International Journal of Security and Its Applications
Vol. 11, No. 4 (2017), pp.11-26
http://dx.doi.org/10.14257/ijsia.2017.11.4.02

An Improved Dendritic Cell Algorithm Based Intrusion Detection System for Wireless Sensor Networks

Weipeng Guo[1] and Yonghong Chen[2]

[1,2] College of Computer Science & Technology, Huaqiao University, China
[1]fyman_gwp@163.com, [2]djandcyh@163.com

Abstract

Base on the similarities between WSNs intrusion detection and artificial immune system. This paper utilizes the benefits of one of the Danger Theory based AIS intrusion detection algorithms, namely the Dendritic Cell Algorithm (DCA) to design a distributed and hierarchical intrusion detection model for WSN. Beside, because of the shortcomings of DCA about its Dendritic Cell (DC) evaluation mechanism and lymph decision mechanism, the false alarm rate is high. Therefore, this paper puts forward an improved Dendritic Cell Algorithm reference to the idea of data fusion theory. In this algorithm, we firstly define a scoring function to evaluate the DC context in DC part. And then in lymph part, we fuse multiple DCs' evaluation through Dempster rule to make global decision. The experimental results show that the improved DCA based IDS proposed can effectively improve the accuracy rate without depending on the MCAV threshold and show advantages in flexibility and adaptability.

Keywords*: WSNs, IDS, Danger theory, DCA, Improved DCA*

1. Introduction

Wireless sensor networks (WSNs) have been widely used in military, environmental monitoring and other business applications since their flexibility, low cost and distribution [1]. However, owing to the resource constraint and wireless communication characters in wireless sensor networks, it has been suffered from various attacks [2]. Beside, due to the distributed and resource constrained features of WSNs, the security mechanism in WSNs is more challenge than in traditional network. Therefore, it is necessary to study a distributed and lightweight intrusion detection mechanism for WSNs.

In WSNs, IDS should be kept simple, distributed and lightweight, favoring algorithms that demand low memory, low computation and low energy consumption [2-3]. With this aim in mind, many researchers working on developing new methodologies for intrusion detection in WSNs [3]. At present, intrusion detection for WSNs based on the artificial immune system(AIS) has been proposed[4-7], for it is considered a promising approach for IDS implementation in WSNs, since networks security tasks have great similarities with AIS concerning the need of maintaining system stability in a highly changing environment. Some of the AIS's main features, such as self-organization, adaption and fault tolerance, are similar to the wireless sensor networks desired characteristics [5, 8].

In this paper, we focus on the immune Danger Theory which implies that the concentration of the danger or safe signals which come from the body tissues and caused by specific antigens control the response of the Immune System [8]. As an effective danger theory algorithm, dendritic cell algorithm[9] that based on the features of dendritic cell has already been used in the intrusion detection in WSN and achieved a higher detection rate [4-5, 10]. As stated by Kim *et al.* [4], the properties of danger theory based AIS intrusion detection algorithms, especially DCA can meet the security requirements of sensor networks environment as a distributed, limited power and limited capacity wireless sensor networks.

ISSN: 1738-9976 IJSIA

Nevertheless, the DCA suffers from some shortcomings [12] when utilized in WSN intrusion detection. The first drawback is the crisp separation between semi-mature(normality) and mature (abnormality), in DC evaluation phase of the DCA, it evaluates the antigen context by the way of voting, either semi-mature(normality) and mature (abnormality), which can change the decision of the context affection and has a negative effect on the detection accuracy. The second drawback is the lymph decision phase of the DCA. It depends on the MCAV abnormal threshold seriously. However, it is hard to set the MCAV threshold reasonable, while setting too small will result in a high false alarm rate and high false negative rate in contrast. These drawbacks have resulted high false alarm of the intrusion detection in wireless sensor networks [11]. And the dependence of the MCAV abnormal threshold also makes the detection system lacking of flexibility.

In this paper, a new improved DCA algorithm is proposed to design intrusion detection system for WSN. Firstly, in DC part of the DCA, we propose a scoring function to evaluate the antigen context, and present the evaluation result to the lymph in a more detail way--scoring. Presenting the possibility of normal, abnormal and uncertainty to the lymph. And then in lymph part, utilizes the Dempster rule [13] to fuse multiple sources of evaluations to make global decision. Through the new evaluation way, the crisp separation between DCs' contexts (semi-mature and mature) can be alleviated. And by the way of using D-S evidence fusion rule to make decision, we can avoid the dependence on the MCAV threshold and shows more flexibility.

Based on the new algorithm, an architecture of IDS for WSN that based on the improved DCA is proposed. Sensor nodes in the network are divided into two roles: sensor-DC and sensor-Lymph, nodes cooperative to detect intrusion.

The experiments in this paper show that compare to the traditional DCA and SNS model based intrusion detection system, the improved DCA based intrusion detection system can effectively reduce the false alarm rate and at the same time, avoid the dependence on MCAV anomaly detection threshold, and show advantages in flexibility and adaptability.

The remainder of this paper is organized as follows. In Section 2, related works of the immune based intrusion detection for WSN is discussed. In Section 3, detail of the DCA is described and the improved algorithm are proposed. In Section 4, the proposed IDS is described. And in Section 5, different experiments and their results are analyzed. Finally, our conclusions and future work are presented in Section 6.

2. Related Works

AIS is considered a promising approach for IDS implementation in WSNs, since networks security tasks have great similarities with AIS concerning the need of maintaining the system stability in a highly changing environment [4-9]. In this section, a literature review of AIS based IDS in WSNs will be introduced.

