Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8898847, 16 pages
https://doi.org/10.1155/2020/8898847

Research Article

Intrusion Detection Algorithm Based on Change Rates of Multiple Attributes for WSN

Hongying Bai,[1,2] **Xiaotong Zhang**,[1] **and Fangjie Liu**[1]

[1]*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China*
[2]*Department of Mathematics and Computer Engineering, Ordos Institute of Technology, Ordos 017000, China*

Correspondence should be addressed to Xiaotong Zhang; zxt@ies.ustb.edu.cn

Received 25 April 2020; Revised 4 October 2020; Accepted 16 November 2020; Published 2 December 2020

Academic Editor: Ernestina Cianca

Copyright © 2020 Hongying Bai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Intrusion detection system (IDS) is a second line of the security mechanism for the wireless sensor network (WSN), and it has a great influence on confidentiality, integrity, and availability. However, many existing IDS only detect single attack or multiple known attacks. In this paper, a novel intrusion detection algorithm based on change rates of multiple attributes (CRMA) is proposed, which can detect multiple attacks including known and unknown types simultaneously. The change rates of multiple attributes for sensor nodes usually reflect the running states of WSN over a period of time. First, the Observed Change Rate of attributes at different times is obtained by observing multiple attributes of different sensor nodes. Then, the convex optimization is alternately used to obtain the Normal Change Rate and corresponding weights by minimizing the distance between the Observed Change Rate and the Normal Change Rate of each attribute. Finally, the WSN is considered to be attacked when the weighted deviation of the Observed Change Rate and Normal Change Rate is beyond the corresponding threshold. Experimental results show that the CRMA can detect multiple attacks including known and unknown types simultaneously and has a fast convergence rate. The average true positive rates (TPR) of CRMA are high, and the average false positive rates (FPR) of CRMA are low. The detection performance of CRMA is superior to that of the ARMA and NeTMids algorithms.

1. Introduction

Due to the characteristics of flexibility, low cost, wireless communication, and self-organization ability, the wireless sensor network (WSN) plays an important role in healthcare [1, 2], the military [3], industry [4], and many other fields, for instance, traffic monitoring, smart home system, medical facilities, and so on [5, 6]. However, the WSN is vulnerable to be attacked because sensor nodes are usually deployed in the unmanned environment. Therefore, the security issue is the main challenge to construct a robust and reliable WSN [7].

Researchers have paid attention to encryption, decryption, identification, authentication, key management, and secure routing of the WSN. But such security measures cannot provide a wide range of protection against a variety of attacks and threats in the WSN. The intrusion detection system (IDS) is one possible solution to address a wide range of security attacks in the WSN [8]. The main tasks of an ID are to detect intruders trying to disrupt the WSN network [9, 10] and to monitor the security of WSN and identify vulnerability to guarantee the accurate network performance [11–13].

The key intrusion detection technology of the WSN has attracted a lot of attention in recent years. Misuse detection does very well in detecting known attacks, but it works badly in detecting attacks which are unknown or undefined [14]. Mehmood et al. proposed a knowledge-based context-aware approach for handling the intrusions generated by malicious nodes [15]. Ghosal and Halder proposed a survey on energy efficient intrusion detection in wireless sensor networks [16]. A hybrid anomaly detection method for misdirection and black hole attacks employing the K-medoid customized clustering technique is proposed in [17].

A lot of existing intrusion detection schemes of the WSN detects some known attacks. Hu et al. detect selective forwarding attacks in WSN by monitoring the loss rate of the packet and construct a trusted mechanism [18]. Motamedi and Yazdani use UAV to detect black hole attacks in WSN

[19]. Gara et al. proposed a mobile WSN intrusion detection system based on IPv6, which specifically detects selective forwarding attacks in the network [20]. Many papers present IDS for WSN which only detect one kind of attack, such as the DoS attack [21, 22], selective forwarding attack [23], and sinkhole attack [24].

Some intrusion detection algorithms detect attacks by predicting attributes of network flow, such as using the Autoregressive Moving Average (ARMA) or Markov model to predict traffic. It indicates that an attack occurring in the network when the normal flow value is significantly different from the predicted flow value [25]. Although the ARMA intrusion detection algorithm has higher detection accuracy, it only detects attacks related to the selected flow value, and it cannot detect multiple attack types at the same time.

Few intrusion detection algorithms can detect multiple attacks simultaneously. Sajjad et al. proposed IDS based on the trustworthiness of neighbor nodes. Each node in the intrusion detection system analyzes the trust level of its neighbor nodes by analyzing the statistical data in the network and calculates the credibility value, thus determining the credibility of neighbor nodes. It can detect hello flood attacks, blocking attacks, and selective forwarding attacks. The intrusion detection system uses a lightweight intrusion detection algorithm NeTMids [26]. The NeTMids algorithm applies a variety of attributes to intrusion detection and analysis of nodes in the network and can detect multiple attack types at the same time. However, the accuracy of detection of NeTMids is not very high.

According to the above circumstances, there are many problems in IDS for WSN as follows:

(a) The detection accuracy of some intrusion detection systems is low

(b) Many IDS only detect known attack types and cannot detect unknown attack types

(c) Many IDS only detect one or two attack types at the same time and cannot detect multiple attacks simultaneously

Therefore, we should design or improve the intrusion detection algorithm for the WSN to improve current intrusion detection technology.

Aiming at detecting a variety of internal attacks of the WSN, a novel change rates of multiple attributes (CRMA) intrusion detection algorithm is proposed in this paper, which can detect multiple intrusion attacks including known and unknown types simultaneously. In CRMA, we obtain the Observed Change Rate of attributes through observing the values of different attributes of different nodes over a period of time. The Normal Change Rates of attributes are calculated by minimizing the weighted deviation between the Observed and Normal Change Rates by convex optimization. The IDS considered to be attacked when the Observed Change Rate deviates from the Normal Change Rate beyond the corresponding threshold.

This paper is organized as follows. Section 2 gives the IDS model and multiple attributes of the WSN. In Section 3, we describe the CRMA intrusion detection algorithm and discuss some issues in the algorithm. In Section 4, we offer experimental analysis and performance evaluation of the IDS. In the final section, the conclusion is given.

2. IDS Model and Multiple Attributes of WSN

In this section, we introduce the IDS model, attributes of the WSN, and symbol representations of CRMA.

2.1. IDS Model. The model of the intrusion detection system designed in this paper is shown in Figure 1. The IDS agents perform intrusion detection and data transmission. We assume that the IDS agents are trusted nodes and have sufficient energy. IDS agents interact with sensor nodes and base stations (BS). IDS agents will perform deep packet inspection on the ID and attributes of nodes. We assume encrypted traffic by default and IDS agents know the keys of the detected nodes in advance. The IDS agents can decrypt received data and perform deep packet inspection.

The deployment principle of IDS agents is to make IDS agents cover as many nodes as possible and reduce the area of overlap. IDS agents should be deployed in the monitoring region and as far as possible to cover the entire WSN.

2.2. Attributes of WSN. The sensor nodes of the WSN have some characteristic attributes that can be utilized by intrusion detection algorithms. In [27], the attributes of the WSN are divided into two types. One is the audit data in local detection which includes the packet collision rate, the waiting time of transmission, the number of neighbors, the energy consumption rate, and the rate of sensor reading report. Second, the audit data based on packets in the network includes the packet type, RSSI, arrival rate of sensor data, and packet loss rate.

The WSN attributes may be affected by different types of attacks. We find that the more attributes you choose, the more they reflect the WSN situation. However, due to the limited resources of the WSN, it is necessary to select several different attributes to participate in the intrusion detection calculation according to the situation.

2.3. Symbolic Representations. Some symbols which would be used in the CRMA intrusion detection and the explanations of what they represent are shown in Table 1.

3. Intrusion Detection Algorithm Based on Change Rates of Multiple Attributes (CRMA)

The basic idea of the CRMA intrusion detection algorithm is as follows:

(a) The *Observed Change Rate* $\Delta v_n^{(t,m)}$ of attributes is obtained by observing multiple attributes of different nodes

(b) Convex optimization is alternately used to obtain the *Normal Change Rate* of attribute $\Delta v_n^{(*,m)} (i < t < j)$ and corresponding weights

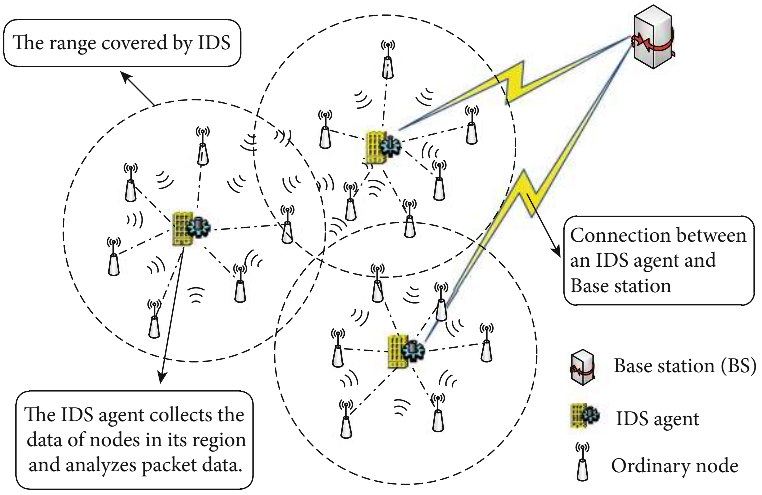
The range covered by IDS
Connection between an IDS agent and Base station
The IDS agent collects the data of nodes in its region and analyzes packet data.
Base station (BS)
IDS agent
Ordinary node

Figure 1: IDS model of WSN.

