American Journal of Applied Sciences 5 (5): 496-503, 2008
ISSN 1546-9239

Behavioral Modeling: an Overview

Roman V. Yampolskiy
Center for Unified Biometrics and Sensors and Department of Computer Science and Engineering
and IGERT in GIS
University at Buffalo, Buffalo, NY 14260, USA

Abstract: This exploratory paper begins with an overview of a multidisciplinary problem of behavior modeling and correlation of different behaviors. It looks at many possible applications of such technology and proposes some novel directions for future research. From the security point of view the paper proposes and explores some novel behavioral biometrics and research paths as well as some universal descriptors of behavior in general. It concludes with an analysis of how behavior can be influenced by the environment in particular location of the individual engaging in the behavior.

Keywords: Behavior modeling, behavioral biometrics, user profiling

INTRODUCTION

It is often the case in the scientific discovery process that multiple sub-fields of science study the same concept simultaneously but are not aware of the contributions made in the other fields to what essentially is the same problem. Multiple disciplines use different motivation for their research as well as create unique vocabulary to deal with the problem at hand. A lot of progress in finding a solution to such a problem can be made by realizing similarity of research goals and making scientists realize the wealth of available techniques from other fields which may be used with little to no modification for solving a problem at hand. We start by presenting just such a problem addressed by many fields, which are relatively unaware of each other, but all attempt to model human behavior.

User Profiling is studied by researchers in the field of Intrusion Detection. It consists of observing someone interacting with a computer, creating a model of such behavior and using it as a template for what is considered a normal behavior for that particular user. If the behavior of supposedly the same user is significantly different we can speculate that perhaps it is a different user masquerading as the user whose profile is stored in our security system as a template.

User Modeling is studied for marketing and customization purposes. It aims at creating a representation of the user for the purpose of customizing products and service to better suite the user. For example software can be made to only display options which are in the field of interest of this particular user making it easier for him to interact with an otherwise very complicated piece of software.

Opponent Modeling is related to the field of Game Theory and studies different models for understanding and predicting behavior of players in different games. While for many games such as chess it is sufficient for victory to play the best possible strategy and ignore the unique behavior of your opponent in many other games such as poker it is not. Having a well performing prediction model of your opponent's behavior can give you an edge necessary to defeat him in an otherwise equal game.

Behavioral Biometrics are a subset of biometrics, which are generally studied by security system developers. Behavioral biometrics are measurable properties of person's actions which can be used to verify user's identity[1-3]. An example of a popular behavioral biometric is the way a person types on a keyboard; it has been definitively shown that it is unique enough to provide reliable person verification[4].

Criminal Profiling as done by police and FBI investigators is the practice of trying to determine personality and identity of an individual who has committed a crime based on the behavior, which was exhibited during the criminal act.

Jury Profiling is a technique used by lawyers to attempt to predict how a particular potential juror will

Corresponding Author: Roman V. Yampolskiy, University at Buffalo, 2145 Monroe Ave. #4, Rochester, NY, 14618, USA.
Tel: (585)269-9629

vote with respect to the verdict based on juror's current behavior, answers to a questioner and overall physical and psychological appearance of the juror.

While the researchers faced with the above problems represent relatively unrelated disciplines they are all essentially trying to achieve the same exact goals. They want to be able to do the following: By analyzing past and current actions create an accurate model of individual human's behavior capable of predicting future actions based on a given situation and environmental factors. Given a description of behavior either identify an individual likely to conduct himself in such manner or to verify if a given individual is likely to behave in such a way.

Basically in its most generalized form the problem boils down to a mapping from the set of behaviors to individuals and vise versa. However we can ask if it is possible to create more complicated mappings between personality and behavior.

Given occurrence of some behavior by an individual can we predict happening of another smilingly unrelated behavior by the same individual? It is obvious that in the case of related behaviors the answer is definitely - yes, for example someone who buys a first and second album by a famous rap artist is likely to also purchase a third one. But in the case of completely unrelated behaviors we don't have any strong evidence supporting or disproving possibility of such correspondence. For example do people who collect stamps are also more likely to enjoy horseback riding?