Drozda *et al.* [6] took the Self-non-Self (SNS) model into wireless sensor network intrusion detection to solve the problem of wormhole, packet drop and packet forwarding delay. The proposed IDS were based on the Negative Selection Algorithm(NSA), however, owing to the shortcoming of NSA, the proposed method have high false alarm rate, and great computational resource is required, which can't meet the requirement of WSN. Beside, in order to get the global information, promiscuous mode was set for each node to monitor the traffic of the network. In this way, the node can get the global information, however, it prevents the node to sleeping mode, forces the node to work in receiving state, which extremely consume the energy.

Greensmith *et al.* [14] took the danger theory of dendritic cell algorithm into intrusion detection, DC cooperative with T cell to make immune response. The paper abstracted DCs' feature to design dendritic cell algorithm, and applied it to detect port scanning

attack over wired network. Kim *et al.* [4-5] continued Greensmith's work, proposed a DCA implementation to a WSN. Implying that the properties of danger theory based algorithms, especially DCA can meet the security requirements of sensor networks. This IDS allowed to detect a new type of attack called "interest cache poisoning attack" that occur in a WSN environment. However, it utilized the cache information in local only, not considering the global information which is far from enough to intrusion detection in WSN.

Helio *et al.* [10] used the danger theory and a customized DCA to perform the anomaly detection of attacks in WSN. The IDS was distributed among the sensors, where the sensors were assumed different roles from the features of HIS. It is not necessary to install the whole IDS in all nodes of the network. Node playing the DC role collect the parameter values requested by the intrusion detection manager and, when executing the DCA, send message that represent the migration of a DC either in the mature(danger) or the semi-mature(safe) state to the node playing the lymph node role. In lymph node, calculating the MCAV and decide whether is attacked or not according to the MCAV decision threshold. The experiments showed that the DCA based AIS intrusion detection algorithm have high detection rate. However, the false alarm rate is high, and depend on the MCAV decision threshold seriously.

It is obviously that recently, some of the research on IDS based on AIS for WSN took the sensor node as the whole body of immune system without considering the limitation of sensor node [6-7]. However, it is not suitable to install the whole IDS on a resource constrain sensor node. On the other side, some of the current researches introduce promiscuous mode to get global information, which is energy inefficient because it prevents the wireless interface from entering sleep mode, forcing it into either idle or receive mode. According to [15], power consumption in idle and receive modes is about 12-20 higher than in sleep mode.

With the respect to the above reviews work, in this paper, our aim is to design a distributed and hierarchical intrusion detection model in WSNs as a suitable metaphor for the danger theory based Dendritic Cell Algorithm. And proposed an improved DCA based on D-S evidence fusion theory to intrusion detection. Details will be discussed in the follows.

3. Improved Dendritic Cell Algorithm

Dendritic Cell Algorithm is one of the most well-known Danger Theory algorithm, which is abstracted from immune dendritic cell by Greensmith *et al.* [9] and has been subject to various modifications [12]. In this section, detail about DCA will be introduced and an improved DCA based on D-S evidence fusion theory will be proposed to solve the problems of traditional DCA.

3.1. Dendritic Cell Algorithm

Dendritic cells are types of antigen-presenting cells. They are sensitive to the concentration of signals(PAMPs, Danger and Safe) received from local or their neighborhood. Hence, resulted in three different maturity level. The first maturation state of a DC is the immature state(iDCs). iDCs differ either to a full or partial maturation state. It depends on the combination of the various signals received. Under the reception of safe signals, iDCs migrate to the semi-mature state and they cause antigens tolerance. iDCs migrate to the mature state if they are more exposed to danger signal and PAMP than SS. They present the collected antigens in a dangerous context.

Dendritice Cell Algorithm introduced by Greensmith *et al.* [9] abstracted a number of properties of DCs that are possibly advantageous to design AIS for anomaly detection. The DCA is capable of adhering several signals and antigen to fix the context of each object (DC). The input signals of the system are pre-categorized as "PAMP", "danger"

and “safe”. Likely in biology, PAMPs definitely indicate an anomalous situation. Danger signals are the indicators of abnormality but with lower value of confidence than PAMPs signal. Safe signals are indicators of normality generating a tolerance to the collected antigen. These signals are processed by the algorithm according to equation (1) in order to get three output signals: co-stimulation signal (csm), semi-mature signal(semi) and mature signal (mat). Where W_P, W_D, W_S are the weight shown as Table.1

$$O_{[csm,semi,mat]} = \frac{(W_P \times P) + (W_D \times D) + (W_S \times S)}{|W_P| + |W_D| + |W_S|} \quad (1)$$

Table 1. Suggested Weight Used for Equation(1)

Weight	csm	semi	mat
W_P	2	0	2
W_D	1	0	1
W_S	2	3	-3

A migration threshold is incorporated into the DCA in order to determine the lifespan of a DC. As soon as the ∑CSM exceed the migration threshold, the DC ceases to sample signals and antigens. The DC differentiation direction is determined by the comparison between ∑semi and ∑mat. If the ∑semi is greater than the ∑mat, then the DC goes to semi-context (context=0), which implies that the antigen data is collected under normal conditions. Otherwise, it goes to mature context(context=1), signifying a potentially anomalous data item.

Then this DC migrates to the lymph to make aggregation. The response is determined by measuring the number of DCs that are fully mature and is represented by the value: MCAV(the mature context antigen value). The MCAV is used to evaluate the degree of anomaly of a given antigen. It is clear that the closer the MCAV is to 1, the greater the probability that the antigen is anomalous. By applying thresholds at various levels, analysis can be performed to assess the anomaly detection capabilities of the algorithm. Those antigens whose MCAV are greater than the anomalous threshold are classified into the anomalous category, while the others are classified into the normal category. For a detailed description of the DCA and its pseudo-code, we kindly invite the reader to refer to paper [9].