Table 1: Symbol representations.

Symbol	Representation
m	The mth attribute of sensor node of WSN. The total number of multiple attributes is $M, m \in \{1, \cdots, M\}$.
$v_n^{(t,m)}$	The value of mth attribute of nth sensor node at moment t. The total number of nodes is $N, n \in \{1, \cdots, N\}$.
$v_n^{(t-1,m)}$	The value of mth attribute of nth node at moment $t-1$. The $t-1$ is previous adjacent time of t. The total number of nodes is $N, n \in \{1, \cdots, N\}$.
$\Delta v_n^{(t,m)}$	The "*Observed Change Rate*" of mth attribute of nth node between time t and $t-1$.
$\Delta v_n^{(*,m)}$	The "*Normal Change Rate*" of mth attribute of nth node in the period of interval time $i \sim j$. The i and j are not adjacent times.
ΔV_n^*	A set of $\Delta v_n^{(*,m)}$. At every interval time $i \sim j$, the attribute vector comprises a fixed number of *Normal Change Rates* of all attributes $\Delta V_n^* = \left\{\Delta v_n^{(*,m)}\ ; n = 1, \cdots, N\ ; m = 1, \cdots, M\right\}$.
ω_n^t	The parameter ω_n^t is the weight of nth node at time t.
Ω_n	The weights of nth node in the period of $i \sim j$. $\Omega_n = \left\{\omega_n^i, \omega_n^{i+1}, \cdots, \omega_n^j\right\}$.
D -value	The difference value of the two adjacent iterations.
$\omega_n^{(t,m)}$	The weight of mth dimension attribute of nth node at moment t.

(c) When the *Observed Change Rate* $\Delta v_n^{(t,m)} (t > j)$ deviates from the *Normal Change Rate* $\Delta v_n^{(*,m)}$ beyond the corresponding threshold, the IDS would determine that the WSN is attacked

3.1. CRMA Framework. The change rates of attributes are steady or change slowly when the WSN is running normally. For instance, the reduction of energy will follow a regular pattern when the sensor node transmits packets at a certain rate. If the change rates of attributes are abnormal, the network is considered to be under attack. In CRMA, convex optimization is used to obtain the *Normal Change Rates* of attributes and corresponding weights by minimizing the distance between the *Observed Change Rate* and the *Normal Change Rate* of each attribute.

3.1.1. Observed Change Rate. The $|v_n^{(t,m)} - v_n^{(t-1,m)}|$ is the difference between the mth attribute of nth node between time t and the previous time $t-1$. The range and magnitude of each attribute may be different. We define the relative change rate as the Observed Change Rate $\Delta v_n^{(t,m)}$ in CRMA.

$$\Delta v_n^{(t,m)} = \frac{|v_n^{(t,m)} - v_n^{(t-1,m)}|}{v_n^{(t-1,m)}}. \tag{1}$$

3.1.2. Deviation Function. The $\Delta v_n^{(*,m)}$ is the *Normal Change Rate* of mth attribute of nth node in the period of interval time $i \sim j$ which can reflect the regular pattern during the stable operation. In CRMA, the *deviation function* $d(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)})$ is the square of the distance between the $\Delta v_n^{(t,m)}$ and $\Delta v_n^{(*,m)}$. The value of the deviation function is small when the Observed Change Rate is close to the Normal Change Rate.

$$d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) = \left(\Delta v_n^{(*,m)} - \Delta v_n^{(t,m)}\right)^2. \tag{2}$$

3.1.3. Constraint Function. The corresponding time weight represents the reliability of the Observed Change Rate in a certain period of time. The parameter ω_n^t is the weight of n th node at time t. A higher ω_n^t indicates that the *Observed Change Rate* of the nth node at time t is closer to the *Normal Change Rate*. The Ω_n is set of ω_n^t, $\Omega_n = \{\omega_n^i, \omega_n^{i+1}, \cdots, \omega_n^j\}$, which is the weights of the nth node in the period time of $i \sim j$. The *constraint function* $\delta(\Omega_n)$ specifies the range of time weights which reflects the distributions of weights at different times. The constraint function maps the time weights uniformly to a particular range which can improve the convergence speed and accuracy of the IDS. We define a constraint function and a domain S to make ω_n^t locate at a certain numerical range. Different constraint functions may have different influences on the result. We set the value of $\delta(\Omega_n)$ to be 1 for the sake of simplicity. We choose an exponential function as the constraint function, and the domain of weights expands into $[0, +\infty)$.

$$\begin{gathered}\delta(\Omega_n) = \sum_{t=i}^{j} e^{-\omega_n^t} = 1, \\ S = [0,+\infty).\end{gathered} \tag{3}$$

3.1.4. Optimization Problem of CRMA. The intrusion detection algorithm based on the change rates of multiattributes is proposed in this paper. The $\Delta v_n^{(t,m)}$ is a known value, and the $\Delta v_n^{(*,m)}$ is an unknown value. We construct a convex optimization problem to calculate the *Normal Change Rate* $\Delta v_n^{(*,m)}$ of attributes by minimizing the weighted deviation between the Observed Change Rate and the Normal Change Rate. The objective function is shown as follows:

$$\begin{gathered}\min_{\Delta V_n^*,\Omega_n} \quad f(\Delta V_n^*, \Omega_n) = \sum_{t=i}^{j} \omega_n^t \sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ \text{s.t.} \quad \delta(\Omega_n) = 1 \\ \Omega_n \in S,\end{gathered} \tag{4}$$

where the ΔV_n^* is a set of $\Delta v_n^{(*,m)}$. The attribute vector comprises a fixed number of *Normal Change Rate* of all attributes $\Delta V_n^* = \{\Delta v_n^{(*,m)} \mid n = 1, \cdots, N ; m = 1, \cdots, M\}$. Each node constructs some attribute vector which reflects the operation status of the network in interval time $i \sim j$. The ΔV_n^* and Ω_n are unknown vectors that correspond to the set of $\Delta v_n^{(*,m)}$ and time weights, respectively. For an optimization problem with two unknown vectors, to minimize the objective function, a vector can be fixed and another unknown vector can be found through multiple iterations until the vector converges. This iterative approach, referred to as the block coordinate descent method [28], will gradually reduce the updated value of the objective function until it reaches the minimum value. The ΔV_n^* and Ω_n can be obtained by following two iterative convergent procedures.

(1) Weight Update. We determine the Ω_n by fixing ΔV_n^*. With the estimation of the initial the value of ΔV_n^*, we can obtain Ω_n through minimizing the objective function, as follows:

$$\begin{gathered}\Omega_n \leftarrow \operatorname*{argmin}_{\Omega_n} f(\Delta V_n^*, \Omega_n) \\ \text{s.t.} \quad \delta(\Omega_n) = 1 \\ \Omega_n \in S.\end{gathered} \tag{5}$$

(2) Normal Change Rate Update

We determine the $\Delta V_n^* (\Delta V_n^* = \{\Delta v_n^{(*,m)} ; n = 1, \cdots, N ; m = 1, \cdots, M\})$ by fixing $\Omega_n (\Omega_n = \{\omega_n^i, \omega_n^{i+1}, \cdots, \omega_n^j\})$. We obtain the *Normal Change Rate* minimizing the weighted deviation between the *Observed Change Rate* and the *Normal Change Rate* based on the Ω_n calculated in the step above.

$$\Delta v_n^{(*,m)} \leftarrow \operatorname*{argmin}_{\Delta v_n^{(*,m)}} \sum_{t=i}^{j} \omega_n^t \cdot d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right). \tag{6}$$

The D -value is the difference in the value of the two adjacent iterations. When the *D -value* is less than the threshold, the iterative process is stopped. During multiple iterations, the $\Delta v_n^{(*,m)}$ gradually converges to a fixed value, which is the *Normal Change Rate* in time period $i \sim j$.