Some research suggests that there is a connection between one set of behaviors and another. Rentfrow et al. in the Journal of Personality and Social Psychology report that they found a connection between person's musical preferences and other unrelated social behaviors[5]. The most famous example from the field of data mining tells us that people who buy diapers also tend to buy beer while at the store. Clearly this is a very interesting and beneficial area of research. The possible applications for cross-behavioral prediction are numerous. Perhaps it is possible to make judgments about intelligence or health of an individual from something as benign as routine computer interaction. Maybe we can learn to judge suitability of a potential mate from table manners or find a reliable business partner by watching a person park his car.

Another interesting question to ask is: if two different individuals have similar behavioral profiles and individual A performs a novel behavior is it likely that individual B will also perform the same behavior in the near future. Intuitively it seems very plausible, for example, if two different people recently got married and left on a honeymoon we can expect that seeing one of them buy baby related items may allow us to predict similar purchases by the other in the nearest future. Obviously in this contrived example we had alternative ways of figuring this out.

It would seem desirable to have a single discipline devoted to solving such an important problem for many fields, but in reality a number of somewhat different fields all attempt to work on it to some degree, not mentioning the fields listed above we have:

Behaviormetrics which studies human behavior on the basis of statistics and information technology. Methodology in behavioral sciences is studied and mathematical or statistical models for understanding human behavior are developed[6].

Behavioral Sciences "essentially investigates the decision processes and communication strategies within and between organisms in a social system. BS encompasses all the disciplines that explore the behavior and strategies within and between organisms in the natural world. It involves the systematic analysis and investigation of humans and animal behavior, through controlled and naturalistic experimental observations and rigorous formulations"[7].

Both of which can be put under a more general umbrella of science of psychology defined as: "scientific study of human behavior, mental processes, and how they are affected and/or affect an individuals or group's physical state, mental state, and external environment. It's goal is to describe, understand, predict, and modify behavior"[8].

We propose attacking the given problem from the point of view of computer science in general and Intrusion Detection Systems (IDS) and Biometrics research in particular. Our choice is motivated by the fact that IDS and Biometrics has tools and methodologies necessary for solving the problem. IDS would benefit from all aspects of such research and already has a proven track record in the field. The rest of this paper analyzes potential future directions of research in analyzing peculiarities of human behavior.

BIOMETRICS

There are two types of biometrics: Physical Biometrics (PB) and Behavioral Biometrics (BB) also known as Kinetics[9]. PB are defined as: biological properties of an individual that uniquely determine identity. BB are defined as: "characteristic traits exhibited by a person that can determine identity" in other words they attempt to quantify the unique actions that people perform[10]. Physical biometrics are typically considered to be more reliable and so may be used for user identification or verification. Behavioral Biometrics are considered less reliable and so are only used for verification, but it might be possible to achieve certain levels of accuracy even in recognition applications particularly by utilizing multi-modal behavioral biometrics[1]. Behavioral biometrics also have some advantages over Physical biometrics, such as:

- Collection of data for BB is far less intrusive, often unnoticeable by the person being profiled.
- Behavioral biometrics tend to raise fewer privacy concerns since the behavior is already publicly observable[11].
- Based on the needs of the application behavioral measurements can be collected to accommodate different security thresholds. The longer we observe a particular behavior the more accurate description of it we can generate[12].
- BB are also often less expensive to implement since they require less or none of specialized hardware[13].

Software Interaction Biometrics

A large number of behavioral biometrics is currently under investigation including: voice, signature, keystroke dynamics, handwriting, lip motion, gait, gesture and grip[9]. Behavioral biometrics can be subdivided into a number of groups, one such group being comprised of behaviors related to the manipulation of computer software. This particular type is also known as User Profiling based. Up to this point a lot of research in behavioral biometrics concentrated on a very low level behavior of the users such as keystroke dynamics and mouse movements which are used to interact with a computer. While relatively accurate, those behavioral biometrics only concentrate on manifestations of behavior dependent on physical abilities of an individual and completely ignore higher level intentional behaviors, which may provide superior descriptors for successfully verifying identity of human beings.

