


Algorithm “DPTM” for continuous authentication with behavioural biometrics

 openaccessgovernment.org/article/algorithm-dptm-for-continuous-authentication-with-behavioural-biometrics/176858/

Takeshi Yamada, Professor from Daiichi Institute of Technology, describes the algorithm “DPTM” for continuous authentication with behavioural biometrics, beginning with the current device security outlook

Cyberattacks and cybercrimes increase every year. Under such a scenario, the user’s need for security enhancement is urgent. Looking at current user authentication, most are authenticated only at the login stage, with ID and password, biometrics, or other forms.

Recently, multi-factor authentication has become popular and enhanced security, which also authenticates, but only when logged in. Therefore, if users forget to log out or lock the screen, leaving the device unattended, such as a PC or smartphone, unauthorised users can easily manipulate the device and cause severe damage. If an unauthorised user can easily manipulate the screen, the security level will be low, and some measures to increase security are necessary.

“Continuous Authentication”

To increase security after login, a method called “Continuous Authentication” is performed (continuously). Everyone may immediately think of the process in which conventional ID and password authentication is performed periodically. In addition, there are physical or behavioural biometrics for continuous authentication. Each characteristic of the methods is as follows:

1. Conventional method with ID and password for continuous authentication

The method periodically prompts users to enter their ID and password. The advantage is that the authentication accuracy is 100%. This can be used to confirm that the authorised user is operating the terminal. However, this method requires users to enter their ID and password several times during their working day, and such an interruption is a significant burden.

Another problem is the “leakage” of IDs and passwords. If a legitimate user’s ID and password are known to unauthorised users, it is impossible to continue the authentication, and unauthorised users can operate the terminal freely.

2. Physical biometrics for continuous authentication

A method with physical biometrics for continuous authentication includes fingerprint, iris, and face recognition. This method is highly accurate and practical. However, as with the ID and password scenario described above, it requires periodic authentication, which burdens users enormously. Moreover, the cost is high, as a dedicated device is needed.

Furthermore, face recognition also involves a significant psychological burden because the camera always points at the face, and many users are concerned about the unpleasant possibility that video may have been leaked onto the Internet.

Another disadvantage is that it can be easily forged, as the face is constantly exposed to the outside world. Also, continuous authentication by remote access has information leakage and privacy violation issues, as the information on the nasal cords must be transmitted over the network. The most severe problem is that it cannot be used for authentication again once the information is stolen, even if the user is the person themselves.

3. Behavioural biometrics for continuous authentication

A method with behavioural biometrics for continuous authentication includes handwriting, voice print, and gait: the person's habits (features). Although the accuracy and speed are inferior to those using human body features, the users are not required to authenticate periodically because the feature values are obtained from terminal operations (e.g., critical operations, mouse operations, touch operations, etc.) with no burden on the user. In addition, there is no need to install specialised equipment or devices, and it is difficult to forge with low privacy, causing almost no psychological stress. Behavioural biometrics for continuous authentication would be a suitable and easy-to-adopt method.

Algorithm "DPTM" research for continuous authentication

We have researched Behavioural Biometrics for Continuous Authentication, and in 2017, the author proposed the Dynamic Probability Trust Model (DPTM) algorithm.⁽¹⁾

The contents and results of the evaluation experiments were as follows:

Two hundred eighty-seven subjects provided logs of PC keystrokes and mouse operations, and features were extracted from the log data to get the Equal Error Rate (the value at which the trade-off between the False Rejection Rate and the False Acceptance Rate becomes equivalent), which was found to be 4.86%. The accuracy was higher than that of the machine learning-based continuous authentication. The Equal Error Rate of less than 5% meets the general security requirements.

Plus, a performance table was created to evaluate the performance of the continuity authentication proposed in the literature.⁽²⁾ The table was proposed to consider that the equivalent error rate is insufficient and the continuation of actions by legitimate users should be required to detect illegal users' activity. The result showed that DPTM is superior in almost all aspects compared to machine learning.

DPTM's current initiatives and prospects

We are currently applying DPTM to the touch operation of mobile terminals and confirm its usefulness. In addition, we are researching user-specific features and how much we can increase the accuracy and speed of behavioural biometrics for continuous authentication.

Moreover, we are also studying how to respond to changes in legitimate users' characteristics over time. Although there are still issues to be solved, once biometrics is established, it can be applied to enhance the security of PCs, mobile terminals, various systems, remote access, etc. and many other things. Continuous authentication using IDs and passwords or biometric continuous authentication using physical characteristics has a narrow range of applications because of the nature of periodically checking whether a pattern matches a predetermined one.

On the other hand, behavioural biometrics for continuous authentication comprehensively determines whether a user is authentic or not based on several features collected in real time. This is not limited to continuous authentication for security enhancement but can also be applied to support anomaly detection, situation recognition, situation judgement, and decision-making with the selected feature values. For example, detecting abnormalities is possible by continuously extracting appropriate features from constantly changing situations, such as security camera images or health monitoring via wearable devices.

Similarly, in rapidly changing environments such as sports and automated driving, the continuous collection and analysis of appropriate features enables the comprehensive understanding of the current situation and decision-making support. Other potential applications of this technology include emotion reading through facial expressions or tone of voice and comprehension of students' understanding in an educational environment.

The study of behavioural biometrics for continuous authentication is not limited to mere security enhancement but has unlimited possibilities. We are confident that the research will contribute to making it an indispensable part of your daily life in the future.

References

1. Takeshi YAMADA, Shinya FUKUMOTO, Masayuki KASHIMA, Kiminori SATO, and Mutsumi WATANABE, "Proposal and Authentication Accuracy of continuous Authentication Algorithm DPTM Using Dynamic Biometrics of Keystroke and Mouse Dynamics", The IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences A, Vol. J103-A, No. 11, pp. 255-269, 2020.
2. S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics", Neurocomputing, vol. 230, pp. 1-22, 2017.

Please Note: This is a Commercial Profile



This work is licensed under [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).