Journal of Information Security and Applications 40 (2018) 173–182

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security

Dipak Kumar Jana[a,*], Ramkrishna Ghosh[b]

[a] Department of Engineering Science, Haldia Institute of Technology, Haldia Purba Midnapur West Bengal, 721657, India
[b] Department of Information Technology, Haldia Institute of Technology, Haldia West Bengal, India

ARTICLE INFO

Article history:

Keywords:
Type-2 Fuzzy inference system
Type-2 Fuzzy logic
Risk assessment
Statistical analysis

ABSTRACT

In this research paper, we have developed a novel interval type-2 fuzzy logic controller (IT2FLC) for improving risk assessment model for cyber security. The proposed IT2FIS implements this model to gain the total risk for such cyber security system which is combined with three sub models as a) Overall Capabilities, which is controlled by Capabilities, Intent, Targeting, b) Overall Likelihood, which depends on Vulnerability, Overall Capabilities and finally c) risk, which is measured by Overall Likelihood, Impact. Combining these three sub models, we have formulated and optimized the total risk assessment for a cyber security. This approach will have an enhanced control to forecast the possibility of risk assessment of cyber security despite the uncertainty in the data and information of cyber security due to various risks caused by the impacts of criminal activities depending upon the types of the offence, the victim and origin of the effects of the cyber crime. Finally, validity of the proposed model is discussed with the help of statistical analysis, Adaptive neuro-fuzzy inference system (ANFIS) and Multiple Linear Regression (MLR).

1. Introduction

Cyber security is the topic of global significance and attention. Cyber security is a very difficult job that depends on domain knowledge and needs cognitive abilities to decide most probable threats from huge amounts of network data. Nowadays the most significant matter that different organizations are facing, is cyber attacks caused by Denial of Service (DoS), Distributed Denial of Service (DDoS), malware, spam, Phishing attack. The series and span of those unfamiliar attacks produce the requirement of different organizations to prioritize the method in which they guard themselves. In this concern each organization requires to ponder the threats that they are often at risk and perform in such a technique as to reduce the vulnerabilities as much as possible [6]. Andrew et al. [7] have considered three possible decision support techniques for security managers to deal with this challenge. They developed techniques based on game theory, combinatorial optimisation, and a hybrid of these two methodologies. Their model begins by building a structure where they can examine the usefulness of a cyber security control as concerns the guard of various assets observed as targets in existence of commodity threats.

Rossouw et al. [8] have disagreed that, even if there is a considerable overlap between cyber security and information security, these two concepts are not completely equivalent. Furthermore, they have discussed cyber security goes beyond the limitations of conventional information security to contain not only the guard of information resources, but also that of other assets, including the person him/herself.

Noam et al. [9] have investigated how information in network operations and information security manipulate the detection of intrusions in a simple network. They have developed a simplified Intrusion Detection System (IDS), which permit them to observe how individuals with or without knowledge in cyber security perceive malevolent actions and speak out an attack based on a sequence of network events. Their outcomes showed that more knowledge in cyber security helped the correct detection of malevolent actions and reduced the fake categorization of benevolent events as malevolent.

Zhuo et al. [10] have focused on reviewing and analysis of safety needs, network vulnerabilities, attack countermeasures, safe communication protocols and robust architectures in the Smart Grid. They have provided a bottomless discussion and analysis of security vulnerabilities and solutions in the Smart Grid and upcoming research directions for Smart Grid security.

According to McHugh [11], the cyber-attack is the disturbance of computers' normal performance and the loss of responsive in-

* Corresponding author. .
E-mail addresses: dipakjana@gmail.com (D.K. Jana), ramkr.ghosh@gmail.com (R. Ghosh).

https://doi.org/10.1016/j.jisa.2018.04.002
2214-2126/

formation through malevolent network actions is becoming more extensive. Protecting these attacks is an important part of the Information Technology supremacy performed by cyber analysts, as many private organizations have shifted to distributed systems.

According to Burden et al. [12], due to cyber crimes progression, recognizing and measuring security risk is vital to access data from innovative technologies, and also attempting to realize how technologies can be neglected. Consequently, there is a need to build up a particular cyber security risk evaluation model to attempt over those cyber threats.

According to Vagoun et al. [13], the uppermost cyber vulnerability to individuals, private and government organizations is predictable as malware. Cyber attackers commence malware attacks by dint of sharing channels such as emails, permitting the malware to develop the host machines by causing malfunctions. The malevolent software may also be part of larger botnets that act as zombie which help the originator to carry out additional crimes like sharing spam and viruses.

Recently, Cherdantseva [40] have developed the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. It describes the essence of the methods and they analyse in terms of aim; application domain; the stages of risk management addressed; key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support for cyber security.