There is another CRMA intrusion detection framework. The objective function is shown as (7). The $\omega_n^{(t,m)}$ is the weight of the mth dimension attribute of the nth node at moment t. The solving process of (7) is similar to (4). But this form of CRMA intrusion detection assigns weights to each node at each time of the observation phase. Calculating the state of each node separately can improve the accuracy of the IDS. However, it greatly increases the complexity of the algorithm, and larger space is needed to store weights, which is a huge burden for resource-constrained sensor nodes.

$$\begin{gathered}\min_{\Delta V_n^*,\Omega_n} \quad f(\Delta V_n^*, \Omega_n) = \sum_{t=i}^{j} \sum_{m=1}^{M} \omega_n^{(t,m)} \cdot d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ \text{s.t.} \quad \delta(\Omega_n) = 1 \\ \Omega_n \in S.\end{gathered} \tag{7}$$

The selection of attributes depends on what type of attack you want to detect. For example, when the WSN is under a flooding attack, the distribution of the packet type would be abnormal immediately and the RSSI would be exceptionally high. In order to detect the flooding attack successfully, the IDS should involve the attributes that would be affected in the detection procedure. On the other hand, if we select multiple attributes properly, we could detect multiple types of attacks at the same time.

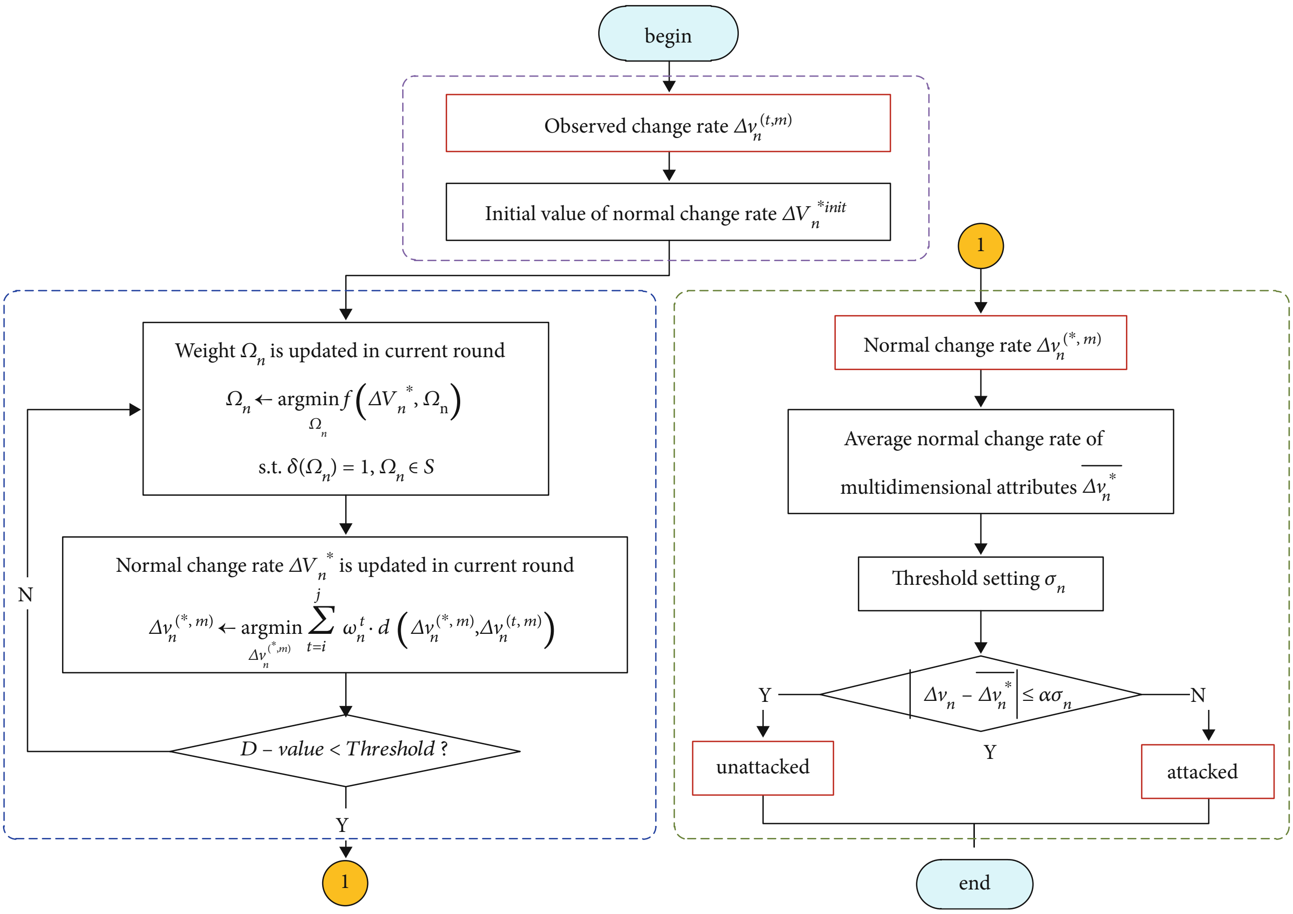
begin
Observed change rate $\Delta v_n^{(t,m)}$
Initial value of normal change rate ΔV_n^{*init}
Weight Ω_n is updated in current round
$\Omega_n \leftarrow \operatorname{argmin}_{\Omega_n} f\left(\Delta V_n^*, \Omega_n\right)$
s.t. $\delta(\Omega_n) = 1, \Omega_n \in S$
Normal change rate ΔV_n^* is updated in current round
$\Delta v_n^{(*,m)} \leftarrow \operatorname{argmin}_{\Delta v_n^{(*,m)}} \sum_{t=i}^{j} \omega_n^t \cdot d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right)$
N
D – value < Threshold ?
Y
1
1
Normal change rate $\Delta v_n^{(*,m)}$
Average normal change rate of multidimensional attributes $\overline{\Delta v_n^*}$
Threshold setting σ_n
Y
$\left|\Delta v_n - \overline{\Delta v_n^*}\right| \leq \alpha\sigma_n$
N
Y
unattacked
attacked
end

Figure 2: Flow chart of CRMA intrusion detection algorithm.

3.2. Parameter Setting and Performance Analysis of CRMA

3.2.1. Initial Value of the Normal Change Rate. The *Normal Change Rate* $\Delta v_n^{(*,m)}$ is obtained by solving the convex optimization problem by minimizing the weighted distance between the Observed Change Rate and solving the Normal Change Rate of each attribute. However, we need to set the initial value of $\Delta v_n^{(*,m)}$ at first which is crucial to solving the convex optimization problem efficiently. In theory, if the optimization problem is convex, the initial value of $\Delta v_n^{(*,m)}$ would not affect the final optimal solution. But good initial values make the algorithm converge quickly and save computing resources. The selecting principle of the initial value of Normal Change Rate $\Delta v_n^{(\text{init}*,m)}$ is that the chosen value is close to actuality. In CRMA, we use the average method to set the initial value of the Normal Change Rate.

$$\Delta v_n^{(\text{init}*,m)} = \overline{\Delta v_n^m} = \frac{\sum_{t=i}^{i} \Delta v_n^{(t,m)}}{j-i+1} \quad (n = 1, \cdots, N, m = 1, \cdots, M). \tag{8}$$

3.2.2. Threshold Setting. The threshold setting is related to the accuracy of the intrusion detection. There are two methods that can be used to set the threshold according to the actual situation to improve the accuracy of the detection.

(1) In the training phase of the intrusion detection algorithm, the average and standard deviation of each attribute are calculated by collecting and analyzing data of each node in the time period $i \sim j$. The value of average attribute is as shown in (8). The standard deviation is calculated as shown in

$$\sigma_n^m = \sqrt{\frac{1}{j-i+1} \sum_{t=i}^{j} \left(\Delta v_n^{(t,m)} \text{-} \overline{\Delta v_n^m}\right)^2}. \tag{9}$$

The α is the parameter determined during the experiment. For any $t > j$, $m \in [1, M]$, $n \in [1, N]$, if $\left|\Delta v_n^{(t,m)} - \Delta v_n^{(*,m)}\right| \leq \alpha\sigma_n^m$, it can be judged that there are no intrusion attacks in the WSN. Otherwise, it can be judged that the network is attacked. The corresponding parameters in different environments of the WSN may be different

(2) If the multiple attributes are independent, the joint judgment will increase the false negative rate. If the multiple attributes are related to each other, the joint

judgment will get a higher true positive rate. The value of the average attribute is shown in (10). The standard deviation is shown in (11). The average Normal Change Rate of multiple attributes of the node is calculated as shown in (12).

$$\overline{\Delta v_n} = \frac{\sum_{t=i}^{j}\sum_{m=1}^{M} \Delta v_n^{(t,m)}}{(j-i+1)M}, \tag{10}$$

$$\sigma_n = \sqrt{\frac{1}{(j-i+1)M}\sum_{t=i}^{j}\sum_{m=1}^{M}\left(\Delta v_n^{(t,m)} - \overline{\Delta v_n}\right)^2}, \tag{11}$$

$$\overline{\Delta v_n^*} = \frac{\sum_{m=1}^{M} \Delta v_n^{(*,m)}}{M}. \tag{12}$$

Similarly, if $|\Delta v_n - \overline{\Delta v_n^*}| \le \alpha\sigma_n$, it can be judged that there are no intrusion attacks in the WSN. Otherwise, it can be judged that there are intrusion attacks in the WSN. The α is the parameter determined during the experiment

The computational complexity of (11) is much greater than (9). We can decide which judgment to choose according to the actual situation.

