Research Journal of Applied Sciences 7 (5): 282-285, 2012
ISSN: 1815-932X

Functional Dependency and Performance Strategy in Deception Detection using Fuzziness and Uncertainty with Underlying Randomness Syndromes

[1]S. Rajkumar, [2]V. Narayani and [1]S.P. Victor
[1]Bharathiar University, CSE/NIET, Coimbatore, Tamilnadu, India
[2]CS/St. Xaviers College, Tirunelveli, Tamilnadu, India

Abstract: Deception detection is an essential strategy for the efficient and secure communication. The implementation of soft computing techniques such as fuzzy logic, uncertainty, randomness, neural networks and genetic algorithm plays a vital role in identifying the deception in an information sharing system. The combined implementation of fuzziness, randomness and uncertainty provides the maximum output than compare it with the individual implementations is an obvious result. In this study, researchers analyze the combined performance and dependency computation for the combined application of randomness, fuzziness and uncertainty towards deception detection. Researchers considers two different domains for the proposed model and the final results are discussed.

Key words: Deception, detection, uncertainty, randomness, fuzziness

INTRODUCTION

Deception Detection is a tedious process when researchers perform manual information handling system (Mitnick and Simon, 2002). When we implement the soft computing tools such as fuzzy logic, uncertainty and randomness as a combined application which produces the good results when compare it with the individual implementation (Bond, 2006).

Fuzzification: Fuzzy sets have movable boundaries, i.e., the elements of such sets not only represent true or false values but also represent the degree of truth or degree of falseness for each input (Luber *et al*., 2009). Fuzzy logic is the part of artificial intelligence or machine learning which interprets a human's actions. Computers can interpret only true or false values but a human being can reason the degree of truth or degree of falseness. Fuzzy models interpret the human actions and are also called intelligent systems (Burgeon and Qin, 2006).

Randomness: Random can be defined as having no definite aim or purpose not sent or guided in a particular direction; made, done, occurring, etc., without method or conscious choice; haphazard. This concept of randomness suggests a non-order or non-coherence in a sequence of symbols or steps such that there is no intelligible pattern or combination (McCabe *et al*., 2011).

Uncertainty: Uncertainty must be taken in a sense radically distinct from the familiar notion of risk from which it has never been properly separated. Although, the terms are used in various ways among the general public, many specialists in decision theory, statistics and other quantitative fields have defined uncertainty, risk and their measurement as:

Uncertainty: A state of having limited knowledge where it is impossible to exactly describe existing state or future outcome, more than one possible outcome.

Measurement of uncertainty: A set of possible states or outcomes where probabilities are assigned to each possible state or outcome.

Risk: A state of uncertainty where some possible outcomes have an undesired effect or significant loss.

Measurement of risk: A set of measured uncertainties where some possible outcomes are losses and the magnitudes of those losses variables. Uncertainty represents the situation where neither the probability distribution of a variable nor its mode of occurrence is known (Mitnick and Simon, 2002).

MATERIALS AND METHODS

The randomness acts as an underlying feature which uplifts the fuzziness and uncertainty component dependencies in a deception detection system and it is illustrated in Fig. 1.

Corresponding Author: S. Rajkumar, Bharathiar University, CSE/NIET, Coimbatore, Tamilnadu, India

The Mathematical Randomness Model adopts several techniques for implementing it in deception detection. Researchers mainly focuses on a predefined model as Entropy Model with a choice of probability theory and also the alternative as a randomized algorithm which resembles the Fig. 1 proposed model.

Randomness Model and its computation time: The implementation of Randomness Model consumes the following mathematical strategies:

- R1: Linear-entropy-2 units-(allocation and computation)
- R2: Optimal-probabilistic-3 units-(design, allocation and computation)
- R3: Complex-randomized algorithm-5 units (design, substitution, implementation, evaluation, extraction)

Fuzziness Model and its computation time: The fuzziness in identifying deception from an information sharing system aims towards the association of fuzzy membership value which can be implemented with the following combined group of techniques:

- F1: Assumption-2 units (design and implementation)
- F2: Category-2 units (design and implementation)
- F3: Anamoly-2 units (design and implementation)

