusive angle model uses one tuning parameter to vary the degree of randomness in the intrusive angle pattern by using the random distribution.
3. *Airborne intruders*: We use special airborne intruder to make intrusive behavior more general. The *airborne rate* is ratio of airborne intruders.

III. PROBLEM FORMULATION

The notations used to model the problem are listed as follows.

TABLE I
NOTATION OF THE CONTROL PARAMETER

Notation	Description
M_r	The total evaluation frequency for all intruder categories in round *r*

TABLE II
NOTATIONS OF THE GIVEN PARAMETERS

Notation	Description
K	The total intruder categories.
T_{kr}	Total evaluation frequency of each intruder type in round r (where $k \in K$, $r \in R$).
F	All possible defense strategies.
$\vec{I}_k$	The strategies of an intruder, comprising his motion and intrusive angle.
$G_{kjr}(\vec{F}, \vec{I}_k)$	1 if the intruder j of the k^{th} intruder category can intrude in the core field before be detected under $\vec{F}$ defense strategies in round r, and 0 otherwise (where $k \in K$).
S	The set of all sensor nodes.
C_s	The initial energy level of sensor node s.
E_m	The energy consumption for sensor nodes to sense data.
R	The upper bound of number of rounds.
D	The defense rate.
L	The distance of early warning.
W	The early warning rate.
C	Core field: $x_c^2 + y_c^2 \le h^2$, (x_c, y_c) is coordinate of core and h is radius of core.
N	The set of candidate location (x, y) if intruder be detect.

TABLE III
NOTATIONS OF THE DECISION VARIABLES

Notation	Description
π_{sr}	1 if sensor s is awake in the round r; and 0 otherwise.
z_r	1 if satisfy total defense rate and early warning rate in the round r, and 0 otherwise.
$\vec{F}$	The strategies of defender that sensor s is awake in the round r.
$b^{kjr}_{(x,y)}$	1 if the intruder j of the k^{th} intruder category that Euclidean distance between location (x, y) and *core* greater than or equal to L in round r, and 0 otherwise.

Problem (IP):

$$\max \sum_{\forall r \in R} z_r \qquad \text{(IP)}$$

subject to:

The defense rate constraint

$$z_r - \left(\left(1 - \frac{\sum_{k=1}^{K}\sum_{j=1}^{T_{kr}} G_{kjr}(\vec{F}, \vec{I}_k)}{M_r}\right) - D\right) \le 1 \qquad \forall r \in R \qquad (1)$$

The early warning rate constraints

$$b^{kjr}_{(x,y)} - \frac{\sqrt{x^2+y^2} - L}{\sqrt{x^2+y^2} + L} \le 1 \qquad \forall k \in K,\ j \in T_k,\ r \in R,\ (x,y) \in N \qquad (2)$$

$$z_r - \left(\frac{\sum_{k=1}^{K}\sum_{j=1}^{T_{kr}} b^{kjr}_{(x,y)}}{M_r} - W\right) \le 1 \qquad \forall r \in R,\ (x,y) \in N \qquad (3)$$

The battery capacity constraints

$$\sum_{r \in R} \pi_{sr} E_m \le C_s \qquad \forall s \in S \qquad (4)$$

The all possible defense strategies constraints

$$\vec{F} \in F \qquad (5)$$

The total evaluation frequency constraints

$$\sum_{k=1}^{K} T_{kr} = M_r \qquad \forall r \in R \qquad (6)$$

The integer constraints

$$\pi_{sr} = 0 \ or\ 1 \qquad \forall s \in S,\ r \in R \qquad (7)$$

$$z_r = 0 \ or\ 1 \qquad \forall r \in R \qquad (8)$$

$$b^{kjr}_{(x,y)} = 0 \ or\ 1 \qquad \forall k \in K,\ j \in T_k,\ r \in R,\ (x,y) \in N. \qquad (9)$$

The objective function is to maximize the system lifetime of the given sensor network configuration. The lifetime is defined as the number of rounds.

Constraint (1): The defense rate constraint and if round r satisfies defense rate constraint then enforce z_r=1.

Constraints (2)-(3): The early warning rate constraints and if satisfying early warning rate constraints then enforce z_r=1.

Constraint (4): For each sensor node s, the total sensing consumption can not exceed its initial energy level.

Constraint (5): The all possible defense strategies constraints.

Constraint (6): The total evaluation frequency constraints

Constraints (7)-(9): The integer constraints for decision variables π_{sr}, z_r, and $b^{kjr}_{(x,y)}$.

IV. SOLUTION APPROACH

Definition 3: *Check points*: The check points are virtual points in monitoring region. They are used to check coverage rate.

Definition 4: *Coverage rate*: The number of covered check points by awake sensors divided by the total number of checks points.

A. Simple Algorithm

The simple algorithm (SA) first find sensor s to cover check point a, then sensor s is awaken in the round r, and repeat the assignment process until this full coverage all check points (*coverage rate*=1).

