**1)Intrusion Detection System based on KNN algorithm:**

K-Nearest Neighbor is one amongst the only Machine Learning algorithms supported Supervised Learning technique. This algorithm assumes the similarity between the new case/data and available cases and put the new case into the category that's most just like the available categories. It stores all the available data and classifies a brand-new datum supported the similarity. This implies when new data appears then it will be easily classified into a well suite category by using K- NN algorithm.

In this survey, we use data processing technology to style and implement the intrusion detection system. The system has three advantages: (1) *K*-value for mining has little effect on the results. (2) the cutoff value accustomed to determining the abnormal node is simple to work out. (3) the algorithm is fast and efficient.

***1.1. An overview of KNN algorithm:*****

Figure 1: Schematic diagram of KNN intrusion detection algorithm.

The wireless sensor network intrusion detection algorithm supports the KNN classification algorithm if the cutoff value is set to K. The K value refers to the number of most adjacent nodes in a graph. The cutoff value refers to the point at which the node is judged to be abnormal. This is done by taking the feature vector describing the node and dividing it by the feature vector describing the average node. There are n nodes in the network, including abnormal and normal nodes. The Euclidean distance between two nodes is the distance between those nodes in the network.

***The algorithm calculation:***

1)Select the number K of the neighbors

2)Calculate the Euclidean distance (d = √[(x2 – x1)2 + (y2 – y1)2]) of K number of neighbors

3)Choose the K nearest neighbors based on the calculated Euclidean distance.

4)From these k neighbors, count the number of the data points in each category.

5) The new data points are assigned to the majority category.

***1.2. System implementation of intrusion detection algorithm:***

The intrusion detection system includes various modules, including a wireless network interface module, a data storage module, an analysis and judgment module, and a response module. The wireless network interface module is implemented by GAINZ wireless sensors. The data storage module receives data from the wireless network interface module, extracting statistical information, and storing the information into the data domain for use by the analysis and judgment module. The intrusion response module adds abnormal nodes to the red list and sends the red list to the wireless network interface unit, and a red list will be broadcast that records the abnormal nodes in the network; After that, you will not receive all regular nodes or hires Routing RREQ messages from abnormal nodes. At the same time, the red list will be forwarded to other nodes to help with the flooding attack response.

***1.3. System Test node:***

The network test model is composed of a detection node, several common sensor nodes, and a few attacking sensor nodes. The detecting node is a computer system and a single sensor node that receives messages from all the other sensor nodes. The sensor nodes are responsible for the collection and detection of network data, providing alarm information, and making a response. The common sensor nodes are responsible for establishing the test network using the AODV protocol. Attackers are sending a lot of Requests for Resources packets to the network, which is causing the network to become overloaded and using up resources away from other nodes.

**References:**

1. <https://www.researchgate.net/publication/2948052_KNN_Model-Based_Approach_in_Classification>
2. <https://www.hindawi.com/journals/jece/2014/240217/> [1]