User interaction with almost every type of software can be used to generate a personalized behavioral signature capable of verifying user's identity. While some research in that area has been done, particularly with command line interfaces[14, 15] and more recently with point and click interfaces[16] much more can be accomplished. Usually low-level side effects of user activity are all that is taken to generate a user profile[2]. For example one study concentrated on things like number of open windows, time between new windows and number of words in a window title[16]. As the technology advances it may become possible to use higher-level behaviors to generate more accurate user profiles:

Operating system interaction behavior: A profile consists of OS specific behaviors of the user. Almost every task in a modern OS can be accomplished with multiple equally well performing approaches. So a user's choice of doing some task may constitute a single data point in the behavioral signature. For example using a desktop icon to start an application as apposed to going through the Start button in the MS Windows environment. Dozens if not hundreds of similar choices provide a wealth of behavioral information sufficient to verify if the same user is interacting with the OS.

Web browsing behavior: Just as unique as the OS manipulation behavior can be the set of actions user takes to work with a network such as Internet. The choice of web browser, search engine, collection of often-visited sites and other similar web related choices could be a great personal identifier. Online searching behavior can be a particularly telling descriptor since the choice of keywords used, topics of searching and skill necessary to construct complicated logical predicates say a lot about who the person is.

Email checking – sending behavior: In addition to the different people we all chose to communicate with via email, we all have unique ways of composing emails. Even a simple task of replying to an email can be done very differently. Some people choose to include the original message in the response there is others insist on deleting it[17]. Some add a complicated personalized signature to the end of the message while others simply send "regards". The number of emails sent and received also greatly varies. Many other personal choices can also be considered such as how a person reads his new messages. Some people tend to read them all first and choose to reply to some at a later time, while others always immediately reply to a new message not wishing to keep the sender waiting for a response.

Word processing behavior: There is a million different ways to format a document[18]. Choices of fonts, styles, paragraph structure and so on can be as unique as the users who compose those documents. In addition a great amount of additional information can be collected about the actual writing of the individual such as common topic, vocabulary size, common spelling and grammatical errors.

Media interaction behavior: Modern computers serve as DVD players, stereo systems, photo albums and art galleries to name just some media related applications. How a user organizes a play list of songs, speed with which he looks through a photo album and which news feeds he likes to listen too can be used to tell different users a part.

Photo editing behavior: An operation of a complicated photo processing software such as Photoshop requires a significant level of skill. Just like with OS or word processors no two users will perform many complicated tasks exactly the same way. Since many different images require similar processing we can quickly collect enough data to start verifying user identities in the creative environments such as provided by image processing software.

Game playing strategy: Ramon[[19] et al. with Go (not for security purposes) and Yampolskiy[20-22] et al. with Poker (for security purposes) have demonstrated that it is possible to utilize the strategy used while playing a game as a type of behavioral biometric. The approach works as follows: first a player profile is generated either by data mining an existing database of games or by observing a live game in action. Next a similarity measure is obtain between the feature vector generated based on the recently collected player data and the data for the same player obtained in previous sessions. A score is generated indicating how similar the current style of play is to the historically shown style of play for a particular player. If a score is above a certain threshold, it might indicate that a different user from the one who has originally registered is using the account and so the administrator of the site needs to be alerted to that fact. If the score is below some threshold, the system continues collecting and analyzing the player data.

Any other software: An attentive reader can clearly notice a pattern in the above behavioral biometrics related to software use. All software provides many ways and options for accomplishing similar tasks. The more complicated a piece of software is the more unique will be a behavioral signature generated by the user of the said piece of software. This might be particularly true in security sensitive domains of power management companies and intelligence agency's databases where verifying user's identity is a task second in importance only to the primary function of the software.