Based on the above description, the flow chart of the CRMA intrusion detection algorithm is shown in Figure 2.

(a) The Observed Change Rate $\Delta v_n^{(t,m)}$ of attributes at different times obtained by observing the values of different attributes of sensor nodes over a period of time. We set the initial value of the Normal Change Rate as $\Delta v_n^{(init*,m)}$

(b) Convex optimization is used to obtain the normal attribute change rate $\Delta v_n^{(*,m)}$ by minimizing the weighted distance between the rate of the Observed Change Rate and the normal change of each attribute. When the *D*-value is less than the threshold, the iterative process of convex optimization is stopped

(c) The IDS would turn on the alarm when the Observed Change Rate deviates from the Normal Change Rate beyond the corresponding threshold. If $|\Delta v_n - \overline{\Delta v_n^*}| \le \alpha\sigma_n$ (or $|\Delta v_n^{(t,m)} - \Delta v_n^{(*,m)}| \le \alpha\sigma_n^m$), it can be judged that there are no intrusion attacks in the WSN. Otherwise, it can be judged that there are intrusion attacks in the WSN

3.2.3. Proof of Convexity. Based on the CRMA intrusion detection algorithm described above, the following theorems are given.

Theorem 1. *The constraint function (3) and the optimization problem (4) constitute a convex optimization problem when ΔV_n^* is fixed.*

Table 2: Simulation parameters.

Parameter	Value
Deployment field	100 m × 100 m
Number of nodes	30~190
Deployment method	Random
Initial energy of node	0.5 J
BS position	(50 m, 50 m)
E_{elce}	50 nJ/bit
ε_{fs}	10 pJ/bit/m^2
ε_{mp}	0.0013 pJ/bit/m^4
E_{DA}	5 nJ/bit/signal

Proof. According to constraint condition (3), the change domain of ω_n^t is $[0, +\infty)$ which is a convex set. So, the domain of the objective function in (4) is a convex set. When ΔV_n^* is fixed, the objective function is a linear affine function for ω_n^t.

For any $0 \le \theta \le 1, x, y \in [i, j]$,

$$\begin{aligned} f(\theta x + (1-\theta)y) &= \sum_{t=i}^{j}\left(\theta x_n^t + (1-\theta)y_n^t\right)\sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ &= \theta \sum_{t=i}^{j} x_n^t \sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ &\quad + (1-\theta)\sum_{t=i}^{j} y_n^t \sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ &= \theta f(x) + (1-\theta) f(y). \end{aligned} \tag{13}$$

It satisfies the definition of a convex function $f(\theta x + (1-\theta)y) \le \theta f(x) + (1-\theta)f(y)$. Therefore, the objective function is a convex function. The constraint function (3) and optimization problem (4) constitute a convex optimization problem involving equality and inequality constraints, which can be solved by the convex optimization solution method. We use the *Lagrangian* multiplier λ to solve Ω_n.

Let $\varphi = -e^{-\omega_n^t}$, then, $\sum_{t=i}^{j} \varphi = 1$, $S = [0, +\infty)$.

The optimization problem is converted to

$$L(\Omega_n, \lambda) = \sum_{t=i}^{j} \ln\varphi \sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) + \lambda\left(1 - \sum_{t=i}^{j}\varphi\right). \tag{14}$$

Let the partial derivative of φ be 0, and get

$$\lambda\varphi = -\sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right). \tag{15}$$

Table 3: Characteristics and impacts of simulated attacks.

Simulated attacks	Characteristics	Impacts
Hello flooding attacks	The attacker uses a high-power transmitter to broadcast and send Hello packets every round, so that each node of the network mistakes the attacker for its neighbor node.	The energy consumption of the attacked node will increase rapidly. The proportion of Hello packets will increase significantly, and proportion of other data packets will decrease.
Selective forwarding attacks	The attacked nodes probabilistically forward or drop specific packets. It has a significant impact on the node with forwarding function.	The proportion of sending and receiving packets of the forwarding node will change. The forwarding rate of the node will decrease.
DoS attacks	The attacker interferes with or controls user data, causing refusal of service on correct data transmission.	The sending rate and forwarding rate of the attacked node will be significantly reduced.
Sinkhole attacks	The attacker uses his powerful features to make himself more like a base station, so it can receive more data.	The number of packages received by the attacked nodes suddenly increases, and the energy is rapidly reduced due to collection.
Multiple attacks	The Hello flooding attacks, Selective forwarding attacks, DoS attacks, and Sinkhole attacks exist simultaneously.	A combination of the impacts of the above four kinds of attacks.

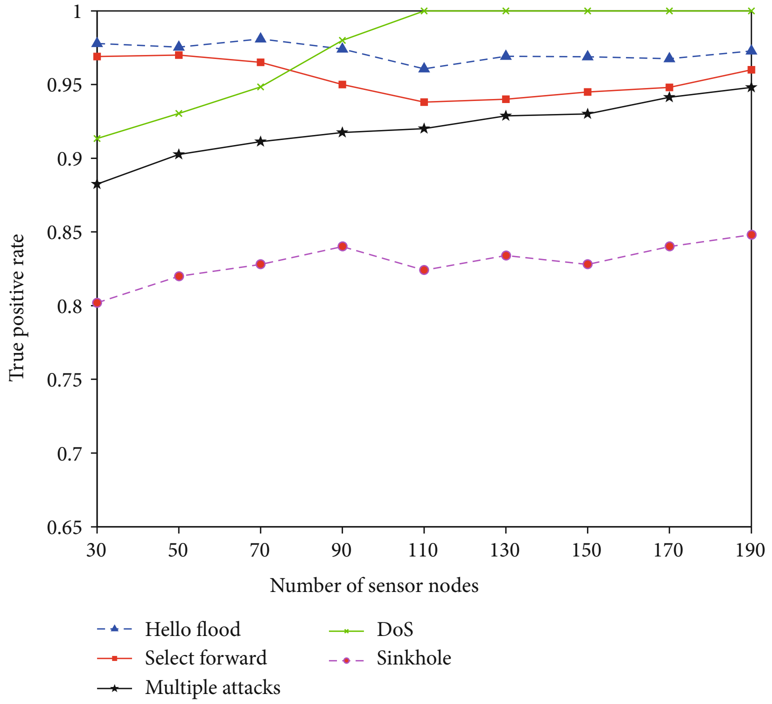

Figure 3: True positive rates of CRMA under different attacks.

Obtained by the constraint $\sum_{t=i}^{j}\varphi = 1$,

$$\lambda = -\sum_{t=i}^{j}\sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right). \tag{16}$$

Combine with $\varphi = e^{-\omega_n^t}$ and obtain

$$\omega_n^t = -\ln \frac{\sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right)}{\sum_{t'=i}^{j}\sum_{m=1}^{M} d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t',m)}\right)}. \tag{17}$$

It is obvious that the weight is inversely proportional to the deviation between the observation and the actuality which means the weight is greater when the Observed Change Rate is closer to the Normal Change Rate.

Theorem 2. *The change rate (1), deviation function (2), constraint function (3), and optimization problem (4) constitute a convex optimization problem when Ω_n is fixed.*

Proof. The change rate (1) limits the value range of the property change rate to the real number domain R, so the set of the definition domain of the independent variable $\Delta v_n^{(t,m)}$ of the deviation function $d(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)})$ is a convex set.

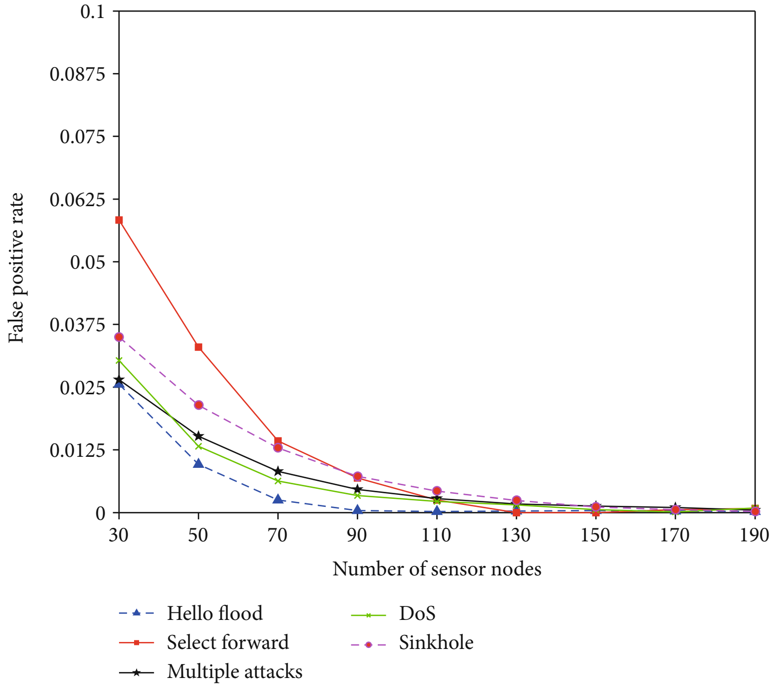

Figure 4: False positive rates of CRMA under different attacks.

