ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.6

Intelligent Trip Modeling for the Prediction

S.Sageengrana[1], P.Senthil[2], T.Gurusamy[3]
Assistant Professor[1, 2], PG Scholar[3]
Deparment of Computer Science and Engineering, [1, 2], Master of Computer Applications[3]
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India

Abstract:
Intelligent transportation systems (ITS) are sophisticated applications with a focus to generate and spread creative services related to different transport modes for traffic management and hence enable the terrorist passenger informed about the traffic well a head and to use the transport networks in a better way. The Intelligent travel system which will provides an eminent Neural Network based on the intelligence system which will provides an automatic allocation of travel's through the Global Information system across the path of the terrorists travel, this may help in prediction of attacking region and type of attack etc…by the terrorist.

Keywords: map, reduce, data mining, transpose, minify.`

1. INTRODUCTION

Terrorism is one of the major issue in the current generation. We don't have any proper system to monitor the travel pattern of the normal civilians and predict the possibility of the undercover terrorists as normal people. Based on their actions such as travel pattern, each person's can be monitored and identified whether, there is a possibility of terrorism involvement and possibility of affected or monitored zones of an undercover personnel. This is an innovative system which will provide the pattern movement via Google maps.

2. SYSTEM ANALYSIS

2.1, ON HAND SYSTEM

We don't have enough base to identify the criminals pattern and possibility of attacks .Mining the patter of the individual and integrate same with the google maps to identify the possibility of attack is one of an innovative system which we are designing and it's not available with the existing system .Existing system comprehensive talk about the pattern and corner detection of an individual and didn't specify much more details on the possible attacks and prediction, Heuristic problem space algorithm is used to identify the pattern of an individual.

2.2, ON HAND ALGORITHM

SPNNS Algorithm_The SPNNS algorithm contains neural networks (NNs) trained to make short-term traffic forecasts at traffic sensor locations. The forecasting is made based on traffic congestion levels, and the length of forecasting time intervals. The SPNNS can predict the traffic speed at each sensor location in short terms up to 30 min ahead of the beginning time of a trip based on traffic sensor data available only at the trip starting time. DTSP algorithm puts the SPNNS together with the dynamic traversing algorithm to generate the whole speed profile from the trip origin to the destination by traversing the space and time domain and calling the SPNNS with dynamic time intervals

2.3, PROJECTED STRUCTURE

An Intelligent Trip Modeling System (ITMS) is developed to predict the traveling profile for a selected route based on the traffic information available at the trip starting time .The ITMS contains artificial intelligence based ideas to predict the short-term traffic of a users based on the pattern collects. The data needs to be feed in to our travel pattern system with the latitude and longitude values and its co-related with the Google maps. This pattern needs to be mined with the proposed algorithms to identify the possible of attacks.

Computational Optimized Allocation Agorithm
Computational Optimized Allocation Algorithm_This is optimal ,computationally efficient, Integer-bit power allocation algorithm for discrete multi_one modulation .Using efficient lookup table searches and a Lagrange-multiplier bisection search, our algorithm converges faster to the optimal solution than existing techniques and can replace the use of suboptimal methods because of its low computational complexity .Fast algorithms are developed for the data rate and performance margin maximization problems. Lagrange solution, Integer-bit restriction, fast algorithm via table look up these are all the methods involved in computational optimized allocation algorithm .

3. METHODOLOGY

The various function are be invoked in the project for the prediction of threatening individual

Terrorists information Feed segment
This module provides an information storage on the terrorists which is received by the cyber crime team. The information includes, Terrorists name, Type of Attacks, Previous Attack History, Type of Attacking Places, Any Other information's about the terrorists, Image of the terrorist

Travel Pattern feed Module
This module involves the travel pattern history of the user the below information needs to be loaded. It includes the latitude, longitude, Location, Severity of attack location, Travel pattern range.

Attacking Type – Mining Module
In This module provides an analysis of Terrorists Vs Attacking Type. Machine learning model is emphasized for supervised classification approaches. Prior to applying the learning model, the data is pre-processed to remove any unwanted data and

ensure data mining principle is applied on real data. In predictive modeling, data is collected, a statistical model is formulated, predictions are made and the model is validated or revised as additional data becomes available. The outcome of this module is a fine tuned output of prediction on Attacking type the user is involved.

Attacking Location – Mining Module

This module provides an efficient lookup table searches and a Lagrange-multiplier bisection search. Preparation and data preprocessing are the most important and time consuming parts of this module. In this step, the data is converted into an acceptable format for our prediction algorithm. On top of it, we find the remarkable tuning up of data to identify the defective data set filter it and utilized for mining process. The data sets converges faster to the optimal solution than existing techniques and can replace the use of suboptimal methods because of its low computational complexity .The outcome of this module provides the attacking location of the terrorists.

Finalized Attacking Pattern Define Module

This module provides a consolidated report of the possibility of attacking location and places cum type of attacks from the previously mined datasets. The finalized output of this project provides a convex nature of data tuneup by narrowing the data to the fine grained exact data.