Video Surveillance Biometrics

Big brother is watching you. The surveillance cameras are no longer limited to convenience stores. Banks, libraries, airports, factories and even street corners are under constant observation not to mention prisons, police stations, and government buildings. For example in London there are at least 500,000 cameras in the city, and one study showed that in a single day a person could expect to be filmed 300 times[23]. With such a wealth of data it is only logical that we will try to use this information to find, recognize, identify and verify people.

Obviously the best approach to doing so is via face recognition but since it is not always possible, as in the cases there no clear face shot is available, alternative biometric solutions can be exploited. Gait has been one such alternative being researched at multiple centers around the world. We propose a number of behavior-based biometrics, which can be extracted from surveillance videos and analyzed without inconveniencing even a single person with document checks, body searches and similar extreme measures.

Today the processing necessary to obtain desired behavioral information may be well beyond capabilities of our technology, but the capabilities of biometric science are quickly growing and it is entirely possible to have prototypes of such technologies available in a few years and working systems in a decade or so. In any case, the first step is to identify what technology is desirable to have before any such technology begins its way from research lab to the deployment in the field, and this is precisely this first step this paper aims at taking.

Eating and drinking behavior: Since many restaurants and café houses with outside sitting enjoy the security provided by surveillance cameras it is possible to consider person's eating habits as a behavioral biometric. The type of a diet a person follows such as vegetarian, vegan, kosher, or Atkins is a good personal descriptor. How a person eats, how they hold a fork, use a napkin, cut their stake all that can be useful for identification purposes. What sides they choose with their meal, do they use a lot of salt, paper or hot sauce all such information can add uniqueness to their behavioral signature. Additionally we can consider interaction with the restaurant staff such as ordering and tipping habits.

Interaction with electronics: In our everyday life we are constantly using different electronic devices. We get money from ATMs, talk on our cell phones, watch TV or listen to radio, in all such situations we are very particular about just how we interact with the above-mentioned devices. If we take cell phones as an example some people prefer to use speakerphone while others go with a hands free ear set. We all use different dialing fingers, hold phone at a different angle, and keep the phone in various locations in or on our wardrobe. Similar observations can be made about all other interactions with electronics, from TV channel flipping habits to notebook carrying style.

Driving Style: Be it an automobile or a plane the way we control such a contraption is very unique. Take driving for example, how fast one accelerates, applies breaks, makes turns all can be taken to uniquely identify a particular driver[24-26]. An in car computer can provide lots of such information to supplement outside monitoring by traffic cameras. This intimate knowledge of the driver's behavior can be used to identify an incident of auto theft or to customize the car's handling to a particular driver.

Shopping habits: Shopping habits of people have long been subject to intense Data Mining scrutiny in hopes of finding ways to improve sales and increase success of special promotions. For a behavioral profile we can look at what form of payment a person uses. Do they go with a shopping cart or a basket, which order do the take scanning shelves of different products, not to mention which products they select and how those products can be used to better characterize them.

Exercise routine: Lots of people try to stay lean and healthy by going to the gym. Gyms provide an enormous amount of personal choices for the individual. Hundreds of different machines each one with unique settings options, swimming pools, saunas, and locker rooms. A security system can keep track of the times of attendance, duration of exercise, machines and weights used, and type of exercises performed.

Dress and appearance choices: Many people have a very unique dress style, often with a particular piece of attire so unique it is sufficient to immediately identify them. Even though the daily choice of wardrobe changes the style frequently remains the same. Some people like loose hanging T-shirts, some prefer cloths so tight they have hard time putting it on. Hats, high heels, scarfs, jewelry, hairstyles all allow us to show our personality and at the same time to successfully profile us.

Vocabulary: while voice has long been used to identify people we can add a lot of additional variables to the successful behavioral equation. What languages does a person speak, what words he likes to use a lot, even overuse? How big is his vocabulary and what words he never uses? Is he very talkative? How many words per unit of time? The above descriptors can easily be used not just with spoken word but with emails, writings, reports basically any documents.