3.2. Limitations of the Original Dendritic Cell Algorithm

Although DCA can meet the security requirements of sensor networks environment as a distributed, limited power and capacity wireless sensor networks [4]. Nevertheless, the DCA suffer from some shortcomings about its DC evaluation and lymph decision mechanism.

Firstly, the drawback of DCA is the result of an environment characterized by a crisp separation between normality(semi-mature) and abnormality(mature). As mention above, in DCA’s evaluation phase, DC evaluates the antigen context by the way of voting, either normal (semi -mature) or abnormal (mature). However, if the difference between these two DC’s contexts is small, then the context of the DC will be hard to be defined. Thus, it could change the decision of the context affectation. Especially in WSN, the information is incompleteness and uncertainty. Ignoring this case will have a negative effect on the accuracy.

Secondly, when it come to the decision phase in lymph, the mature context antigen value(MCAV) is used to assess the degree of anomaly of the context. However, it is difficult to set the MCAV threshold reasonable, while setting too small will result in a

high false alarm rate and high false negative rate in contrast. Beside, we can't setting a fix MCAV abnormal threshold that suitable for various strength of attacks.

In this paper, considering the shortcomings of DCA and characteristics of IDS in WSN, a new developed DCA based on the D-S evidence theory is proposed to optimize the evaluation mechanism and decision mechanism. A powerful feature of the D-S theory in such a distributed detection system is its usefulness in combining evidence provided by different observers. Details about the D-S evidence theory will be introduced in the next section.

3.3. D-S Evidences Theory

The Dempster-Shafer's (D-S) Theory of evidence was first formulated by Shafer [13]. This theory can be considered as a generalized Bayesian theory. It can be interpreted from either a probabilistic or an axiomatic point of view [17]. It has been applied in the fields of statistical inference, diagnostics, risk analysis, and decision analysis.

D-S Theory is the theory based on the non-empty finite field Ω, where Ω is regarded as the frame of discernment, representing the finite system status $\{A_1, A_2...A_n\}$ and the elements are independent. The goal of D-S theory is to inference the status of system according to the evidence$\{E_1, E_2...E_n\}$ from the observation of the system. Here are a few related concepts:

A. Definition of Basic Probability Assignment(BPA)

Each status is assigned a value by an observer from the mass probability function *m*, which is defined as:

$$m: 2^{\Omega} \to [0,1]$$

And satisfies with the following conditions:

$$m(\Phi) = 0$$

$$m(A) \geq 0, \forall A \subseteq \Omega$$

$$\sum_{A \subseteq \Omega} m(A) = 1$$

Then function *m* is treated as the Basic Probability Assignment(BPA);and *m(A)* named the basic probability, indicates the degree of confidence in the set A, the A is namely focal elements when $m(A)>0$.

B. Definition of D-S Evidence Fusion Rule

The core of D-S evidence theory is the rule to fuse multiple evidences. It is known as Dempster rule. Assume m_1 and m_2 is the BPA of two different evidence, then the BPA of the fusion of m_1 and m_2 is:

$$m_1(A) \oplus m_2(A) = K^{-1} \sum_{B \cap C = A} m_1(B) m_2(C) \text{ when } A \neq \varnothing \tag{2}$$

Where *K* is the normalization factor.

Then we can fuse n evidence through Dempster rule as follow:

$$m_{1..n}(A) = K_n^{-1} \sum m_1(A_1) m_2(A_2) .. m_n(A_n) \qquad when A \neq \phi$$

$$K_n = \sum_{\cap A_i = A} m_1(A_1) m_2(A_2) .. m_n(A_n) \tag{3}$$

Research [17] have been proved that in the case of frame of discernment have only two exclusive elements, such as anomaly detection, which just need to distinguish normal and abnormal, the Dempster rule meets the associative law:

$$m_{1..n}(A) = m_{1..n-1}(A) \oplus m_n(A) \tag{4}$$

Based on this, we can inference through mathematical induction:

$$m_{1..n}(A) = m_1(A) \oplus m_2(A) \oplus .. m_N(A) \tag{5}$$

Beside, voorbraak *et al.* [18] proposed an approximate calculation idea to decrease the computational complexity of D-S fusion rule. The idea indicated that we can simplified calculation through reduce the number of focal elements. It is useful for the condition that only care about the elements in the frame, but not the subset of the plurality of elements as the result, such as abnormal detection.

3.4. Improvements of Dendritic Cell Algorithm

In this section, measures based on the idea of D-S Theory of evidence will be proposed to solve the questions proposed above. We will introduce the improvements of DC evaluation phase and Lymph decision phase, respectively.

3.4.1. Improved the DC Evaluation Phase

Firstly, in this paper, the evaluation mechanism of DC is changed from the way of "voting" to "scoring". A scoring function is defined to evaluate the status of DC when DC reach the migrate threshold according to the value of (∑mat-∑semi). In this way, when DC migrate to the lymph, it will no longer voting whether the antigen collected is normal or not, but to presenting the possibility of the status in normal and abnormal according to the evaluation of DC.

A. Definition of Scoring Function

The scoring function in this paper is regarded as the BPA function in D-S theory. According to the description of D-S Evidence Theory, we firstly define the frame of discernment.

