Deceptive call recognition in a network using machine learning[1]

V. A. Narayana[2], Abhinav Chamakura[2], Ramakrishna Gandi[2]

Abstract. This paper considers the construction of an effective beam finite element for the blade as the component of cyclic symmetric system. Spontaneously sensing and thwarting deceitful calls on a network. The call history on the network is collected for a given time span, call topographies for each of the collected call history by recipient number and using machine learning to make choices for identifying whether recipient number and a call to recipient number may be deceitful. The choice model may be incorporated on network to sense and thwart deceitful calls.

Key words. Network, deceptive call recognition, machine learning.

1. Introduction

The task of ensuring the vibration reliability concerning the rotor systems of turbomachines and their elements is accompanied by the implementation of a large amount of computational studies for the set of design models. The telecommunication industry is facing lot of challenges in terms of deceptive calls communication among the network. The worldwide yearly damages due to deceptive calls or deceptive activities increasing to US$40 billion according to various survey instruments. The losses are increasing faster than the profits in small and medium sized telecom industry. To monitor full time deceptive activities, it is an overhead on the Government and non-Government organizations. To overcome this challenge an attempt made in this paper to address the problem using decision tree generation using clustering analysis and machine learning module in a cost effective way.

[1] This work was supported by the Management of CMR College of Engineering & Technology.

[2] CMR College of Engineering & Technology, Hyderabad-501401, India

2. Related work

Niall J. Conroy [2] proposes linguistic and network analysis methods deceitful counterfeit news indicator system. Linguistic methods where the content of deceptive posts is mined and examined to associated language patterns with deception and network methods likewise post meta data or organized network inquiries will be coupled to provide collective deception actions.

Anton Wiens [3] proposes user profiles are used to train for sensing deceit calls by the values of each profiles. Lacking labeling data only some algorithms can be used for deceit call sensing using supervised methods.

Iulia Lefter [4] proposes enunciation on every stage in the growth of an sentiment recognition system from the existing databases, the sentiment specific topographies which are pertinent for sentiment recognition and machine learning approaches used. Support Vector Machines(SVM) classifiers in dialogue sentiment recognition used. SVM will regulate a hyper plane exploits the boundary of the two datasets, and the trials that lie on the boundary are called support vectors to create orator sovereign cross justification framework.

Gideon Mendels [5] proposes repeatedly sensing deception from dialog. CXD exploited large-scale corpus of deceptive and non-deceptive dialog for training and assessing spectral, lexical feature sets and acoustic-prosodic, by various machine learning modules. Design a sole hybrid deep model for together acoustic and lexical topographies trained together to achieve advanced outcomes on the CXD corpus.

Larcker, D. [6] proposes estimation linguistic-based classification modules of deceptive calls during conference calls. Prediction modules are established with word groups that are revealed by earlier psychosomatic and linguistic research related to deception.

Baohua Wang [7] assessed classification modules of deceptive calls during conference calls, the model is established through word types related toward deception and by conventional arithmetical examinations. Nonetheless their performance is 60 %–70 % of linguistic topographies are useful to recognize deceptive calls.

Graaff A. J. [8] proposes finding deceptive calls from the average set of calls period and extended call period over calls by client are brief and equated to a determined threshold. A machine learning approach is used to train the best possible threshold levels. Thereby every client has own rules for prediction to sense deceptive calls.

“Life cycle of a phone fraud” proposes to produce machine learning modules to recognize the genuine type of machine/device used to make a call, the geography a call is identifies by its phone print.

Tata Communications technology software monitors to prevent deceitful activities. The software deals with fraud fighting technologies, including machine learning, big data analytics, subscriber alerts, real-time monitoring, crowd sourcing and automated reporting. When the fraud fighting software identifies a deceitful call, blocks the number across whole world wide network avoiding further deceitful activity.

David Lary [11] proposed automated detection & reporting of online auction seller deception risk using call through API interface and web site GUI data harvesting application feedback collection application for data cleaning & analysis module to get cleaned data applying machine-learning algorithm and decision support system.

3. Proposed system

Sensing deceptive activities on a network, by collecting call history on a network for a specified time frame, each call history comprising a plurality of call topographies for a call to a recipient number, call topographies from each of the poised call history by recipient number, resulting in a combination of call features for each recipient number. Resultant data points obtained from set of data points transmuting from call features by dimension reduction, each data point signifying a particular call features for recipient number. The flowchart of the proposed system is depicted in Fig. 1.