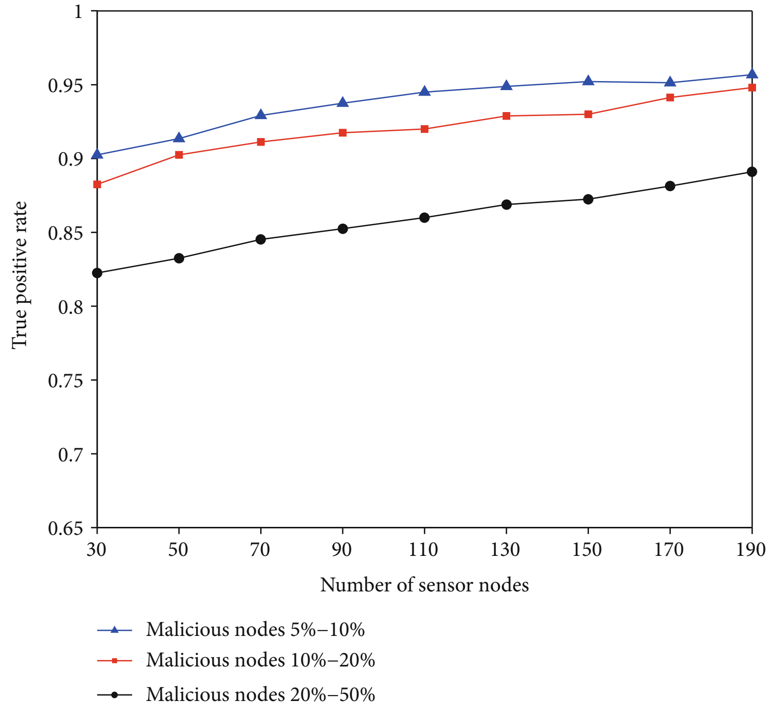

Figure 5: True positive rates of CRMA under different percentages of malicious nodes.

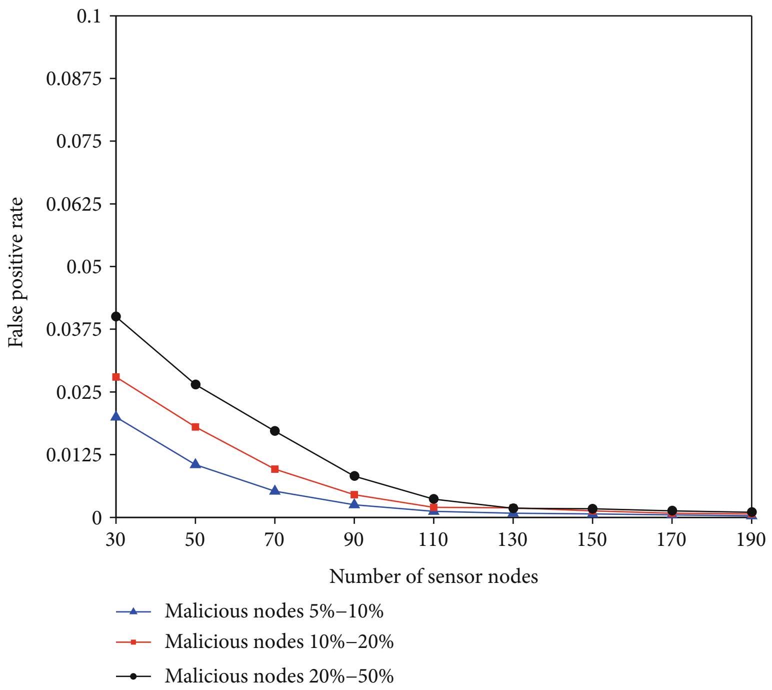

Figure 6: False positive rates of CRMA under different percentages of malicious nodes.

Table 4: Values of objective function in multiround iterations.

Round r	Objective function $f(r)$	Difference of objective function $f(r) - f(r-1)$
1	3042.33066037449	
2	3041.47055739694	0.86010297755
3	3041.46891236754	0.00164502940
4	3041.46890797954	0.00000438800
5	3041.46890796675	0.00000001279
6	3041.46890796671	0.00000000004
7	3041.46890796671	0.00000000000

For any $0 \le \theta \le 1, x, y \in [1, M]$,

$$d\left(\theta \Delta v_n^{(x,m)} + (1-\theta)\Delta v_n^{(y,m)}, \Delta v_n^{(t,m)}\right) > \theta d\left(\Delta v_n^{(x,m)}, \Delta v_n^{(t,m)}\right) + (1-\theta) d\left(\Delta v_n^{(y,m)}, \Delta v_n^{(t,m)}\right). \tag{18}$$

Namely,

$$\left[\theta \Delta v_n^{(x,m)} + (1-\theta)\Delta v_n^{(y,m)} - \Delta v_n^{(t,m)}\right]^2 > \theta \left[\Delta v_n^{(x,m)} - \Delta v_n^{(t,m)}\right]^2 + (1-\theta)\left[\Delta v_n^{(y,m)} - \Delta v_n^{(t,m)}\right]^2. \tag{19}$$

We get that

$$\theta(\theta-1)\left(\Delta v_n^{(x,m)} - \Delta v_n^{(y,m)}\right)^2 > 0. \tag{20}$$

Due to $0 \le \theta \le 1$, the above formula is obviously wrong. So, we get that

$$d\left(\theta \Delta v_n^{(x,m)} + (1-\theta)\Delta v_n^{(y,m)}, \Delta v_n^{(t,m)}\right) \le \theta d\left(\Delta v_n^{(x,m)}, \Delta v_n^{(t,m)}\right) + (1-\theta) d\left(\Delta v_n^{(y,m)}, \Delta v_n^{(t,m)}\right). \tag{21}$$

According to the definition of the convex function, the deviation function is a convex function. The constraint function (3) combined withω_n^t is nonnegative, and the objective function (6) is a nonnegative linear combination of convex functions. According to the nature of the convex function, the objective function of the optimization problem is also a convex function. So, (1), (2), (3), and (4) constitute an unconstrained convex optimization problem. There is only one optimal solution, and the locally optimal solution is also the global optimal solution when the optimization problem is a convex optimization problem [28].

According to (2) and (6), we get that

$$\begin{aligned}\Delta v_n^{(*,m)} &\leftarrow \operatorname{argmin} \sum_{t=i}^{j} \omega_n^t \cdot d\left(\Delta v_n^{(*,m)}, \Delta v_n^{(t,m)}\right) \\ &= \operatorname{argmin} \sum_{t=i}^{j} \omega_n^t \cdot \left(\Delta v_n^{(*,m)} - \Delta v_n^{(t,m)}\right)^2.\end{aligned} \tag{22}$$

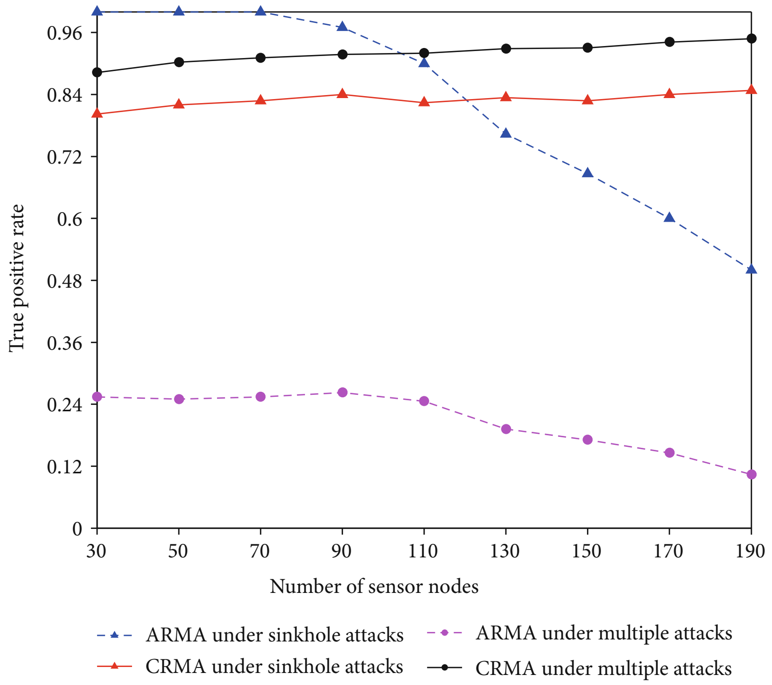

Figure 7: True positive rates of ARMA and CRMA.

