Contribution ID: **631** Type: **Paper**

Information Fusion Analysis of Cyber Attack Identification Based on D-S Evidence Theory

The control of nuclear power plants (NPPs) is increasingly dependent on digital Instrumentation and Control (I&C) systems. The digitization has brought a series of benefits to the I&C systems of the NPPs, and it also results in a growing and previously unforeseen cyber attack threat. Even if the I&C system adopts preventive measures such as physical isolation, the risk of cyber attack is still unavoidable, which has seriously threatened the safe and stable operation of the power plants.

Cyber attack identification of I&C systems is the first step in cyber attack assessment. Different types of attacks have different impact ranges, urgency, consequences, and countermeasures. Therefore, cyber attack identification is also the basis and premise for correct and real-time attack response.

As the network structure and system functions of the I&C system become more and more complex, the attack methods are also more and more diversified, and the representation of the attack is usually reflected in multiple aspects, which increases the difficulty of cyber attack identification. The attack identification by a single information source is difficult to identify various types of cyber attacks. It is necessary to integrate information from multiple sources through information fusion to obtain more comprehensive and reliable cyber attack identification.

On the other hand, cyber attack information from different sources may have some ambiguity, and even the opposite description. Reasonable collection and screening are needed to fully exploit information, eliminate conflicting information, and focus on mutually validated information to obtain more accurate cyber security awareness.

This paper will use D-S evidence theory to integrate data and information from different sources, including real-time network traffic data, equipment status data, process data, and expert experience data. These data and information will be incorporated into a unified fusion framework and preprocessed in the same format, so that information from different sources can be expressed and interpreted under this framework. The Dempster's Combination Rule is used to synthesize the basic probability distributions of each evidence, and the Belief function and Plausibility function of each hypothesis are obtained, and the attack type identification is completed.

We will select three typical types of cyber attacks as the objects to be identified, and select the associated multiple measurement for each type of cyber attack as its attributes, which may be shared by different types of attacks. To obtain the basic probability assignment (BPA) of each attribute, it is necessary to solve the multi-attribute decision problem between the cyber attack type and the attributes. This paper intends to adopt the triangular fuzzy number: firstly, the samples of the three attack types are randomly divided into training samples and test samples, then the triangular fuzzy number model on each attribute of the training samples is constructed, and the test samples are matched with the model, and finally the fusion the BPA of each attribute to complete the modeling process.

Gender

State

China

Authors: Mr GUO, Chao (Institute of Nuclear and New Energy Technology of Tsinghua University, Beijing 100084, China); LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University.); JIA, Qianqian; ZHOU, Shuqiao; CHEN, Fan; HUANG, Xiaojin

Presenter: Mr GUO, Chao (Institute of Nuclear and New Energy Technology of Tsinghua University, Beijing 100084, China)

Track Classification: CC: Information and computer security considerations for nuclear security