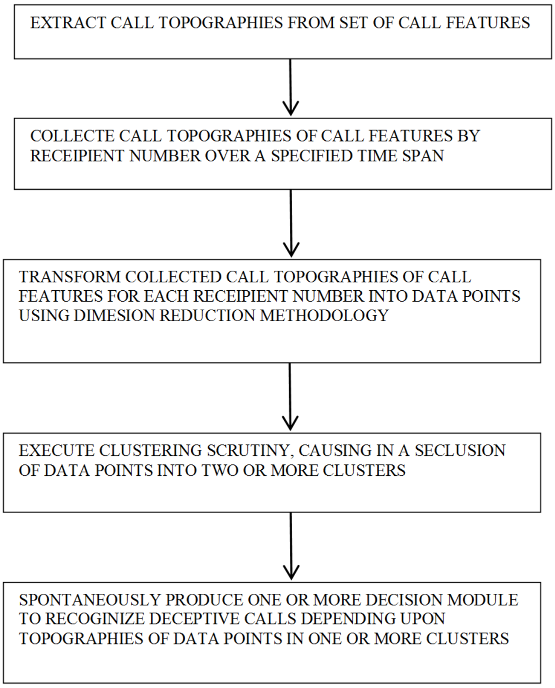
EXTRACT CALL TOPOGRAPHIES FROM SET OF CALL FEATURES
COLLECTE CALL TOPOGRAPHIES OF CALL FEATURES BY RECEIPIENT NUMBER OVER A SPECIFIED TIME SPAN
TRANSFORM COLLECTED CALL TOPOGRAPHIES OF CALL FEATURES FOR EACH RECEIPIENT NUMBER INTO DATA POINTS USING DIMESION REDUCTION METHODOLOGY
EXECUTE CLUSTERING SCRUTINY, CAUSING IN A SECLUSION OF DATA POINTS INTO TWO OR MORE CLUSTERS
SPONTANEOUSLY PRODUCE ONE OR MORE DECISION MODULE TO RECOGINIZE DECEPTIVE CALLS DEPENDING UPON TOPOGRAPHIES OF DATA POINTS IN ONE OR MORE CLUSTERS

Fig. 1. Representation of deceptive calls recognition: approach

Execution of clustering analysis that is formed out of set of data points into two-or more clusters and tagging call features as deceptive or non-deceptive built on cluster of each particular data point. Execution of supervised learning module on each tagged call features as a trained information to produce at least one or more decision module to recognize deceptive calls. Recognizing deceptive calls on the network using at least one decision module and triggering a programmed action based on recognition.

Two types of features are proposed, one is arithmetical and other is categorical features, arithmetical columns containing numbers and categorical columns containing non-numbers features. The deceptive module may smear a one-hot transformation transforms a categorical call feature into an arithmetic number and that they are homogeneous contingent on the machine learning module. The deceptive analysis module smears a supervised learning module to the total dataset to obtain a decision module for identifying whether a call is deceptive. One category of decision module is decision tree. The deceptive analysis module uses a cross validation model to pick up training data points to produce a decision tree module for forecasting about deceptive calls. The major benefits of decision tree module are the forecasting module, which visually describes decision methodology process.

4. Conclusion

Traditional research approaches of discovery of deceptive calls is modest. Trained professionals are anticipated to sense such maneuvers. The study displays that individuals are untruth indicators are scarcely improved than devices on sensing deception communication.

One of major disadvantage of these research findings is that they depend on the arithmetic credibility and they ignored the deceptive communication that escorts the deceitful. The proposed system deals in recognizing deceitful calls in a network using machine learning approach.

References

[1] S. Falaleev, A. Vinogradov, P. Bondarchuk: *Influence research of extreme operate conditions on the face gas dynamic seal characteristics.* Technische Akademie Esslingen International Tribology Colloquium Proceedings *15* (2006), p.208.

[2] N. Conroy, V. L. Rubin, Y. Chen: *Automatic deception detection: Methods for finding fake news.* ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community, 6–10 November 2015, St. Louis, Missouri, USA, Proceeding ASIST'15 (2015), Article No. 82.

[3] A. Wiens, T. Wiens, M. Massoth: *A new unsupervised user profiling approach for detecting toll fraud in VoIP networks.* Advanced International Conference on Telecommunications, 20–24 July 2014, Paris, France, Presented during AICT (2014).

[4] I. Lefter, L. J. M. Rothkrantz, D. van Leeuwen, P. Wiggers: *Automatic stress detection in emergency (telephone) calls.* International Journal of Intelligent Defence Support Systems *4* (2011), No. 2, 148–168.

[5] G. Mendels, S. I. Levitan, K. Z. Lee, J. Hirschberg: *Hybrid acoustic-lexical deep learning approach for deception detection.* Interspeech, 20–24 August 2017, Stockholm, Sweden, Proc. Interspeech (2017), 1472–1476.

[6] D. F. Larcker, A. A. Zakolyukina: *Detecting deceptive discussions in conference calls.* Journal of Accounting Research *50* (2012), No. 2, 495–540.

[7] B. H. Wang, X. L. Wang: *Deceptive financial reporting detection: A hierarchical clustering approach based on linguistic features.* 2012 International Workshop on Information and Electronics Engineering, Published Procedia Engineering *29* (2012), 3392–3396.

[8] A. J. Graaff, A. P. Engelbrecht: *An overview of models to detect and analyze fraud in the telecommunications environment.* School of Information Technology, University of Pretoria, South Africa (2002).

[9] M. Ott, Y. Choi, C. Cardie, J. T. Hancock: *Finding deceptive opinion spam by any stretch of the imagination.* Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, 19–24 June 2011, Portland, Oregon, USA, HLT'11 Proceedings (2011), No. 1, 309–319.

[10] V. Balasubramaniyan, R. Bandyopadhyay, T. Calhoun: *Lifecycle of a phone fraudster: Exposing fraud activity from account reconnaissance to takeover using graph analysis and acoustical anomalies.* In Black Hat USA (2014), "Fraud Protection Toolkit", Tata Communications Ltd.

[11] D. J. Lary, A. Nikitkov, D. Stone: *Which machine-learning models best predict online auction seller deception risk?.* National Aeronautics and Space Administration (NASA) Goddard Space Flight Center (2010).

Received October 12, 2017