Since we are interested in whether the DC is under attack(abnormal) or not(normal), the frame of discernment Ω is defined as $\{N, A\}$, where N is normal, A is abnormal, and $N \cap A = \emptyset$.

The scoring function $\boldsymbol{S}$ is regarded as the basic probability assignment function. Therefore, the $\boldsymbol{S}(A)$ indicates the degree of abnormal, and $\boldsymbol{S}(N)$ indicates the normal degree. To decrease the computational complexity, $\boldsymbol{S}(\{N, A\})=0$. As a BPA function, the scoring function is responsible for mapping a large range of data to the interval [0, 1]. Therefore, in this paper, we choose the *S-Curve* function $y(x)$ as the scoring function $\boldsymbol{S}(A)$.

$$y(x) = \frac{1}{1 + \exp(-A \times (x - C))} \tag{6}$$

It is important to note that the parameter "A" determines the slop of curve. The bigger the value is, the steeper the slop of the curve is; parameter "C" determines the center of curve. In this paper, we adaptively adjust the shape of the curve through adjusting the parameter A and C. We use the steepest descent algorithm as follows to train the parameters.

Define the Cost function:

$$E(x) = (y_d - y)^2 \tag{7}$$

Where y_d is the desired value of intrusion probability, y is the actual value.

$$C(k+1) = C(k) + \alpha \times \frac{\partial E}{\partial C} \tag{8}$$

$$A(k+1) = A(k) + \alpha \times \frac{\partial E}{\partial A} \tag{9}$$

Where

$$\frac{\partial E}{\partial C} = 2(y_d - y) \frac{-A(k)\exp\{-A(k)\times[x - C(K)]\}}{\{1+\exp\{-A(k)\times[x - C(k)]\}\}^2} \tag{10}$$

$$\frac{\partial E}{\partial A} = 2(y_d - y) \frac{A(k)}{\{1+\exp\{-A(k)\times[x - C(k)]\}\}^2} \tag{11}$$

Where α is the training factor. Its value locate between 0 and 1;
Since ***S(A)*** indicate the abnormal degree, the normal degree is ***S(N)=1-S(A)***.

B. New Evaluation way of DC

When DC reach the migrate threshold, it will no longer voting whether the DC is differential to semi-mature (normal) or mature (abnormal). In our improved DCA, each DC is treated as a source of evidence, based on the value of $\sum mat$-$\sum semi$, the possibility of abnormal and normal of the DC status will be calculated utilizing the scoring function proposed above. A message containing the possibility of abnormality and normality will be sent to the lymph as the source of evidence.

3.4.2. Improved Lymph Decision Phase

As mention above, in traditional DCA, the decision depend on the MCAV anomaly threshold seriously. Beside, the new evaluation way of DC proposed above make the MCAV not suitable to describe the abnormality anymore. Therefore, a new decision method is proposed.

In this paper, considering the working principle of DCA and D-S evidence theory, the DC's evaluation of the environment is treated as the source of evidence, and in lymph using the Dempster rule as below to fuse multiple evidences to make comprehensive evaluation.

$$m_{1..n}(A) = m_1(A) \oplus m_2(A) \oplus \ldots \oplus m_n(A) \tag{12}$$

Then we can make a decision through the max value of the confidence of normal and abnormal. As Dempster fusion rule has been considered more detail information than in traditional, it is more reasonable than the simple calculation of the abnormal proportion. At the same time, avoiding the dependence of MCAV anomaly threshold.

3.5. New Dendritic Cell Algorithm

The new improved DCA is divided into two parts: DC part and Lymph part. According to the improvements proposed above, each DC act as the source of evidence. Firstly, in DC part, DC evaluating the context of DC utilizing the scoring function. Presenting the evaluation result that contains the possibility of the status in normal and abnormal as the evidence to the lymph. Then in lymph making decision according to the evidence fusion theory.

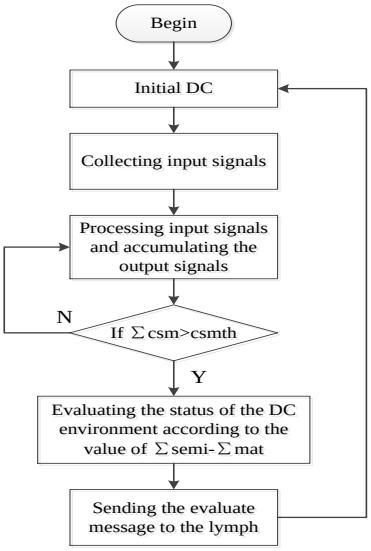

Figure 1. Flow Chart of DC Part of the Improved DCA

Figure 1 show the flow diagram of the DC part of the new improved DCA. The steps in DC part are as follows:

1) Initializing the DC population and parameters;
2) Collecting the input signals: PAMP, Danger Signal, Safe Signal. Normalizing these signals;
3) Processing the input signal according to formula (1) to get output signals: CSM, Semi, Mat. And accumulate the output signals;
4) Repeating step2 and step3 until ∑CSM exceeding the migrate threshold.
5) Calculating the possibility of the DC status of normal(***S****(A)*) and abnormal (***S****(N)*)according to the scoring function;
6) Presenting the evaluate result to lymph node and then, restarting the execution cycle.