Other Behaviors: Any skill behavior, any preference or anything else which makes us who we are can be used as a behavioral descriptor. The list below is not all-inclusive and is only meant to spark ideas for novel research directions and groundbreaking projects. Can a behavior biometric be developed around: Working habits, Social behavior (social contacts, hand shaking), Knowledge (what types of information this person knows about), Sense of humor (how a person laughs), Temper (aggressive, passive), Intelligence (capacity to learn and remember, behavior in a classroom environment), Interests (books, hobbies), Athletic ability (fighting style, dancing style, swimming style), Talents (drawing, singing, playing musical instruments), Likes / dislikes (rap music, tanning), Sexual preferences and physical preference for others, Strategy for using tools, Grooming and hygiene habits, Picture taking(picture posing and acting), Public speaking(presenting mannerisms), Psychological disorders (paranoia, schizophrenia), Credit cards(use and payment pattern), Seat choice(on a plain or movie theater), Investing(stocks, bank account preferences), Interaction with animals(pets).

GENERAL PROPERTIES OF BEHAVIOR

While the set of possible behaviors is truly infinite it might be possible to find some measurable properties of behavior, which can be found in all behaviors and correspond well between different behaviors in the same individual. This would be extremely useful in Multi-modal Behavioral Biometrics (MBB) in which multiple different behaviors are used together to create a single profile. Examples of MBB include combining mouse movement data with keyboard dynamics or voice with lip motion and typically significantly increase accuracy of the system. Ideally at the same time those cross-behavioral property measurements will be somewhat different between different individuals making it easier to tell different people apart. Some possible cross-behavioral properties are presented below:

- **Speed** – how fast a behavior is performed. Examples may include typing speed and number of words spoken per minute.
- **Correctness** – number of mistakes as compared to the desired behavior in a given situation. For example number of mistyped characters or slips of the tongue.
- **Redundancy** – useless repetitiveness of the same behavior per time period. For example saying same thing twice.
- **Consistency** – a statistical measurement of how similar this person's behavior is from one data taking section to the other. Some people are more predictable than others and tend to follow the same routine more precisely.
- **Rule obedience** – some people believe that rules are made to be broken. They park next to fire hydrants, cheat on exams, take 10 items to a 7 or less items cash register and abuse the proper rules of spoken language. The opposite of that behavior is strict following of the rules to the point of absurdity, such as putting a seatbelt on to sit in a parked car. In any case people of those two types are relatively consistent in their rule obedience across different behaviors.

ENVIRONMENT AND BEHAVIOR

One of the problems with behavioral biometrics is that human behavior itself is not perfectly repetitive. People act differently based on their current mood, illness, sleep deprivation, drugs, stress, conflict, hunger, previous events and surrounding environment. For example, a person who did not get enough sleep may act irritated, shout a lot and be sloppy at performing his work duties. While fully understanding human emotions may be well beyond capability of modern computers it might be possible to incorporate the effects of the environment into the behavioral model.

The main component of the environment is the geo-spatial location of the individual. The same person will act very differently if they are in privacy of their home or at a public event. In terms of computer networks we can observe that a person who is connecting to the network from his home computer may perform different actions as compared to the times he was accessing the network from his work computer[27]. This leads us to the following thesis: location influences behavior. We are not claiming that knowing individual's location is sufficient condition for predicting his or her behavior, but we propose that it is one of the factors knowing which may increase the accuracy of behavior prediction.

As more and more computers and mobile devices such as cell phones come equipped with GPS (Global Positioning System) chips identifying location of an individual will become trivial. For now individual's location can be obtained by looking up IP address information for the computer from which individual is accessing the network.

Continuing with our previous example of a person accessing a network from different locations and assuming that the network in question is Internet we can predict that if an individual is accessing Internet from his home computer he will be more likely to check the schedule of movies at a local theater playing within the next hour then to perform a search for suppliers of aluminum tubing (assuming he works in the acquisitions department). So knowing the geo-spatial location of an individual our behavior prediction model can be fine-tuned to produce much better results. While the above example is trivial, it might be possible to anticipate some changes in behavior caused by any number of factors and include such changes in our dynamic personal behavior model.