B. Efficient Layered Defense Strategies Algorithm

In this section, we propose efficient layered defense strategies algorithm (ELDSA) for solve the problem. The algorithm includes three phases. In first phase, the “initial solution phase”, we propose a heuristic algorithm for initial defense policy. In second phase, the “objective function evaluation phase”, we propose efficient and effective simulations are conducted to evaluate the effectiveness of the current defense policy. In third phase, the “add-and-drop phase”, we use add-and-drop algorithm to improve and satisfy the defender strategies. An efficient layered defense strategies algorithm is listed in Fig. 3.

```
Algorithm EFFICIENT LAYERED DEFENSE STRATEGIES
Input: Coordinate of check points and sensor nodes, and sensing radius of sensor nodes
Output: The defense strategies of defenders ($\vec{F}$)
begin
  for $r$=1 to $max\_k$ do
  begin
    initial solution phase();                          /* phase 1 */
    for $add\_drop$ =1 to $max\_a\_d$ do
    begin
      objective function evaluation phase(); /* phase 2 */
      add-and-drop phase();                          /* phase 3 */
    end
    if ($counter_{no\_improve}$ = $no\_improve\_ub$)
      then break;
  end
end
```

Fig. 3 The efficient layered defense strategies algorithm.

1. Initial solution phase

For solve the original problem efficiency. We use the concept of “cover” to decide whether sensor *s* is awake in the round *r*. The “cover” is 1 if the check point *a* is in the sensing range of the sensor node *s* and 0 otherwise.

We introduce the concept of check point. The check point can assist to check coverage rate. Besides, it can save energy consumption because the concept can check coverage rate more efficiently for arbitrary topology, obstacle, and disjoint monitoring regions.

We first find sensor *s* to cover check point *a*, and then sensor *s* is awaken by this phase in the round *r*, and repeat the assignment process until this phase satisfies coverage rate. In addition, we must turn off redundant waked up sensor nodes in the phase.

2. Objective function evaluation phase

Since our scenario and environment are very dynamic, it is difficult to solve the problem by mathematical programming alone. The proposed evaluation process enables us to better describe the behavior of different intruders. In each intruder category, there is some randomness in the behavior of the intruders, even though they are classified as the same type.

The number of total intruders is set to the same value as *M*, which is determined by experiment. First, we select an initial value, for example, 10000. Then, if the diagram shows a stable trend, it implies that the value of *M* is ideal. Fig. 4 shows the experiment results, and *M* is set to 2000 intruders.

After deciding the value of *M* and initial solution configuration, we can apply our evaluation process to simulate behavior of intruders. Based on this, we run the evaluation *M* times with different categories of intruders to attack the core field. Then, we divide this frequency by *M* to obtain the average defense rate and average early warning rate. We take this result as the benchmark to evaluate the performance of each round.

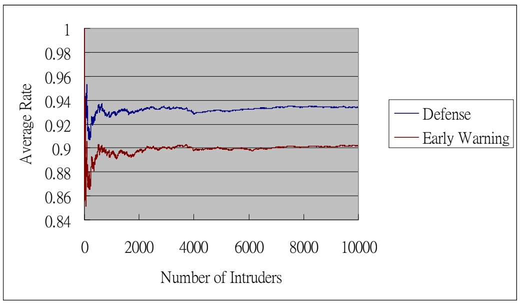

Fig. 4 Experiment results: the number of total intruders.

3. add-and-drop phase

In this phase, we improve the quality of the solution by removing wake up sensor nodes and adding sleep sensor nodes to wake up sensor nodes. Then, we run the evaluation another *M* times using the adjusted defense parameters and obtain the average defense rate and average early warning rate. Finally, we check whether one of the stopping criteria is satisfied. If it is, we terminate the procedure.

V. COMPUTATIONAL EXPERIMENTS

To evaluate the performance of the proposed algorithm, we conduct an experiment. The performance is assessed in terms of total rounds.

A. *Experiment Environment*

The proposed algorithm is coded in C under a Dev C++ 4.9.9.2 development environment. All the experiments are performed on a Core 2 Duo 2.2G Hz CPU running Microsoft Windows Vista. The algorithm is tested on a 2D monitoring region. We distribute 400 and 1600 sensor nodes (*sn*) and 100 and 400 check points (*cp*) respectively in 2D monitoring region 1000×1000 and 2000×2000 m^2. The radius of different sensors types (s_a, s_b) is (100, 200). The energy consumption of aware different sensor types (s_a, s_b) is (1, 4) in each round.

Before the evaluation process, we need to determine the value of *M*. Therefore, we run a number of experiments to find the proper value for our scenario. In Fig. 4 illustrates that the diagram shows a stable trend in *M*=2000. Hence, we set *M* as 2000. The ratio of airborne intruders is listed in Table IV.

TABLE IV
RATIO OF AIRBORNE INTRUDERS

Types of Intruder	Ratio
Airborne Intruders	20%
Non-airborne Intruders	80%

B. *Experimental Results*

Fig. 5 shows the comparison of the number of rounds in different nodes and different scenarios. Fig. 6 shows the comparison of the number of rounds in airborne intruders.

