Enhancing Social Security through Network of Intelligent Human Nodes Trained by Computer Algorithm

Dulal Acharjee
Dept. of Information Technology
Purushottam Institute of Engineering and Technology
Rourkela, Orissa, India.

Bhabani Shankar Panda
Dept. of ETE
Purushottam Institute of Engineering and Technology
Rourkela, Orissa, India.

Basudev Mahapatra
Dept. of ETE
Purushottam Institute of Engineering and Technology
Rourkela, Orissa, India.

ABSTRACT

In near future, all manual decisions will be more authentic, scientific and logic based. Through continuous evolutionary process, scientist developed different technologies of computer, communication network and Information Technology using automated computing systems to make their work more perfect, accurate and errorless. Important information has been made more secured with the help of computer algorithms. Vulnerable intruders can't break the security levels easily though exceptions are there. Different levels or stages of security checking encryption-decryption systems check protection to the valuable databases created everyday throughout the world. Information is secured by computer algorithm; information is required for making secured society. But, strange is that yet most of valuable wealth of the Universe is left unsecured. After having much terrorist attack on civil creations, it is imagined that only police, army or any security people are not sufficient to provide security of the creation of the Universe. Trained and intelligent human network is required to develop who can scan neighbour phenomena all time and gather information for analysis and taking decision purposes dynamically. This paper aims to develop some conceptual training aspects of people which are similar to information security algorithm of computers.

General Terms

Social security and network, computer algorithms for security, viruses, Social Security Servers of computer.

Key Words

Social security, hole area, terrorists attack, history database.

1. INTRODUCTION

In 'human rights, terrorism and counter terrorism' published by the Office of the United Nations High Commissioner for Human Rights, written that "In order to be considered lawful, the use of lethal force must always comply with the principle of necessity … or for the defence of another's life. It must always comply with the principle of proportionality, and non-lethal tactics for capture or prevention must always be attempted if feasible"[3].

A terrorist can destroy the whole creation of the world. A criminal can kill his neighbour persons. As example, the Ex-Prime Minister of India, Mrs.Indira Gandhi, was killed by her own security guard. X a leader of BJP(Bharatia Janata Party) was killed by Y, his own brother. A man sitting beside of you within train or a bus may switch on the remote controller to burst a bomb for destroying a train or an air plane or any other public carrier. The attack on WTA(World Trade Association) of America indicates that our social security system is so poor. It is not the lack of duty of security forces but lack of proper training to the people of the world regarding terror attack. So, question arises, if a terrorist make a plan to burst a bomb at the time of praying within a temple, mosque or a Church then how to detect that malicious person to nullify his intention of destroying the civil creation.

In computer algorithm, there are some techniques to detect a malicious node(device or computer) which is spreading viruses or stealing information or destroying the target system. Within any network of information, an internet network or any intranet(local network), all electronic equipments including computers are connected to each other. When data move from one place to another, it carries source, target and route addresses. Any critical programmer intended to do some evil job, may collect these addresses and data for their interest. Analysing the flow and movement nature it is possible to detect what type of attack is happening on the network. This concept may be applied in social network. It is called bit by bit wise scanning. A bit does not contain any information. Multiple bits make information. If it is possible to develop a social intelligent network for scanning and sharing information quicker than happening time of danger, then it is possible to minimize the probability of accident.

As a concept of technology, neighbourhood is monitored by sensor network which sense any phenomena of neighbour and aggregate data collected by different sensors, analyse it and send to server computer(Sink Node) for taking decision. If people are trained properly they can scan the neighbour and gather information through some human machine interface placed at some convenient positions for gathering security information of a locality. It does not mean that all people should disbelieve their neighbours, but means that all people should initiate an additive process in their thinking to give more security to others. It means, as people are becoming more social responsive, now they would be more organized with the knowledge of technological general concept. General people do not understand technology, but they can be trained by the high level concept of technology.

2. DIFFERENT WAYS OF VIGILANCE

As human, people do some humane activity throughout their lives. They don't ask any remuneration for that and it has become practice of civil society. So, one more activity is proposed to add with other activities those are practised every time. This extra activity could be performed in many ways:

a. Observing neighbour.
b. Processing observed data.
c. Taking decision by human intelligence.

It is tried to model the activity as a structured manner. To model this type of volunteer activity is hard. Side effects of this model should be considered also when it would be implemented in an area as an experimental case. This model is an activity of mass people who will be trained by different institutes/school/colleges or by govt. semi govt. security organizations.