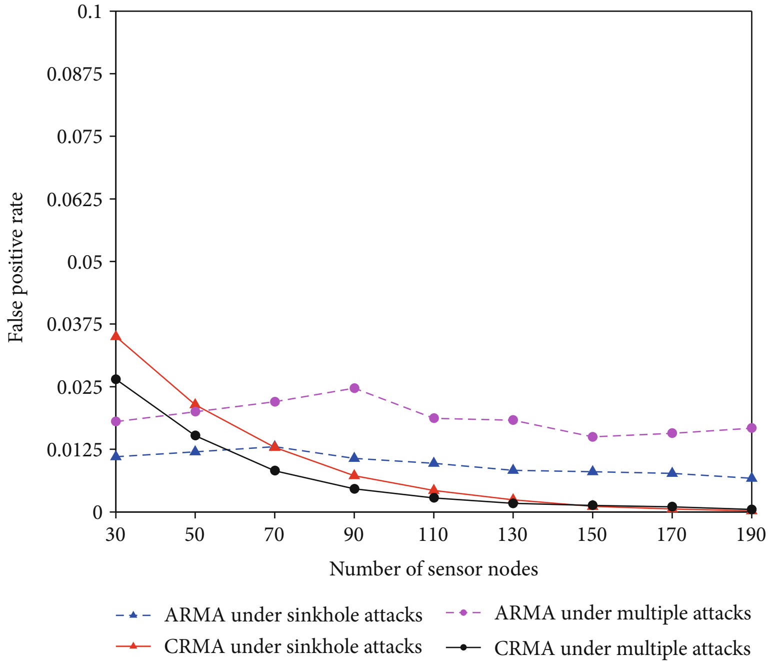

Figure 8: False positive rates of ARMA and CRMA.

Let the partial derivative with respect to $\Delta v_k^{(*,m)}$ be equal to 0, and then, we derive the solution of Normal Change Rate $\Delta v_n^{(*,m)}$.

$$\Delta v_n^{(*,m)} \leftarrow \frac{\sum_{t=i}^{j} \omega_n^t \cdot \Delta v_n^{(t,m)}}{\sum_{t=i}^{j} \omega_n^t}. \qquad (23)$$

Therefore, the CRMA intrusion detection algorithm will converge to fixed value during the iterative process.

3.2.4. Time Complexity. The time complexity of the CRMA intrusion detection algorithm will vary when using a different deviation function, constraint function, and objective function. If (2), (3), and (4) are used, the time complexity of

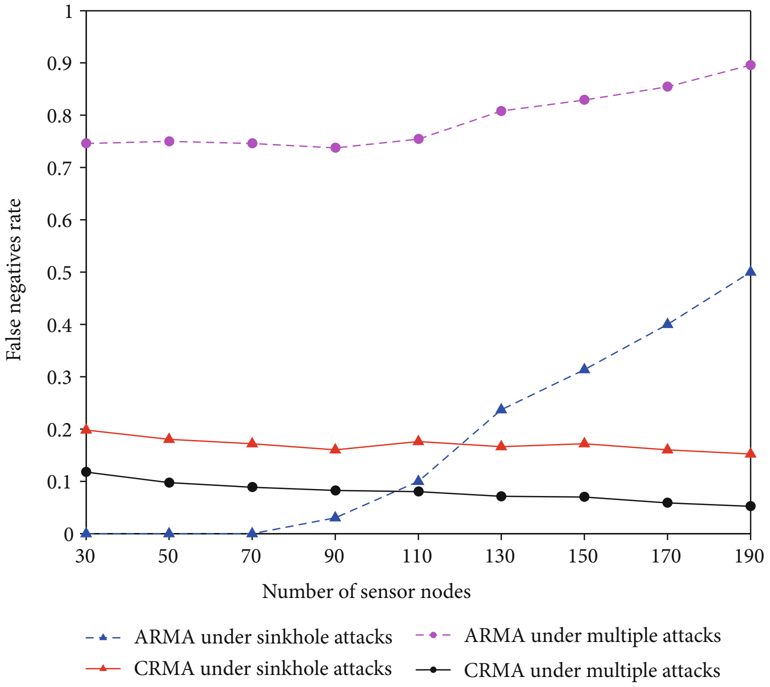

FIGURE 9: False negative rates of ARMA and CRMA.

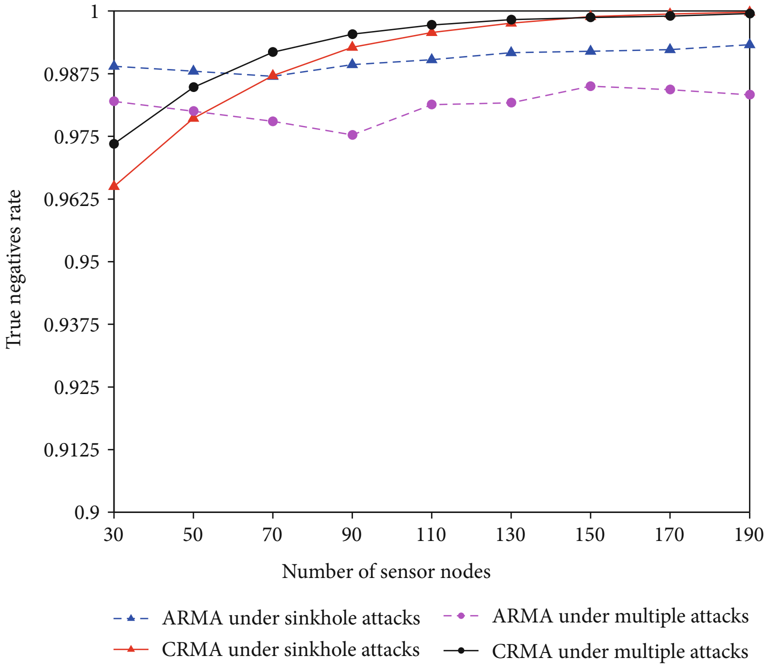

FIGURE 10: True negative rates of ARMA and CRMA.

CRMA is shown as follows:

$$T(n) = O(T \times N \times M), \tag{24}$$

where T is the time range and $T = j - i + 1$, N is the number of sensor nodes, and M is the number of attributes of the nodes.

If the squared deviation function (2), (3), and (7) is used, the time complexity of CRMA is (25).

$$T(n) = O\left(T^2 \times N \times M\right). \tag{25}$$

In (7), the CRMA intrusion detection assigns weights to each node at each time of the observation phase. Calculating the state of each node separately can improve the accuracy of

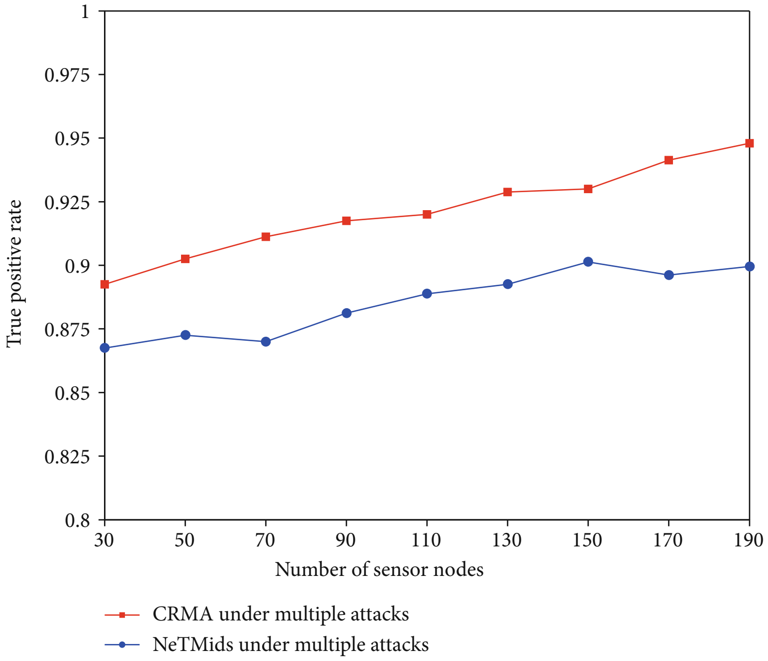

Figure 11: True positive rates of NeTMids and CRMA.