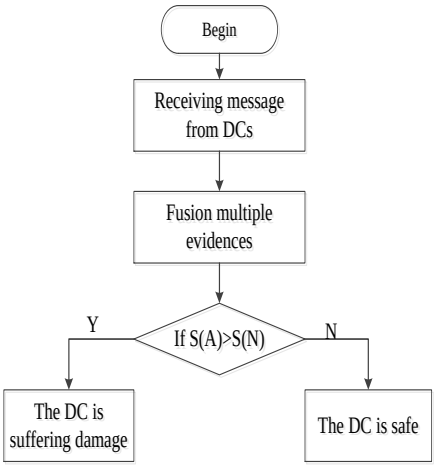

Figure 2. Flow Chart of Lymph Part of the Improved DCA

Figure 2 show the flow diagram of the Lymph part of the improved DCA. The steps in lymph part are as follow:

1) Receiving the evaluation results presented by DCs;
2) Using Dempster rule to aggressive the evidences provided by different DCs to get comprehensive evaluation.
3) Making decision according to the comprehensive evaluation. If *S(A)>S(N)*, then marking as abnormal and sending an alert message.

4. Improved DCA Based Intrusion Detection System

From the standpoint of the resources friendly and to improve the detection performance, it is not suitable to run a complete intrusion detection system on a single node. In this section, a distributed and hierarchical intrusion detection system model that based on our improved DCA is proposed.

4.1. Architecture of Hierarchical Wireless Sensor Networks

As shown in Figure 3, the wireless sensor network consists of several sensor nodes and a Base Station(BS). A hierarchical and distributed intrusion detection system that divided into three levels: intrusion detection manager subsystem, cluster head detection subsystem and local detection subsystem is constructed around the whole networks.

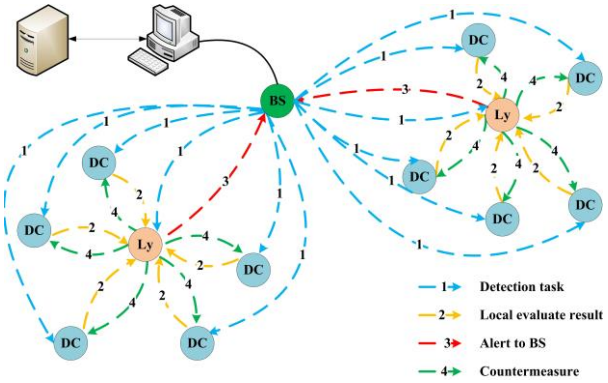

Figure 3. Wireless Sensor Networks Intrusion Detection System

Nodes in the network cooperatives to detect intrusion. According to the new improved DCA, in the hierarchical intrusion detection system, sensor nodes in the network are divided into two roles: sensor-DC and sensor-Lymph. Sensor-DC manage the local intrusion detection subsystem, sensor-lymph manage the cluster head detection subsystem and the BS manage the intrusion detection manager subsystem.

According to the improved DCA, Sensor-DC distributed in the network, collecting the signals to sense danger, and presenting the local evaluation of the context as the evidence to sensor-Lymph. Sensor-Lymph is responsible for gathering the evidences presenting by the sensor-DCs to make global decision. And the BS is responsible for organizing the intrusion detection tasks and combating the identified attacks.

4.2. Logical Architecture of IDS

According to the hierarchical architecture introduced above, an improved DCA based intrusion detection system for wireless sensor networks learning from the common framework of IDS [20] is shown as Figure 4.

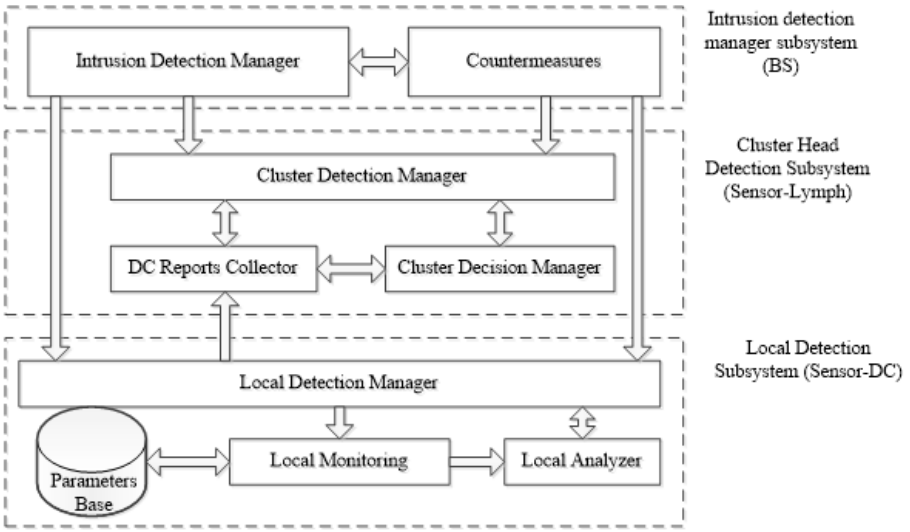

Figure 4. IDS Logical Architecture

The framework consists of several components, namely Intrusion Detection Manager, Cluster Detection Manager, DC reports Collector, Cluster Decision Manager, Countermeasures, Local Detection Manager, Local Monitoring, Parameters Base, Local Analyzer, and are divided into three layer.

The first layer is the local detection subsystem operated by the sensor-DC. It executing the DC part of the improved DCA proposed above. It collecting the input signals and analyzing the status of the sensor-DC as a source of evidence according to the scoring function. The Local Detection Manager, Local Monitoring, Local Analyzer, and Parameters Base are installed in this subsystem.

The Local Detection Manager is responsible for managing the detection task of the sensor-DC. It receiving the detection task from the BS.

The Local Monitoring component is responsible for collecting the values of the parameters defined by the parameter base according to the detection task, such as the energy consumption rate, which is used to detect DOS attack.