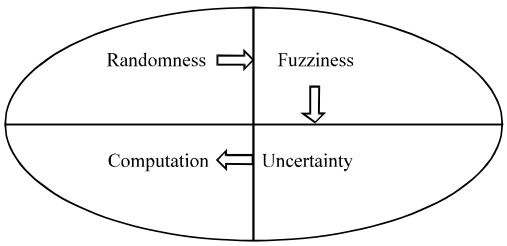

Fig. 1: Proposed Model

- F4: Condition-5 units (design, substitution, implementation, evaluation, extraction)
- F5: Operation rules-5 units (design, substitution, implementation, evaluation, extraction)
- F6: Allocation-5 units (design, substitution, implementation, evaluation, extraction)
- F7: Probableness-7 units (design, substitution, implementation, selection, computation, evaluation, extraction)

Uncertainty Model and its computation time: The Uncertainty evaluation can be done on an information sharing system for t5he identification of deception detection can be carried out by the following techniques:

- U1: Random uncertainty = suspicious (max factors-min factors)/total factors-2 units-(design and implementation)
- U2: Number of disbelief factors/total no of factors-3 units-(design, implementation and computation)
- U3: Probabilty measures-5 units-(design, substitution, implementation, evaluation, extraction)

RESULTS AND DISCUSSION

In the experiment, researchers consider two domains from the electronic communication media; initially we implement the proposed research methodology for the Fake Short Messaging Service System. The analysis is shown in Table 1. Finally, researchers implement the proposed research methodology for SPAM EMAIL Analysis. The analysis is shown in Table 2.

In the proposed research model experiment we used categorized factor schema evaluation for the efficient and flexible computation. The general observations are discussed in study the impact scope of the combined implementation using Table 1 and 2 from the experiment domain is as also shown for a domain containing single factor to 10 factors schema:

Table 1: Fake SMS domain computation

Deception component	Randomness factor type	Fuzzified analysis requirement	Uncertainty computation	Computational units
Message frequency	Linear	F1,F2,F3	U1	2+(2+2+2)+2 = 10
Message length	Optimal	F1,F2,F3,F4,F5,F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Message sender	Complex	F1,F2,F3,F4,F5,F6,F7	U1,U2,U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Age/Sex/Location				
Message type	Linear	F1,F2,F3	U1	2+(2+2+2)+2 = 10
Message motive	Complex	F1,F2,F3,F4,F5,F6,F7	U1,U2,U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Message multimedia content	Linear	F1,F2,F3	U1	2+(2+2+2)+2 = 10
Message language	Optimal	F1,F2,F3,F4,F5,F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Message time	Linear	F1,F2,F3	U1	2+(2+2+2)+2 = 10
Message Model/Prototype	Optimal	F1,F2,F3,F4,F5,F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Message mobile network	Linear	F1,F2,F3	U1	2+(2+2+2)+2=10
Total	Linear-5	F1-10,F2-10,F3-10	U1-10	223 Units
	Optimal-3	F4-5,F5-5,F6-5	U2-5	-
	Complex-2	F7-2	U3-2	-

Table 2: Spam mail domain computation

Deception component	Randomness factor type	Fuzzified analysis requirement	Uncertainty computation	Computational units
Prize/Lottery/Travel trip	Optimal	F1, F2, F3, F4, F5, F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Friend invitation	Complex	F1, F2, F3, F4, F5, F6, F7	U1,U2,U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Love/Marriage/Sex	Linear	F1, F2, F3	U1	2+(2+2+2)+2 = 10
E-shopping	Optimal	F1, F2, F3, F4, F5, F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Magazines/Club/Subscription	Linear	F1,F2, F3	U1	2+(2+2+2)+2 = 10
Movie/songs/Video/File downloads	Optimal	F1,F2, F3, F4, F5, F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Help self/Others/Sympathy	Complex	F1,F2, F3, F4, F5, F6, F7	U1,U2,U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Charity/Welfare/Disaster donation	Complex	F1,F2, F3, F4, F5, F6, F7	U1,U2, U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Games/Play or download	Optimal	F1,F2, F3, F4, F5, F6	U1,U2	3+(2+2+2+5+5+5)+(2+3) = 29
Advertisements/Marketing	Complex	F1,F2, F3, F4, F5, F6, F7	U1,U2,U3	5+(2+2+2+5+5+5+7)+(2+3+5) = 43
Total	Linear-2	F1-10, F2-10, F3-10	U1-10	308 Units
	Optimal-4	F4-8,F5-8, F6-8	U2-8	-
	Complex-4	F7-4	U3-4	-