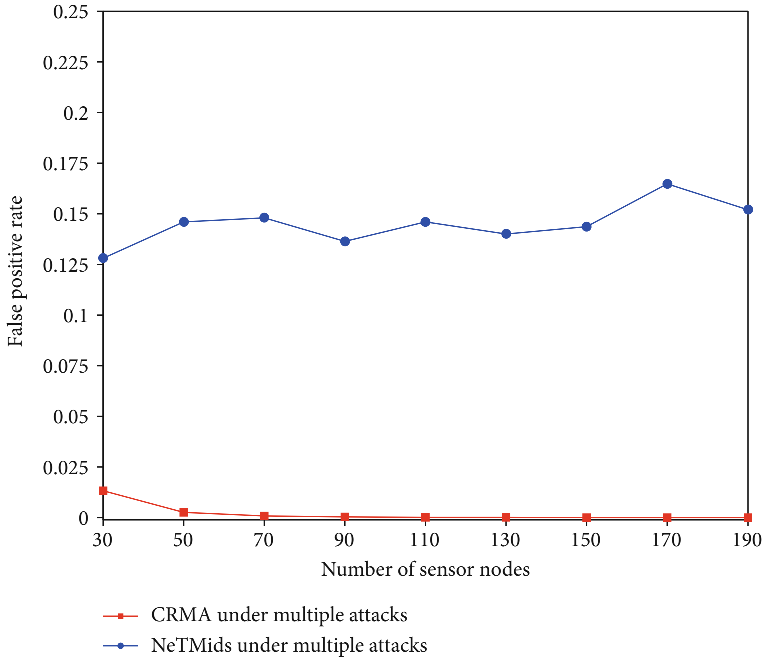

Figure 12: False positive rates of NeTMids and CRMA.

the IDS. But, it greatly increases the complexity of the algorithm.

4. Experiments and Discussion

Attacks from the internal network are the biggest threats to the WSN. Attacks from the external network only make the attacker become a legitimate node to obtain the network information. However, internal attacks often destroy or modify the network data. In this paper, we hope to find an effective way to detect internal attacks.

The parameters to measure the performance of the intrusion detection system are set as (26)–(29). There are four concepts: true positive (TP), false positive (FP), true negative (TN), and false negative (FN). The TP occurs when normal patterns are correctly classified as normal. The FP occurs

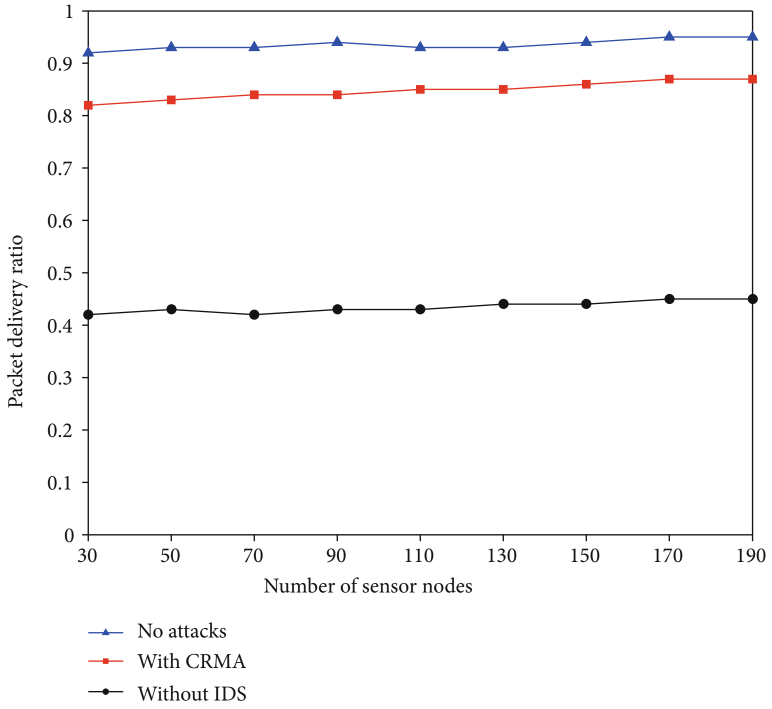

Figure 13: Packet delivery ratio with CRMA and without IDS.

when abnormal patterns are incorrectly classified as normal. The TN occurs when abnormal patterns are correctly classified as abnormal. The FN occurs when normal patterns are incorrectly classified as abnormal. The true positive rate (TPR) is the probability of successfully detecting the intrusion attacks. The true negative rate (TNR) is the probability that abnormal patterns are incorrectly classified as normal. The false positive rate (FPR) is the probability that attacks will be issued no attacks. The false negative rate (FNR) is the probability that nonattacks will falsely be classified as attacks [29, 30]. The high performance of IDS should achieve a high TPR and low FPR to ensure the efficiency and reliability of the IDS and guarantee the security of the network.

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}, \qquad (26)$$

$$\mathrm{TNR}=\frac{\mathrm{TN}}{\mathrm{TN}+\mathrm{FP}}, \qquad (27)$$

$$\mathrm{FNR}=\frac{\mathrm{FN}}{\mathrm{TP}+\mathrm{FN}}=1-\mathrm{TPR}, \qquad (28)$$

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}=1-\mathrm{TNR}. \qquad (29)$$

We simulated several typical attacks based on MATLAB; the simulation parameters are given in Table 2.

We validate our algorithms with several typical internal attacks in the WSN including hello flooding attacks, selective forwarding attacks, DoS attacks, sinkhole attacks, and their hybrid attacks (multiple attacks). Table 3 shows the characteristics and impacts of simulated attacks. The multiple attacks are that the above four kinds of attacks exist simultaneously.

In the CRMA, we detect the change rate of attributes based on the characteristics and impacts of the simulated attacks. We assume that the base station (BS) and IDS agents are trusted nodes. CRMA can detect multiple attacks simultaneously. Each point in the following figures is the average of the results of hundreds of tests, and each line has been accumulated over thousands of tests in this paper.

Figure 3 shows that the CRMA has higher true positive rates (TPR) for the four simulated attacks and their hybrid attack (multiple attacks). The TPR for the sinkhole attacks is relatively low. This is because the change rate of the attribute caused by the sinkhole attack is small. So, the CRMA is not good at detecting such attacks. The TPR of the DoS attacks can reach 100% when the number of nodes is large. This is because once the node launches the DoS attacks, the node stops all functions, which will immediately cause the node to change attributes, such as stopping the sending and receiving of data packets, stopping the collection of sensor data, etc. So, the CRMA will more easily detect changes in these attributes.

Figure 4 shows that CRMA has lower false positive rates (FPR) for the four types of attacks and their hybrid attacks. When the number of nodes is relatively small, the FPR is relatively high. But as the number of nodes increases, the false positive rate will decrease. In (29), the FP occurs when abnormal patterns are incorrectly classified as normal and the TN occurs when abnormal patterns are correctly classified as abnormal. With the increase of nodes, the number of attributes also increases. The ability of the system to judge what is abnormal becomes stronger.

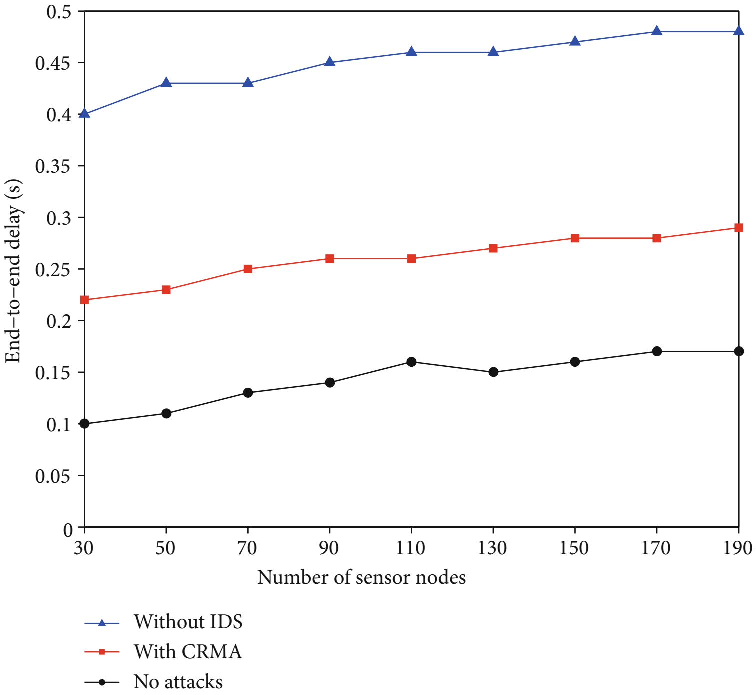

FIGURE 14: End-to-end delay with CRMA and without IDS.

The performance of networks is significantly affected by the malicious nodes [31]. In this paper, it is divided into three levels according to the percentage of malicious nodes. There is a low percentage of malicious nodes when the number of attack nodes is 5%~10% of the total nodes, and there is a medium percentage of malicious nodes when the number of attack nodes is 10%~30% of the total nodes. When the number of attack nodes is 30%~50% of the total nodes, there is a high percentage of malicious nodes.

Figure 5 shows the true positive rate (TPR) of CRMA intrusion detection system under different percentages of malicious nodes. The TPR of the system decreases as the percentage of malicious nodes increases.

Figure 6 shows the false positive rate (FPR) of CRMA intrusion detection system under different percentages of malicious nodes. The FPR of the system decreases as the percentage of malicious nodes increases.

The experimental results show that CRMA has a fast convergence rate. Table 4 shows an example of the value of the objective function of each round in the process of iteration. It can be seen that the value of the objective function gradually decreases, and the difference of the value of the objective function is approximately equal to 0.