The Local Analyzer executing the DC part of the improved DCA. It utilizing the scoring function to evaluate the status of the DC by the collected signals. And presenting the possibility of the normal and abnormal as the evidence to detection manager;

The Parameters Base managing a table which contains the attack type, attack parameters list and for each parameter, a means and standard deviation.

The second layer is the cluster head detection subsystem operated by the sensor-Lymph, where the lymph part of the improved DCA is executed. It collecting multiple evidences from sensor-DC, and combining evidences to make global decision. It consist of Cluster Detection Manager, DC reports Collector and Cluster Decision Manager.

The Cluster Detection Manager is responsible for managing the detection task of the sensor-lymph. It receiving the detection task from the BS and organizing the detection task;

The DC reports Collector is responsible for collecting the evaluation message from sensor-DC. Then presenting the evaluation message to the decision manager component;

The Cluster Decision Manager executing the lymph part of the improved DCA. It combining multiple evidences proposed by different sensor-DC in the cluster to make global decision.

The third layer is the intrusion detection manager subsystem operated by the Base Station. It consist of the Intrusion Detection Manager and Countermeasures components.

The Intrusion Detection manager is the central component of the model, which organizing the detection tasks and coordinating actions and responses to other managers;

The Countermeasures component is responsible for combating the identified attacks. Countermeasures are direct actions performed on a node or action demanding information sent to the administrator.

5. Experimental Results and Analysis

In this section, we will describe simulations performed to analyze the efficiency of the proposed IDS that based on the improved DCA. We will verify the advantages of the improved DCA using in the WSN intrusion detection by analyzed the performance of the model in detection rate, false alarm rate, and flexibility, compare to the traditional DCA and SNS based intrusion detection system.

5.1. Simulation Settings

In our experiments, the Network Simulator(NS-2) is used to evaluated the system performance. It provides an excellent environment to simulate wireless sensor network. Figure 5 show the scenario of simulated wireless sensor network.

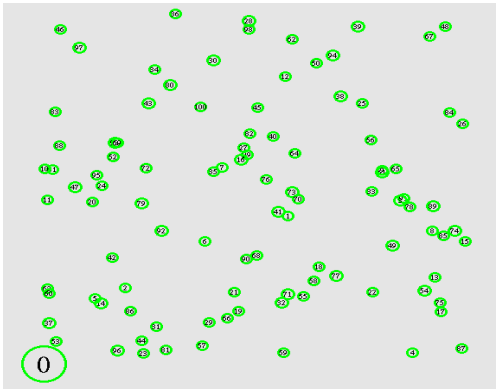

Figure 5. Simulation Scenario of Wireless Sensor Networks

The implementation environment is listed in Table 2. The simulated network consists of 100 nodes randomly distributed in a field of 100m*100m and a Base Station is located in (0, 0). Each sensor node has a transmitting range of 50 meters and send data packet to the base station periodically(every 2 s). We use LEACH protocol as the routing protocol for it is a cluster based protocol which is suitable for our hierarchical model. Considering the balance of energy consumption, 10% of the nodes is selected as the cluster head.

The total simulation time is 3600 sec. At the beginning, the network has a period of 200 to set up the network. After this period, adversaries start their attacks. The attacks randomly execute every 10 second with attacks beginning at 200s.The intrusion is achieved by a Jamming attack, which is a DoS attack of the wireless sensor network. Attackers broadcasting worthless packets in the wireless sensor network periodically to hamper the communication between nodes in the network. It hampers the wireless communication and consumes the energy seriously. In this paper, various strength of attacks will be simulated to analyze the performance of the IDS proposed. All the results shown in this paper are average of 10 repeated experiments.

Table 2. Implementation Environment

Item	value
Simulation	3600s
Number of Nodes	100
Transmitting Range	50m
Simulation Area	100m*100m
Routing Protocol	LEACH

According to W. Xu in [9], metrics such as signal strength, packet delivery ratio and energy consumption rate are used to detect jamming attacks. In order to detect the attack, in our improved DCA based intrusion detection system, the input signals for sensor-DC are defined as follows:(i) the PAMP signal is defined as the energy consumption ratio of the sensor;(ii) the Danger signal is obtained by calculating the incoming messages rate received by the node; and (iii) the Safe signal is defined as the inverse of the variation of the incoming messages rate received by the node.

To estimate the performance of the improved DCA based intrusion detection system for wireless sensor networks, three important formulas are used to evaluate system efficiency: detection rate (DR), false positive rate (FPR). The ADR represents the number of attacks that the IDS has detected out of the total number of attacks. The FPR represents the number of normal process that the IDS has misclassified.

5.2. Detection Performance

Detection rate and false alarm rate are used as detection performance metrics. In this section, setting the broadcasting interval *t=0.5s*, various number of attackers, from 1 to 10 attackers, are generated randomly in the network. Figure 6 and Figure 7 illustrate the detection rate and false positive rate of our improved DCA based intrusion detection system and other model proposed in other works.