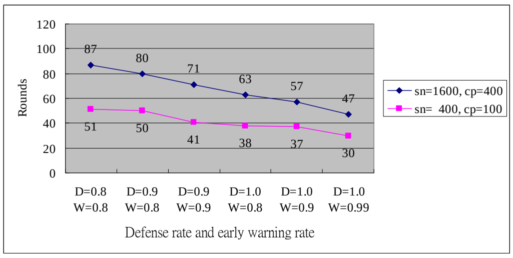

Fig. 5 The comparison of the number of rounds in different nodes and different scenarios.

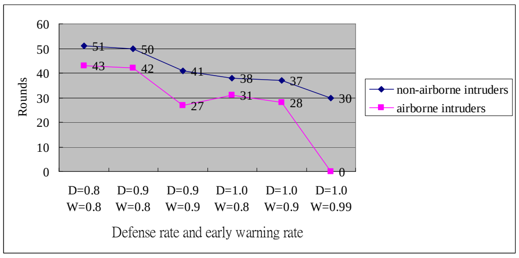

Fig. 6 The comparison of the number of rounds in airborne intruders. (*sn*=400, *cp*=100, and airborne ratio=0.2).

C. Discussion

The results show that the lower defense rate and lower early warning rate have higher rounds, and the airborne intruder cases have lower rounds than non-airborne intruder cases.

The proposed approach can prolong system lifetime by lower defense rate and lower early warning rate, as shown in Figs. 5 and 6. In large region of lower defense rate has higher rounds than small region in Fig. 5, because large scale region has larger depth. Therefore, defenders can use lower density of sensors to cover monitoring region. In Fig. 6 case of airborne intruders, the rounds is 0 in *D*=1 and *W*=0.99, because airborne intruders randomly drop in monitoring region. Therefore, the distance of early warning rate can not be satisfied.

Table V shows the maximum total number of rounds calculated by different algorithms. We can see that the ELDSA outperforms the SA.

TABLE V
THE IMPROVEMENT RATIO WITH SIMPLE ALGORITHM (*D*=1, *W*=0.99)

Number of nodes (*sn*, *cp*)	ELDSA	SA	Improvement Ratio to Simple Algorithm
(400,100)	47	18	161%
(1600,400)	30	16	88%

The results show that the algorithm is better than the simple algorithm. The proposed ELDSA can improve the percentage of energy consumption from 88% to 161%.

VI. Conclusion

This study proposes an efficient layered defense strategies algorithm for wireless sensor networks of grouping capabilities. To our best knowledge, the proposed algorithm is truly novel and it has not been yet discussed in previous researches. The study first formulates the problem as combining mathematical programming problem, and then proposes a heuristic-based algorithm for solving the optimization problem.

We find the maximum *K* groups of sensors for layered defense subject to defense rate, early warning rate, battery capacity, intruder behavior, and defender strategies constraints. The mechanism can prolong the system lifetime and provide lead time alarms. A novel three-phase solution approach, which well combines mathematical programming and simulation techniques, is proposed. Compared with SA, the proposed ELDSA can improve system lifetime since the improvement ratio is from 88% to 161%. Therefore, the experimental results showed that the proposed efficient layered defense strategies algorithm (ELDSA) gets applicability and effectiveness in the layered defense for grouping capabilities.

Our main contribution is that we combine mathematical programming with simulations and develop a novel approach to solve the problem with the imperfect knowledge property. This mechanism helps us prolong the system lifetime of layered defense in WSNs.

As to the next step, we plan to further investigate mobile capabilities model based on layered defense application requirements and heuristic algorithms [4], [5]. In addition, we are looking into the tradeoff of total number of rounds with various system issues, such as mobile capabilities, etc.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Wireless sensor network," *IEEE Communication Magazine*, pp. 102-114, August 2002.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor network: a survey," *Computer Networks*, vol. 38, pp. 393-422, 2002.

[3] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Communication and Mobile Computing*, pp. 483-502, 2002.

[4] G. Wang, G. Cao, T. L. Porta, and W. Zhang, "Sensor Relocation in Mobile Sensor Networks," *IEEE INFOCOM*, vol. 4, pp. 2302-2312, March 2005.

[5] Y. Yoo and D. Agrawal, "Mobile Sensor Relocation to Prolong the Lifetime of Wireless Sensor Networks," *IEEE Conference on Vehicular Technology*, 2008, pp. 193-197, 2008.

[6] W. Yun, W. Xiaodong, X. Bin, W. Demin, and D.P. Agrawal, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 698-711, 2008.

[7] G. Li, J. He, and Y. Fu, "A Group-Based Intrusion Detection Scheme in Wireless Sensor Networks," *The 3rd International Conference on Grid and Pervasive Computing Workshop*, pp. 286-291, 2008.

[8] G. Li, J. He, and Y. Fu, "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks," *The 28th International Conference on Distributed Computing Systems Workshops*, pp. 309-314, 2008.

[9] Y. Wang, Y.K. Leow, and J. Yin, "Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," *International Conference on Parallel and Distributed Systems*, pp. 564-571, 2009.

[10] P.L. Chiu and F.Y.S. Lin, "Sensor Deployment Algorithms for Target Positioning Services," *Doctoral Thesis, Graduate Institute of Information Management of National Taiwan University*, 2007.