However good our algorithms are it is still very possible for a behavior based biometric to generate a number of false alarms. This can be seen as a significant shortcoming, but can also be viewed as beneficial. Suppose the system triggers an alarm for an abnormal behavior pattern, but quick investigation positively verifies individual's identity. So now we can conclude that for some reason the individual is not acting like himself. This information can be beneficial for example in the domain of games, more specifically Poker. Knowing that a very strong player is not using his usual superior strategy may be very valuable. It is possible the player in question is on *tilt* (temporary psychological instability) and so will likely make some bad decisions which a good player can take advantage of. A similar example in workplace may indicate that an individual is out of it, and is likely to be performing a substandard level work and so it might benefit the company to temporarily remove that employee from his position, maybe sending him on a well-needed vocation.

CONCLUSIONS

Fields as diverse as biometrics, marketing, game theory, security and law enforcement all can greatly benefit from accurate modeling of human behavior. The aim of this exploratory paper was to show that the problem at hand is not unique to any given field and that a solution found once might benefit many industries without a need for rediscovering it for each sub-field.

General introduction to the field of biometrics and more particularly behavioral biometrics is given alongside the benefits of this non-intrusive approach. An overview of possible software based behavioral biometrics was given followed by a large exploratory section on potential future lines of research in video surveillance based behavioral biometrics. We proposed and explored some novel behavioral biometrics and research paths as well as some universal descriptors of behavior in general. It was followed with an analysis of how behavior can be influenced by the environment in particular location of the individual engaging in the behavior.

There are a number of conclusions we can draw from the above discussion. Fruitful lines of research will investigate relationship between behavior and identity, different behaviors and correlations in future actions between people who share same personality traits. It may prove extremely valuable for multi-modal behavioral biometrics to study universal behavioral descriptors such as speed and correctness. Much more could to be done to better understand precisely how outside factors such as location influence human behavior and is it possible to predict the changes in behavior if changes in the environment are known.

Future of behavioral research looks very bright. The next decade will bring us technologies providing unprecedented level of security, product customization, social compatibility and work efficiency. Ideas presented in the section on novel behavioral biometrics provide a wealth of opportunities for interesting research and development. A great side effect of such research would be general greater understanding of human behavior, personality and perhaps human mind itself.

ACKNOWLEDGEMENTS

This paper is based upon work supported by National Science Foundation Grant No. DGE 0333417 ”Integrative Geographic Information Science Traineeship Program”, awarded to the University at Buffalo.

REFERENCES

1. Yampolskiy, R.V., April 2-4, 2007. Human Computer Interaction Based Intrusion Detection. 4th International Conference on Information Technology: New Generations (ITNG 2007). Las Vegas, Nevada, USA.
2. Yampolskiy, R.V., October 9-11, 2007 (to appear). Indirect Human Computer Interaction-Based Biometrics for Intrusion Detection Systems. The 41st Annual IEEE International Carnahan Conference on Security Technology (ICCST2007). Ottawa, Canada.
3. Yampolskiy, R.V., April 11-12, 2007. Motor-Skill Based Biometrics. In Assuring Business processes, Proceedings of the 6th Annual Security Conference, Ed. G. Dhillon. Global Publishing. Las Vegas, NV, USA.
4. Gupta, G., C. Mazumdar, and M.S. Rao, 2004. Digital Forensic Analysis of E-mails: A trusted E-mail Protocol. International Journal of Digital Evidence, 2(4).
5. Willett, E., Retrieved October 6, 2005. Music Preferences. Available at: www.edwardwillett .com/Columns/musicpreference.htm.
6. Yutaka, K., Retrieved October 6, 2005. Behaviormetrics. Available at: http://koko15.hus.osaka-u.ac.jp.
7. Wikipedia. Retrieved October 6, 2005. Behavioural sciences. Available at: http://en.wikipedia.org/wiki/Behavioral_sciences
8. Elissetche, M.M., Retrieved October 6, 2005. Social Science Dictionary. Available at: http://www.elissetche.org /dico/P.htm.
9. Caslon-Analytics., Retrieved October 2, 2005. Available at: http://www.caslon.com.au/biometricsnote6.htm.
10. Hart, S., Retrieved October 2, 2005. Comments of Privacilla.org on Formulating and Conducting a Study of Biometrics and Similar Technologies to Combat Identity Theft. Available at: http://www.privacilla.org/releases /FACT_Act_Biometric_Study.html.
11. FAQ's and Definitions., Retrieved October 2, 2005. International Biometric Group, LLC. Available at: http://www.bioprivacy.org/bioprivacy_text.htm.
12. Checco, J.C., Retrieved October 2, 2005. Keystroke Dynamics & Corporate Security. Available at: http://www.wsta.org/publications/ articles/1003_article06.html.