Google Maps Integration Module

This module provides a consolidated report of the possibility of attacking location and places cum type of attacks from the previously mined datasets.The finalized output of this project provides a convex nature of data tune-up by narrowing the data to the fine grained exact data.

4. IMPLEMENTATION

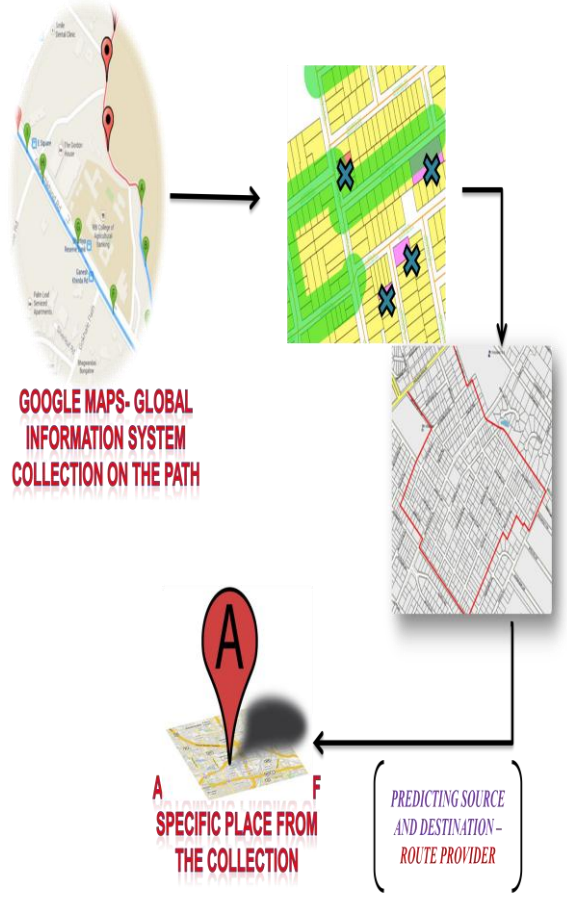

Figure.4.1

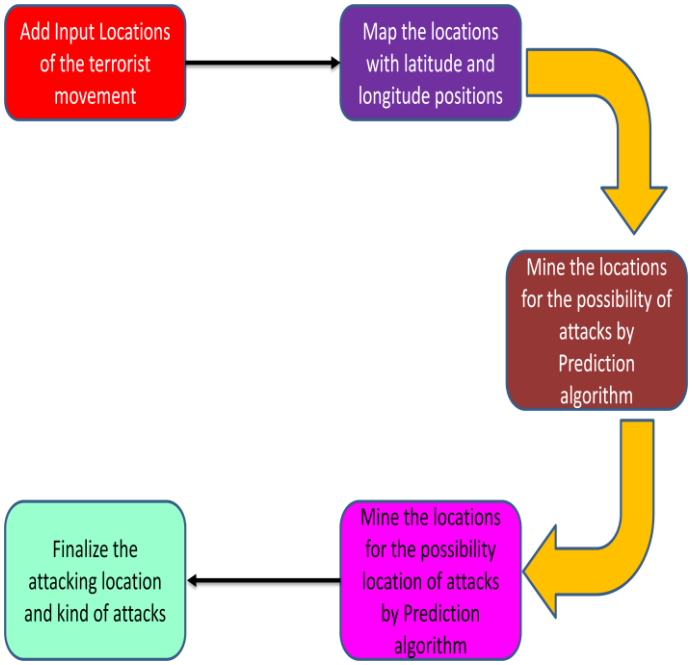

Figure.4.2

5. CONCULSION

This project provides an innovation in the field of cyber crime and it really a needy one in the current situation in India. On the whole, this project gathers preliminary information and rate the importance, likelihood, and implementation timeframe of different detection technologies and strategies; potential terrorism triggers, scope and spectrum; eventual response to prevent attacks, as well as potential ethical and social implications of different strategies.

6. REFERENCES

[1]. Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture,"Proc. ACM SIGCOMM, pp. 55-67,Aug. 2001.

[2]. Z. Yang, H. Ma, and J. Zhang, "A Dynamic Scalable Service Model for SIP- Based Video Conference,"Proc. Ninth Int'l Conf. Computer Supported Cooperative Work in DE,pp. 594-599, May 2005.NISHIYAMA ET AL.: TRAFFIC PATTERN-BASED CONTENT LEAKAGE DETECTION FOR TRUSTED CONTENT DELIVERY NETWORKS 307

[3]. Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture, "Proc. ACM SIGCOMM,pp. 55-67, Aug. 2001.

[4]. O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment,"Proc. Fourth Int'l Conf. Intelligent Environments,pp. 25-30, 2008.

[5]. E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advancesin Digital Video Content Protection," Proc. IEEE,vol. 93, no. 1,pp. 171-183, Jan. 2005.

[6]. S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung, "ResolvingRightful Ownerships with Invisible Watermarking Techniques:Limitations, Attacks, and Implications,"IEEE J. Selected AreasComm.,vol. 16, no. 4, pp. 573-586, May 1998.