Yulia et al. [14] have reviewed the status of the skill in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. They have examined twenty-four risk assessment techniques exploited for a SCADA system. They have described the necessity of the methods and after that examined them in terms of application domain key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support. Based on the investigation, they have suggested a spontaneous idea for the classification of cyber security risk assessment methods for SCADA systems.

Atul et al. [15]. have focused on cyber security promising trends whereas accepting current technologies such as mobile computing, cloud computing, e-commerce, and social networking. In their article they have represented the issues and challenges of cyber security due to lack of management between Security agencies and the crucial IT Infrastructure. In spite of the above mentioned development, lacunas still exist in the formulation and solution methodology for cyber security model, which have been resolved in this model as:

- The system uses interval type-2 fuzzy sets in premises and consequences of rules.
- Interval type-2 fuzzy logic control (IT2FLC) approach for improving risk assessment model of cyber security.
- In T2FLC assists to trace inputs for Model 1 are Intent, Targeting, capabilities, Model 2 are Overall Capabilities, vulnerabilities, Model 3 are Overall Likelihood, impact and final output risk in a well-organized manner for building the inference train, so that system output can be predicted the risk.
- Qualitative factors responsible for improving System Output assessment can be easily included in the type-2 fuzzy prediction model for improving accuracy.
- Validity of the proposed model is done with the help of Statistical Analysis and Multiple Linear Regression.
- A robust IT2FLC model for adapting to pattern changes while maintaining existing rules for improving risk assessment of cyber security model.

The main contribution of this paper is a comparative study based on generalized type-2 fuzzy logic for the design and implementation of fuzzy controllers, which allows for better modeling of the uncertainty that exists in achieving control for cyber security. Also, the comparative study of T1FLC, and IT2FLC has been carried out.

2. Notations and abbreviations

The following notations are used to describe the proposed model.

(i) $T2FIS$ = type-2 fuzzy inference system.
(ii) $MFIS$ = Mamdani fuzzy inference system.
(iii) R^2 = coefficient of determination.
(iv) $RMSE$ = root mean square error.
(v) MAE = mean absolute error.
(vi) $MAPE$ = mean absolute percentage error.
(vii) $ANFIS$ = adaptive neuro-fuzzy inference system
(viii) MF = membership function.
(ix) Dos = denial-of-service
(x) MLR = Multiple Linear Regression.

3. Related research and some preliminary ideas

The type-2 fuzzy soft computing is a collection of methodologies, which aim to exploit tolerance for imprecision, uncertainty and partial truth to achieve tractability, robustness and low solution in cyber security. TYPE-2 fuzzy sets (T2 FSs), originally introduced by Zadeh [30], provide additional design degrees of freedom in Mamdani and TSK fuzzy logic systems (FLSs), which can be very useful when such systems are used in situations where lots of uncertainties are present (cf. [16–29]). The resulting type-2 fuzzy logic systems (T2 FLS) have the potential to provide better performance than a type-1 (T1) FLS (e.g., [33–36]). To-date, because of the computational complexity of using a general T2 FS, most people only use interval T2 FSs in a T2 FLS, the result being an interval T2 FLS (IT2 FLS) [32]. The computations associated with interval T2 FSs are very manageable, which makes an IT2 FLS quite practical [38]. Quite often, the knowledge used to construct rules in a fuzzy logic system (FLS) is uncertain. This uncertainty leads to rules having uncertain antecedents and/or consequents, which in turn translates into uncertain antecedent and/or consequent membership functions.

For examples:

a) A fuzzy logic modulation classifier described in [37] centers type-1 Gaussian membership functions at constellation points on the in-phase/quadrature plane. In practice, the constellation points drift. This is analogous to the situation of a Gaussian membership function (MF) with an uncertain mean. A type-2 formulation can capture this drift.

b) Previous applications of FL to forecasting do not account for noise in training data. In forecasting, since antecedents and consequents are the same variable, the uncertainty during training exists on both the antecedents and consequents. If we have information about the level of uncertainty, it can be used when we model antecedents and consequents as type-2 sets.

c) When rules are collected by surveying experts, if we first query the experts about the locations and spreads of the fuzzy sets associated with antecedent and consequent terms, it is very likely that we will get different answers from each expert. This leads to statistical uncertainties about locations and spreads of antecedent and consequent fuzzy sets. Such uncertainties can be incorporated into the descriptions of these sets using type-2 membership functions. In addition, experts often give different answers to the same rule-question; this results in rules that have the same antecedents but different consequents. In such a case, it is also possible to represent the output of the IT2FLS built from these rules as a fuzzy set rather than a crisp number. This can also be achieved within the type-2 framework.