3. OBSERVING NEIGHBOUR SECURITY

In computer network, all nodes are connected through cables or fibre optical cables or wireless media. Analyzing the flow of data packets, behaviour of the node is assumed and according the analysis report, decision of communication is taken. What jobs are done by each node may be tress. Requirements of enhancing public observation to neighbour would be justified if some examples are cited. (a)Once, in a flat of a multi storied building suddenly havoc explosive sound of bomb-bursting appeared and inhabitants didn't know that there were a terrorist group engaged to make bomb. (b) A person was purchased by an intelligence agency of enemy country and suddenly there are some change in his movement and activities. (c) A person sitting beside of you switched on a bomb to burst a train of another state with the help of his mobile phone. (d) A mentally unhappy armed person suddenly raised his automated arms and fired his neighbour colleagues. These types of many examples can be gathered which are the causes of insecurity of a person or a locality. Now question is that how to tress it and store all relevant information in database and gather information from the analysis report. Sometimes, there would not be much time to analyse data. Occurrences are happening so quick, it is very hard to prevent at this moment.

In computer network also, same type of problems are happening every time. Computers can tress it, can take alternative action, can store data in history file etc. If we consider every computer as a human node, then, the problems cited above may be considered as the problems of Cookie or dangerous viruses which can crash a whole hard disk or the total network system. A cookie is a small program unit sent by any person to do some job within the computer as background process. This unwanted program unit or virus unit can do any dangerous job within the computer. Solutions of these problems are to set incoming protection after checking incoming flow of bit stream in different way. Generally civil people don't do any continuous scanning or checking over the neighbour. Rather, they depend on security persons for maintaining security. Security persons can scan only some limited areas. Coverage area is a concept of wireless communication. There are lot of holes areas which may not be covered by the exiting wireless network system. Problems are created in those uncovered areas. Another important point is that , security persons can scan only some limited attributes of an object, but there are thousands of unknown attributes which may cause harm to society but remains within holes of network as non scanned.

In any position, a person is surrounded by neighbours in different ways. They may be tightly or loosely coupled with the neighbour. Some examples of neighbourhood is modelled and shown through diagrams.

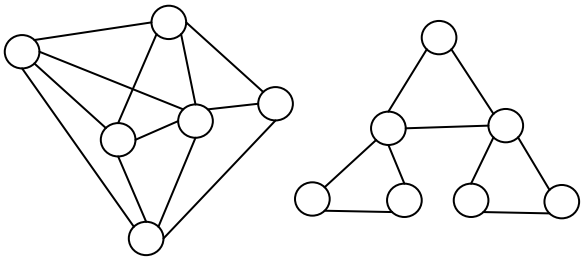

Fig.1.a. Home, hostel and room network to communicate with neighbours

Fig.1.b. Office Network

In [3], they have commented on RFC 3756 (Recommends for commends, group of network protocol formulation) and RFC 3971 regarding IPv6 (Internet Protocol, version 6) Neighbor Discovery (ND) and Trust Models and Threats and SEcure Neighbor Discovery (SEND) as "…it as an expression of an organizational or collective belief, i.e., an expression of commonly shared beliefs about the future behaviour of the other involved parties. Conversely, the term trust relationship denotes a mutual a priori relationship between the involved organizations or parties where the parties believe that the other parties will behave correctly even in the future".

Address resolving is an important work. Now a day, people may have multiple addresses and it has important role to analyse the person activities. In internet, each computer is given an unique number known as IP(Internet Protocol) number and it looks like 192.100.68.255. But in advanced version, IPv6, the address spaces are of 16 bytes meaning that it may have 2^{128} numbers of computers in one network. Address reveals lot of information and we can learn the technique from the algorithm which is used for gathering information of neighbour.

3.1 Confusion created by Malicious Nodes

A malicious node creates confusion to its neighbour in different ways. It is dangerous for a network, so to search and find out is a critical job for a computer. Sometimes it sends wring data, corrupt data, wrong acknowledgement, killing router, generates wrong address for both sender and receiver nodes etc. Some important attacks are listed here:NS/NA spoofing, NUD failure, DAD DoS, Malicious router, Default router killed, Good router goes bad, Spoofed redirect, Bogus on-link prefix, Bogus address config, Parameter spoofing, Replay attacks, Remote ND DoS. After some time, a malicious node may act as a good node also. Due to malicious response detected for a while, new algorithm can make sustain the network.