In this paper, ARMA [25] and NeTMids [26] are compared with CRMA. ARMA predicts the traffic attributes of the WSN and only detects one type of attribute. The packet forwarding rate is selected as an attribute of ARMA. Among the above four intrusion attacks, only the sinkhole attacks will affect the packet forwarding rate. Therefore, the ARMA and CRMA algorithms compare the detection results under sinkhole attacks.

Figure 7 shows the true positive rates of ARMA and CRMA under sinkhole attacks and the aforementioned hybrid attacks (multiple attacks). It can be seen that the ARMA algorithm has a high TPR when the number of nodes is small and a low TPR when the number of nodes is large. The TPR of CRMA is much higher than that of ARMA under multiple attacks. Therefore, CRMA will be a better choice when there are more nodes or multiple attacks in the WSN.

Figure 8 shows the false positive rates of ARMA and CRMA under sinkhole attacks and multiple attacks. When the number of nodes is large, the CRMA intrusion detection algorithm has very low false positive rates for the detection of sinkhole attacks and multiple attacks. In practical applications, the types of attacks are unknown, and the number of nodes maybe very large. At this time, ARMA is not a good choice.

Figure 9 shows the false negative rates (FNR) of ARMA and CRMA under sinkhole attacks and multiple attacks which can be obtained by combining Figure 7 with formula (27). Figure 10 shows the true negative rates (TNR) of ARMA and CRMA under sinkhole attacks and multiple attacks which can be obtained by combining Figure 8 with formula (28). The FNR of ARMA is much higher than that of CRMA under multiple attacks.

The CRMA is compared with the NeTMids [26] intrusion detection algorithm, which uses different attributes of the WSN to detect different attacks. Figure 11 shows the true positive rates of NeTMids and CRMA under the above-mentioned four hybrid attacks (multiple attacks). It can be seen that the true positive rates of NeTMids are significantly lower than those of CRMA.

Figure 12 shows the false positive rates of NeTMids and CRMA under multiple attacks. The NeTMids algorithm has relatively higher false positive rates. Although the NeTMids algorithm is relatively simple and consumes fewer resources, the intrusion detection results are not as good as those of CRMA, and CRMA can detect unknown attacks through the detection of change rates of attributes.

Packet delivery ratio (PDR) is defined as the ratio of the total data packets received to the number of data packets sent [31]. The performance of the WSN is also studied by analyzing the PDR. Figure 13 illustrates the PDR with CRMA and without IDS. The performance of the PDR without any malicious nodes is also presented for comparison. The PDR dramatically decreases from 92% to 43% in the presence of an attacker in WSN. The use of CRMA improves the delivery performance of the system packet from 43% to 85%.

The performance of the network is also studied by analyzing the average end-to-end delay (EED). Figure 14 illustrates the average EED with CRMA and without IDS. The EED dramatically increases in the presence of attacks. The use of CRMA reduces the EED of the WSN.

5. Conclusion

The intrusion detection algorithm based on the change rates of multiple attributes (CRMA) can detect multiple attacks including known and unknown types simultaneously. In CRMA, the Normal Change Rate is calculated by minimizing the weighted deviation between the Observed Change Rate and the normal one through convex optimization. We also give proof that CRMA will converge to a fixed value during the iterative process. Especially in the case where multiple attacks exist simultaneously, the true positive rates of CRMA are 88%~95%. Compared with ARMA and NeTMids, the CRMA has robust detection performance under multiple attacks.

Further, we will improve the CRMA intrusion detection algorithm to reduce its computational complexity and storage requirements. How to set the threshold in CRMA and other parameters according to the actual situation is also a research direction.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was partly funded by the National Natural Science Foundation of China (61971031) and the Scientific Research Projects of Ordos Institute of Technology (KYYB2018006).

References

[1] P. Gope and T. Hwang, “BSN-Care: a secure IoT-based modern healthcare system using body sensor network,” *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[2] M. al Ameen, J. Liu, and K. Kwak, “Security and privacy issues in wireless sensor networks for healthcare applications,” *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[3] K. A. Kumar, A. V. N. Krishna, and K. S. Chatrapati, “New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks,” *Journal of Information & Optimization Sciences*, vol. 38, no. 2, pp. 341–365, 2017.

[4] D. V. Queiroz, M. S. Alencar, R. D. Gomes, I. E. Fonseca, and C. Benavente-Peces, “Survey and systematic mapping of industrial wireless sensor networks,” *Journal of Network & Computer Applications*, vol. 97, pp. 96–125, 2017.

[5] M. C. Chen, W. R. Chang, H. T. Lin, and H. H. Lee, “Design and performance evaluation of aquatic-pollution monitoring scheme over a waterborne wireless sensor network,” *Computer Communications*, vol. 40, pp. 51–64, 2014.

[6] F. Sadoughi, A. Behmanesh, and N. Sayfouri, “Internet of things in medicine: a systematic mapping study,” *Journal of Biomedical Informatics*, vol. 103, article 103383, 2020.

[7] H. Radhappa, L. Pan, J. Xi Zheng, and S. Wen, “Practical overview of security issues in wireless sensor network applications,” *International Journal of Computers and Applications*, vol. 40, no. 4, pp. 202–213, 2018.

[8] N. 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, Article ID 167575, 2013.

[9] F. Raza and S. Bashir, “Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN,” in *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 623–628, Islamabad, Pakistan, 2015.

[10] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: real-time intrusion detection in the Internet of things,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[11] P. Ganeshkumar, K. P. Vijayakumar, and M. Anandaraj, “A novel jammer detection framework for cluster-based wireless sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, 2016.

[12] X. Jin, J. Wei, and W. Tong, “Research on intrusion detection algorithm for wireless sensor networks,” *IOP Conference Series: Materials Science and Engineering*, vol. 452, 2018.

[13] S. Shanthi and E. G. Rajan, “Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks,” in *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, pp. 426–431, Dehradun, India, 2016.

[14] R. Mitchell and I. R. Chen, “A survey of intrusion detection in wireless network applications,” *Computer Communications*, vol. 42, no. 4, pp. 1–23, 2014.

[15] A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin, and H. Song, “Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks,” *IEEE Access*, vol. 6, pp. 5688–5694, 2018.

[16] A. Ghosal and S. Halder, “A survey on energy efficient intrusion detection in wireless sensor networks,” *Journal of Ambient Intelligence & Smart Environments*, vol. 9, no. 2, pp. 239–261, 2017.

[17] B. Ahmad, W. Jian, Z. A. Ali, S. Tanvir, and M. S. A. Khan, “Hybrid anomaly detection by using clustering for wireless sensor network,” *Wireless Personal Communications*, vol. 106, no. 4, pp. 1841–1853, 2019.

[18] Y. Hu, Y. Wu, and H. Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN," *Wireless Sensor Network*, vol. 6, no. 11, pp. 237–248, 2014.

[19] M. Motamedi and N. Yazdani, "Detection of black hole attack in wireless sensor network using UAV," in *2015 7th Conference on Information and Knowledge Technology (IKT)*, pp. 1–5, Urmia, Iran, 2015.

[20] F. Gara, L. B. Saad, and R. B. Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 276–281, Valencia, Spain, 2017.

[21] O. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[22] Y. Cao, L. Han, X. Zhao, and X. Pan, "AccFlow: Defending against the Low-Rate TCP DoS Attack in Wireless Sensor Networks," 2019, https://arxiv.org/abs/1903.06394.

[23] Q. Yaseen, F. Albalas, Y. Jararwah, and M. Al-Ayyoub, "Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 4, 2018.

[24] A. Rehman, S. U. Rehman, and H. Raheem, "Sinkhole attacks in wireless sensor networks: a survey," *Wireless Personal Communications*, vol. 106, no. 4, pp. 2291–2313, 2019.

[25] J. Peng, Q. Yu, and M. He, "WSN intrusion detection technology based on traffic prediction," *Computer Applications & Software*, vol. 2, pp. 310–313, 2016.

[26] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection system for WSN," *Procedia Computer Science*, vol. 63, pp. 183–188, 2015.

[27] Z. Yu and J. J. P. Tsai, "A framework of machine learning based intrusion detection for wireless sensor networks," in *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, pp. 272–279, Taichung, Taiwan, 2008.

[28] T. H. Tsang, D. M. Himmelblau, and T. F. Edgar, "Optimal control via collocation and non-linear programming," *International Journal of Control*, vol. 21, pp. 763–768, 2016.

[29] M. Poggiolini and A. Engelbrecht, "Application of the feature-detection rule to the negative selection algorithm," *Expert Systems with Applications*, vol. 40, no. 8, pp. 3001–3014, 2013.

[30] Z. Sun, Y. Xu, G. Liang, and Z. Zhou, "An intrusion detection model for wireless sensor networks with an improved V-detector algorithm," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 1971–1984, 2018.

[31] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Networks*, vol. 24, no. 5, pp. 1821–1829, 2018.