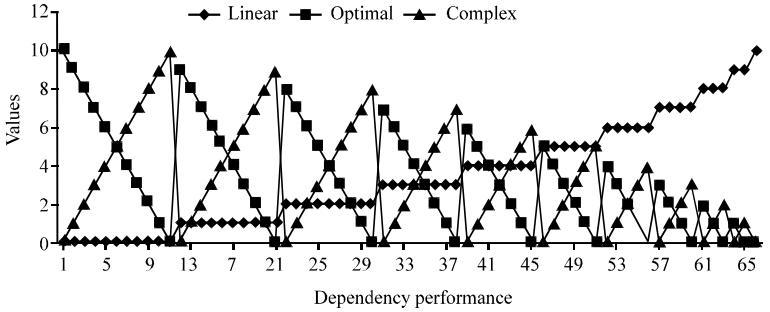

Fig. 2: Intra Dependency Performance of Randomness Model

- Linear-min-10-max-100 units-best-case/minimum evaluation units. If all the factors are linear
- Optimal-10-290 units-average case/average evaluation units. If all the factors are optimal
- Complex-10-430units-worstcase/maximumevaluation units. If all the factors are complex

Researchers don't expect all the randomness models are of trivial issues. The real-time application domain is a mixture of all the classes found in the randomness, fuzziness and uncertainty models so that the corresponding domains of mixture cases are considered in the experimental domain. The performance analysis chart for intra dependency is shown in Fig. 2.

Finally, the performance analysis chart for interdependency of randomness, fuzziness and Uncertainty are shown in Fig. 3. When compare with Fuzziness Model, the Uncertainty and Randomness Model incorporates less computational structures for the evaluation of deception detection in an information processing system. But the efficiency in identifying the deceptions varies according to the choice of the domains which may be from electronic or non electronic mode of communication.

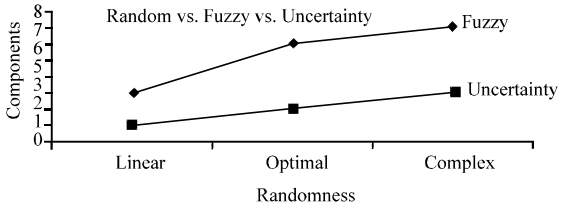

Fig. 3: Inter dependency performance of Randomness, Fuzziness and Uncertainty

CONCLUSION

In this modern era of communication we are facing deceptive information which are formed with combinational techniques of logic and illogical factors together with truth and deceitful components. The Manual deception detection is a tedious process to implement it in various level of complexities. When we are using soft computing tools for identifying deceptions, the basic observation we obtained is the functional dependency of each other.

Based on Fig. 2 and 3 result charts we arrive with a conclusion such that the Randomness Model acts as a basis for identifying the deception detection field in which Fuzziness and Uncertainty adopts itself with the

corresponding components, based on its flexibility uncertainty and fuzzy logic complexity varies with the component consumption. Communication domain with Structured Datum provides more linear factors than with the unstructured datum.

In near future, researchers will try to implement Deception Detection techniques with the combined approach of Mathematical Randomization, Fuzzy logic, Uncertainty, Genetic algorithm and Artificial intelligence to attain 100% efficiency among with the dependent characteristics.

REFERENCES

Bond, C.F. 2006. A world of lies: The global deception research team. J. Cross-culture Psychol., 37: 60-74.

Burgeon, J.K. and T. Qin, 2006. The dynamic nature of deceptive verbal communication. J. Lang. Soc. Psychol., 25: 76-96.

Luber, B., C. Fisher, P.S. Appelbaum, M. Ploesser and S.H. Lisanby, 2009. Non-Invasive brain stimulation in the detection of deception: Scientific Challenges and ethical consequences. Behavioral Sci. Law Behave, 27: 191-208.

McCabe, D.P., A.D. Castel and M.G. Rhodes, 2011. The Influence of fMRI Lie detection evidence on juror decision making. Behave. Sci. Law, 29: 566-577.

Mitnick, K.D. and W.L. Simon, 2002. The Art of Deception: Controlling the Human Element of Security. John Wiley and Sons, USA, Canada, Pages: 352.