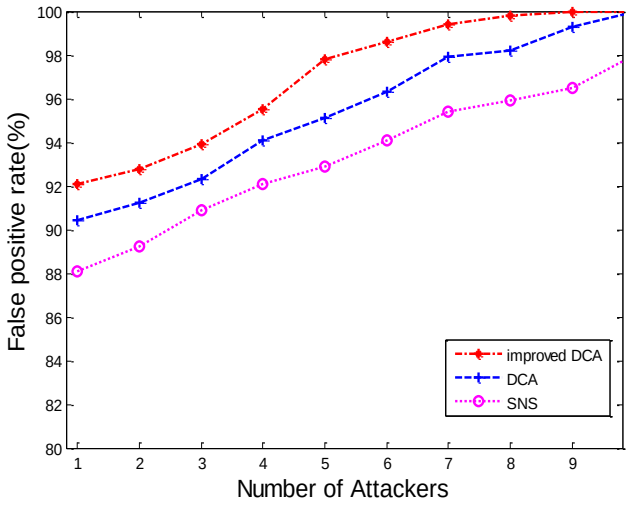

Figure 6. Detection Rate

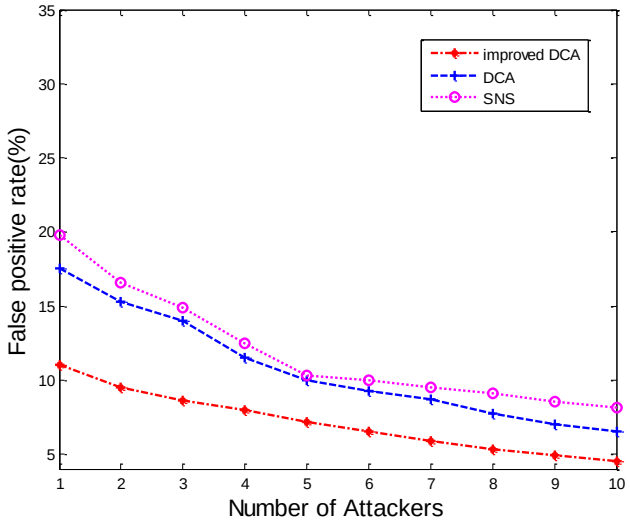

Figure 7. False Positive Rate

From Figure 6, it is apparently that the improved DCA proposed in this paper has an advantage than traditional DCA and SNS model based method. We can see that with the increase of the number of attackers, the effect of the attack get strong, so that the detection rate become higher. However, when the strength of attack is small, the difference between the normal and abnormal is inconspicuous that it is difficult to distinguish accurately, so that detection rate is stay at a lower level. But it is obvious that under few attackers, the method proposed in this paper has a higher detection rate compare to other methods, for it has the ability to integrate global knowledge to detect anomaly.

From Figure 7 we can see that when the attack strength is small, the false positive rate of the SNS model based IDS proposed in [7] is higher relatively followed by the traditional DCA based model. And the improved DCA based model proposed in this paper is stay at a lower level. That is because of the danger model based intrusion detection system exist two level of verification. In the first level, node sensing damage and sending an evaluation result as evidence of the attack to the second level to make global decision so that it can reduce the false alarm rate. Beside, compare to the traditional DCA, the improved DCA has better performance for the way of "scoring" in evaluation phase which is more details than the way of "voting" in traditional DCA.

5.3. Flexibility and Adaptability

However, the cunning attackers always find the ways to disguise attack behaviors to normal. It requests the detection method with high flexibility and adaptability to detect the deceiving anomalies. In this section, we will simulate this kind of situation to analysis the flexibility and adaptability of the model proposed. In this scenario, there is only one attacker exist on the network. The broadcasting interval t is various from 0.1s to 2s, which is more and more similar to the normal behavior.

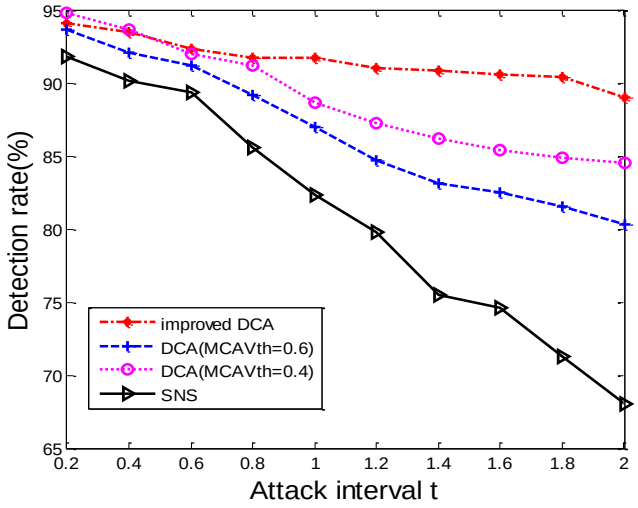

Figure 8. Detection Rate under Different Attack Intervals

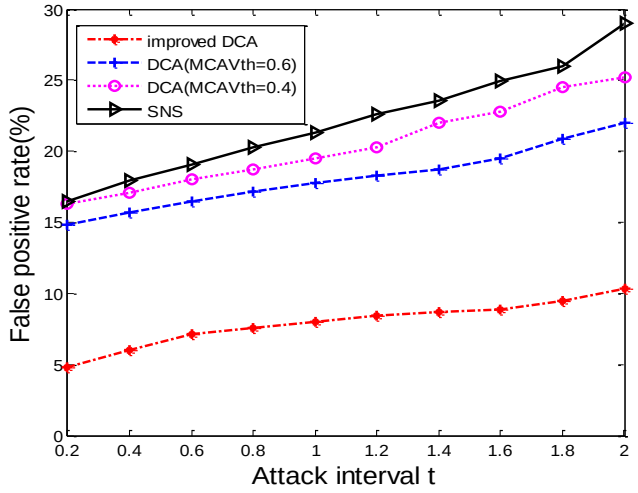

Figure 9. False Positive Rate under Different Attack Intervals

Figure 8 and Figure 9 show the detection rate and false positive rate under this scenario. We can see that when the broadcasting interval approaches to the normal traffic interval, the method proposed in this paper can keep higher detection rate and lower false alarm rate. SNS model based method detect the intrusion by the detectors generated by NSA, which has the problem of "black hole", that the performance degraded when the attack similar to normal. As for traditional DCA based method, we can see that the detection performance depending on the MCAV threshold seriously. It can be seen that the smaller the MCAV anomaly threshold is, the higher the detection rate. However, with the higher of false alarm rate. We can't set a fix MCAV threshold that suitable to various attacks. In other word, the flexibility and adaptability of traditional DCA based intrusion detection system is poor. While in our improved DCA based method, the way of scoring in DC's evaluation and the utilization of the Dempster rule in lymph's decision phase add flexibility and adaptability to detection performance.