Knowledge can be gathered how to tackle these nodes and not to kill those nodes assuming they may behave as a good node after some time. A vary difference with social laws is that 'lawful human don't allow to live a killer but computer don't kill a killer'.

4. SOCIAL SECURITY SERVER(3S)

Now a days, people wear different types of wireless mobile equipments which may tress position, trends of movement, duration of staying in a position etc. Analysis of these data collected from these equipments can give some idea about the profession of the user. Some people do switch off their mobile phone at the time of emergency works, time of sleeping, time of taking rest or at the time of not to disturb. Some criminals may switch off their mobile phone that they may not be tress at

particular time. But, analysing the time and location of switching off and switching on, some clue may be found from these history data. Suspected phones may be kept under vigilance.

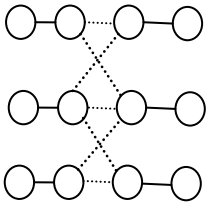

Fig.2.a.Network within Bus,Train and Plane.

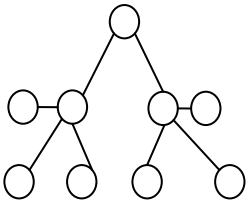

Fig.2.b. Network of security in village.

Storing data of roaming-history needs large database administration system. At present, in all ISP(Internet Service provider) or mobile phone service providers store some data of history of movement of users in their BSC(Base Station Controller), MSC(Mobile Switching Center), HLR(Home Locating Register), VLR(Visitors Locating Register). These are different types of computers placed at different locations of the network in the country. Architecture of these networks was designed aiming to give support for mobile users. At that time it was not thought that these networks could provide some sort of social security services. There may be different approaches and techniques for enhancing social security. One of these techniques is to keep history-data within 3S servers with an extra sub-module of software.

5. BIO-SECURITY DEVICES

Electronic devices used for security purposes are known to all. Due to known technology, terrorists can develop anti policy to nullify all positive activities adopted by civil people. New bio medicine having radioactive or some other type of radiation feature may be injected or fed as medicine which can locate the position of person also can record the mental status of a person within the cell of 3S. At the child age, different vaccines are applied and its effects remain for whole life. Some medicine or bio-devices may be injected at the child age that would have result for whole life. If it is possible to invent, then no children would be lost or no person could be hijacked. If so, then terrorist would try to develop some anti medicine which would destroy the medicines injected previously. As that type of research is not possible for a small group or a person, the model expressed before will remain secure for a long time. Gradually, research and invention would give some measure of security. We know that 100% security is an impractical thinking.

6. ALGORITHM OF COVERAGE AREA

Any service has some coverage areas. Services can't cover all areas. Due to wrong design or limitation of resources, hole-area is generated or non-serviced area is found within the expected service area. All evils come through this hole-area. Different types of algorithms for covering the maximum area are-centralized, disjoint centralized, parallel centralized, distributed algorithms etc. Optimized deployment of human nodes and proposed 3S can minimize the critical hole area generated within the target service area[4].

In computer, covering the area of hole means providing services of some attributes like signal strength or sending receiving data or minimizing BER(Bit Error Rate) within those area also. At present, computers provide limited services with limited attributes. But, Social security demands covering whole area with more attributes of social people than computer can do. Observing neighbour means observing attributes of neighbour objects. Neighbour may be any person or any type of an object.

7. ACTIVITY OF A TRAINED HUMAN NODE

Activities should be defined for all human nodes. There are different levels of responsibilities and are distributed by professional organizations like: police, army, security agencies etc. Some responsibilities may be given by other organizations like NGOs, Schools, Colleges, universities, business organizations, government organizations like-Parliament, local governing body, district management body etc. to their responsible executives. Some trained nodes may take training on particular activities and others can take on other activities. Some of activities names are: observing new comer in neighbour, observing in and out time, gathering information about the types of business they are involved, source of income, sources of expenditure, locations of movement of neighbours, friends and enemies of neighbours etc.