13. Desmarais, N., Retrieved October 2, 2005. Biometrics and Network Security. Available at: www.acrlnec.org/sigs/itig/tc_nov_dec2000.htm.
14. Maxion, R.A. and T.N. Townsend., June 23-26, 2002. Masquerade Detection Using Truncated Command Lines. International Conference on Dependable Systems and Networks. Washington, DC.
15. Schonlau, M., et al., 2001. Computer Intrusion: Detecting Masquerades. Statistical Science, 16(1): p. 1-17.
16. Goldring, T., 2003. User Profiling for Intrusion Detection in Windows NT. Computing Science and Statistics, 35.
17. Vel, O.D., et al., 2001. Mining Email Content for Author Identification Forensics. SIGMOD: Special Section on Data Mining for Intrusion Detection and Threat Analysis.
18. Yampolskiy, R.V., April 2-4, 2007. Secure Network Authentication with PassText. 4th International Conference on Information Technology: New Generations (ITNG 2007). Las Vegas, Nevada, USA.
19. Ramon, J., N. Jacobs, and H. Blockeel., 2002. Opponent modeling by analysing play. Proceedings of Workshop on agents in computer games. Edmonton, Alberta, Canada.
20. Yampolskiy, R.V. and V. Govindaraju., April 9-13, 2007. Dissimilarity Functions for Behavior-Based Biometrics. Biometric Technology for Human Identification IV. SPIE Defense and Security Symposium. Orlando, Florida.
21. Yampolskiy, R.V. and V. Govindaraju., 17-22 April 2006. Use of Behavioral Biometrics in Intrusion Detection and Online Gaming. Biometric Technology for Human Identification III. SPIE Defense and Security Symposium. Orlando, Florida.
22. Yampolskiy, R.V., February 24, 2006. Behavior Based Identification of Network Intruders. 19th Annual CSE Graduate Conference (Grad-Conf2006). Buffalo, NY.
23. Stecklow, S., J. Singer, and A. Patrick., Retrieved October 4, 2005. Watch on the Thames. The Wall Street Journal. Available at: http://online.wsj.com/public/article/SB1120773406 47880052cKyZgAb0T3asU4UDFVNPWrOAqCY _20060708.html.
24. Erzin, E., et al., April 2006. Multimodal Person Recognition for Human-Vehicle Interaction. IEEE MultiMedia.
25. Erdogan, H., et al., June 2005. Multi-modal person recognition for vehicular applications. N.C. Oza et al. (Eds.) MCS 2005, LNCS 3541. Monterey CA.
26. Erdogan, H., et al., September 2005. Experiments on decision fusion for driver recognition. Biennial on DSP for in-vehicle and mobile systems. Sesimbra Portugal.
27. Kim, Y., J.-Y. Jo, and K. Suh., April 2006. Baseline Profile Stability for Network Anomaly Detection. IEEE ITNG 2006, Internet and Wireless Network Security track. Las Vegas, NV.