**Cooperative malicious network behavior recognition algorithm in E-commerce**

*BY- Man Zhoua , Lansheng Hana,∗ , Hongwei Lua , Cai Fua , Dezhi An*

**SUMMARY OF RESEARCH PAPER**

BY UTSAV AGRAWAL

**1.Introduction:**

Collaborative malicious network behaviours, i.e. malicious registration, false authentication, fraudulent transaction and data theft, pose a disastrous threat to e-commerce security.

A classical clustering algorithm, k-means has been widely used in malicious identification. Its main function is to classify a given data set into a predetermined number of clusters. Swarm intelligence algorithm is a representative optimization algorithm, which is efficient, robust, adaptive, and is highly suitable for dealing with global optimization problem.

This paper combines the quantum behaviour-based PSO method with the k-means algorithm to enhance the efficiency and effectiveness of the malicious behaviour detection.

**2.Cooperative malicious network behaviour and its identification:**

The specific malicious behaviours included in the different modules are demonstrated as follows:

1. User module: malicious registration, fraudulent authentication and forgery of user information.

2. Commodity module: counterfeit and shoddy commodities to make exorbitant profits.

3. Order module: imperfect logistics and order capital flow system restricts the transaction efficiency and induces malicious behaviours.

4. Marketing module: malicious price hype often confuse original price, offer false discounts and promotions, or even maliciously denigrate against competitor.

Current malicious detection objects are still limited to the level of a single-node system.

The normal transaction process shows strong orderliness and consistency, but malicious transactions are not. For example, orders of malicious transactions are incomplete or untrace- able. The orderliness and consistency of the transaction process expand the time domain and space for the exploration of malicious features, because it enables to search cooperative malicious features process-by-process according to the information flow of e-commerce transaction.

Since different groups exhibit diverse transaction patterns, clustering algorithms contribute to classify group with similar transaction patterns into the same category, thereby identifying collaborative malicious network behavior. The k-means algorithm is scalable and efficient, however, the parameter value k must be determined in advance.

**3.Information transfer entropy based on e-commerce transaction**

*Information transfer entropy (ITE)* is the amount of directed transfer of information between two random processes. ITE is mainly composed of two parts:

1. The update of neighbor information before communication

2. The change of neighbor information state due to the social activities.

In the identification algorithm of collaborative malicious network behavior, the paper first determines the cluster nodes with greater ITE, and designates them as the cluster centers, then combines the k-means algorithm with rapid convergence ability to complete the clustering.

The fixed point theorem in the probability metric space is used to prove the existence of cooperative malicious behavior and the theoretical feasibility of designating the cluster nodes with the greater ITE as the cluster centers.

**4.Fixed point theorem based on cooperative malicious behavior recognition algorithm**

Rather than assuming, we should identify it first. Fixed point theorem based on *cooperative malicious behavior recognition* algorithm (*CMBR*).

*4.1 Fixed point theorem in probability metric space*

* Definition 1 - Probability metric space
* Definition 2 - Menger probability measurement space (M-PM space)
* Definition 3 - Measurable M-PM space
* Definition 4 - Complete probabilistic metric space
* Definition 5 - Nearest neighbour.
* ***Theorem 1*** -The existence of fixed point

Search for fixed point is an convergent process. CMBR is iterative process which which unique center for each cluster.

*4.2. Proof of fixed point theorem based on cooperative malicious behavior recognition algorithm*

* **Theorem 2**. Combined with the example of malicious complaint event, the probability metric space (S, F) is equivalent to the e-commerce platform, and normal or malicious transaction are performed on the platform.
* **Theorem 3**. The completeness of the M-PM space needs to satisfy the convergence, while the exploration of malicious complaint events is also a convergent process that a large amount of behavioral data are constantly analyzed to narrow down the search scope. When the distinguishing features of the data are identified, the search scope will reduce unceasingly, and this search process is also a convergent process.
* **Theorem 4.** When the single particle of the CMBR algorithm is bounded, there’s only a single fixed point s∗ in S that makes the H(s∗) get the maximum value. By this time, the fixed point is the cluster center and the sequence of iterations is convergent to s∗.

**5. Identification algorithm of cooperative malicious network behavior**

*5.1 Cluster center selection algorithm*

-PSO helps improve spatial distribution and cooperative state of paticle nodes.

- In the cluster center selection algorithm, the ITE of nodes is taken as the Fitness Function, that is, the greater the node’s ITE is, the higher the probability that the node becomes the cluster center.

**Algorithm 1** Cluster centers selection algorithm.

**Algorithm 2** Clustering algorithm to identify cooperative malicious network behavior.

**6. Conclusion and future work**

This paper uses

-the quantum behavior-based PSO method with global search capability, which is combined with the rapidly converging k-means method to improve efficiency and effectiveness.

*Advantages*-

(1) It indicates that the current malicious transaction behaviors are collaborative and proves the existence of collaborative malicious group

(2) It introduces the ITE to designate the nodes with the greater ITE in the cluster as the cluster centers and proves the theoretical feasibility of this algorithm

(3) Quantum behavior-based PSO method is used to extract cluster centers to improve the recognition accuracy of collaborative malicious behavior