6. Conclusion

To overcome the shortcomings of the original DCA about its DC evaluation phase and lymph decision phase, in this paper, we had proposed a new improved DCA based on the idea of the DS evidence theory. In our approach, a scoring function has been defined to evaluate the status of the DC and in lymph, combining multiple evidences proposed by DC through Dempster rule. Beside, a hierarchical intrusion detection system for WSN has been proposed based on the improved DCA. Nodes in the sensor networks were divided into sensor-DC and sensor-Lymph, cooperative to detect intrusion. Compare to other AIS based intrusion detection system, the experiments in this paper showed that the algorithm proposed can effectively reduce the false alarm rate and at the same time, avoiding the dependence on MCAV anomaly threshold, and show advantages in flexibility and adaptability.

In the next step, different attack will be analyzed, simply by choosing appropriate input signals for their identification. We also intend to cooperative the adaptive immune system to construct a whole immune system to the intrusion detection system of wireless sensor networks.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (NO.61370007, 61572206, U1405254), and the Program for New Century Excellent Talents in Fujian Province(2014FJ-NCET-ZR06).

References

[1] C. Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges", Proceedings of the IEEE, vol. 91, no. 8, **(2003)**, pp. 1247-1256.
[2] O. Can and S. O. Koray, "A survey of intrusion detection systems in wireless sensor networks: Modeling, Simulation, and Applied Optimization (ICMSAO)", 2015 6th International Conference on IEEE, **(2015)** May 27-29.
[3] N. A. Alrajeh, S. Khan and B. Shams, "Intrusion detection systems in wireless sensor networks: a review", International Journal of Distributed Sensor Networks, vol. 9, no. 5, **(2013)**.
[4] J. Kim, P. Bentley and C. Wallenta, "Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm", International Conference on Artificial Immune Systems, Springer Berlin Heidelberg, **(2006)** September 4-6.
[5] C. Wallenta, J. Kim and P. J. Bentley, "Detecting interest cache poisoning in sensor networks using an artificial immune algorithm", Applied Intelligence, vol. 32, no. 1, **(2010)**, pp. 1-26.
[6] M. Drozda, S. Schaust and H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: Performance and design principles", Evolutionary Computation, 2007, CEC 2007, IEEE Congress on IEEE, **(2007)** September 25-28.
[7] Y. Liu and F. Yu, "Immunity-based intrusion detection for wireless sensor networks", IEEE World Congress on Computational Intelligence, **(2008)** June 1-8.
[8] U. Aickelin, P. Bentley and S. Cayzer, "Danger theory: The link between AIS and IDS?", Proceedings of the 2nd International Conference on Artificial Immune Systems. Ediburgh, UK, **(2008)**, March 13-16.
[9] J. Greensmith and U. Aickelin, "The dendritic cell algorithm", 7th International Conference, ICARIS 2008, Phuket, Thailand, **(2008)** August 10-13.
[10] H. M. Salmon, C. M. de Farias and P. Loureirol, "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques", International journal of wireless information networks, vol. 20, no. 1, **(2013)**, pp. 39-66.
[11] L. Hong and J. Yang, "Danger theory of immune systems and intrusion detection system", Industrial Mechatronics and Automation, 2009. ICIMA 2009. International Conference on IEEE, **(2009)** May 15-16.
[12] Z. Chelly and Z. Elouedi, "FDCM: A fuzzy dendritic cell method", Artificial Immune Systems, vol. 6209, **(2010)**, pp. 102-115.
[13] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping", Springer Berlin Heidelberg, **(2008)**.
[14] J. Greensmith, U. Aickelin and J. Twycross, "Detecting danger: applying a novel immunological concept to intrusion detection systems", eprint arXiv: 1002.0696, **(2010)**.
[15] L. M. Sun, "Wireless Sensor Networks", Beijing: Tsinghua University Press, **(2005)**.

[16] M. Drozda, S. Schildt, S. Schaust, “An immuno-inspired approach to misbehavior detection in ad hoc wireless networks”, eprint arXiv: 1001.3113, **(2010)**.
[17] J. Kohlas, P. A. Monney, “Theory of evidence—A survey of its mathematical foundations, applications and computational aspects”, Zeitschrift für Operations Research, vol. 39, no. 1, **(1994)**, pp. 35-68.
[18] J. W. Zhuge, D. W. Wang and Y. Chen, “A network anomaly detector based on the DS evidence theory”, Journal of software, vol. 17, no. 3, **(2006)**, pp. 463-471.
[19] F. Voorbraak, “A computationally efficient approximation of Dempster-Shafer theory”, International Journal of Man-Machine Studies, vol. 30, no. 5, **(1989)**, pp. 525-536.
[20] P. Garcia-Teodoro, J. Diaz-Verdejo and G. Maciá-Fernández, “Anomaly-based network intrusion detection: Techniques, systems and challenges”, computers & security, vol. 28, no. 1, **(2009)**, pp. 18-28.