7.1 Communication With 3S

Human Nodes will contain a powerful mobile communication device with high storage capacity. He should has easy access to the 3S for storing, editing, deleting some information of neighbour observed by him. Or he may store a new state of observation as a new record. To test or verify decision or action, some software should be there to analyse local data with full online interaction with 3S. The infrastructure of telecommunication system can be utilized to set new server like 3S. At different locations of mobile phone service providers, different types of 3S servers can be installed with proper software. A conceptual architecture of network with 3S is shown below:

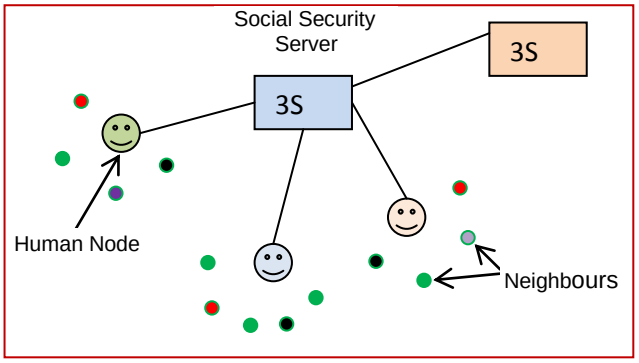

Fig 3: Topology of Social Security Network

The variance of decision making is a term through which we may measure our correctness of the system. If variance is more, then changing different related parameters value we may think for suitable adjustment of error curve.

$$\sigma_n = \sqrt{\frac{1}{n}\sum_{i=1}^{i=n}(X_i - \bar{X})^2}$$

Here, Xi is the different input set and $\overline{X}$ is the mean of input data set. From the fig.3 it is shown that input is attributes of neighbor.

There is another measure in Statistics, named, 'P-Value' which is a statistical value that details and give probability of avoiding the most common explanation for the data set. p-value is the probability that the null hypothesis on input data set is true. For designing the parameters of hypothesis testing, researchers can set fuzzy weight to their options to test level of significance. The sensitivity of the output and standards for the decision can all be sensitive to the smallest error.

So, if we can develop a technology which can provide us correct attribute values, then it is possible to adjust error values using BPN(Back Propagation Algorithm) of neural network. In this algorithm, a small amount of output value is fed back with input or weight data. A simple equation to adjust weight and input values are :

$W_{(new)}=W_{(old)}+\Delta W$ and

$X_{(new)}=X_{(old)}+\Delta X$

Where, ΔW and ΔX are small changes of weight and input values. After many epochs, a moderate decision may be taken on any event[1].

Fuzzy logic can be used for quantifying the decision parameters also. Mostly, social neighbour's attributes are in the form of fuzzy and can't be defines as crisp or numerical form. Let us give an example: *Movement of a man in a locality is suspicious*. Here, 'movement' is the attribute of neighbour, and 'suspicious' is a qualifying parameter expressed in fuzzy form. Movement can be qualified as: 'normal', 'suspicious' and 'dangerous'. These three fuzzy data are in the scale of suspicious.

The mobile device worn by human nodes should contain intelligent software module with different option to support the requirements of people. Sitting at any place, a human node can access 3S and get output of expected data. He should manipulate data in different way for investigation, but he should not suspect a neighbour as suspicious unless data from 3S is analysed.

8. CONCLUSION

Here, we have placed our high level concepts that in future people can develop more secured and logic based neighbour. It is understood that for enhancing social security, active part of all people of the world is required. And it is envisaged that a planned training is required to different sections of people to set extra security measures at different sections as we have set planned antivirus, firewall of shield within operating system. Nodes deployment is an important issue and this point is discussed for minimizing the hole area through optimized human node deployment. Data, system and the creations of human need more secured environment. Valuable creations should not be left without security. Till more investment is not possible, or with the modern electronic system more trained human node should be deployed to cover security holes. Human nodes are not the replacement of electronic instruments. But it is proposed to train people in view point of security.

This paper assumes that in future, human thinking and decision making will be logically automated. In place of imagination, more structured thinking will be acted with the help of intelligent machine. Gradually, in future, all decision will be automated and structured.

9. REFERENCE:

[1] S N Sivanandam , S Sumathi , S N Deepa Introduction To NEURAL NETWORKS USING MATLAB 6.0, Tata McGraw Hill, 2006.

[2] William Stallings, Cryptography and Network Security, PEARSON Prentice Hall, Fourth Edition, 2006.

[3] Office of the United Nations High Commissioner for Human Rights, Human Rights, Terrorism and Counter-terrorism, Fact Sheet No. 32.

[4] Z. Abrams, A.Goel and S.Plotkin,"Set k-kover algorithms for evergy efficient monitoring in Wireless Sensor Network", proceeding of 3rd Int. Symposium on Information Processing in Sensor Networks, ACM 2004, pp.424-432.