

Biometria przez sieć WLAN: Zakłócenia sygnału umożliwiają rozpoznawanie i monitorowanie osób

Włoscy naukowcy opracowali metodę identyfikacji osób wyłącznie na podstawie zniekształceń sygnału Wi-Fi. Kamery nie są tu potrzebne.



(Kompilacja: ZinaidaSopina/Shutterstock.com)

10.08.2025, 11:35

Czas czytania: 4 minuty

- Autor: [Stefan Krempel](#)

Naukowcy z Uniwersytetu Sapienza w Rzymie opracowali technologię, która umożliwia potajemną identyfikację osób wyłącznie poprzez analizę sygnałów Wi-Fi – bez kamer i aktywnego udziału. Ten proces, stanowiący poważne zagrożenie dla prywatności, wykorzystuje fakt, że każdy ludzki organizm zakłóca sygnały Wi-Fi w unikalny sposób. Naukowcy nadali tej technologii, która początkowo brzmi jak dystopijna fantastyka naukowa, nazwę WhoFi, nawiązując do międzynarodowego terminu Wi-Fi.

Podstawą jest fakt, że każdy człowiek pozostawia po sobie niewidzialny ślad Wi-Fi. Naukowcy opracowali specjalny model wykorzystujący sztuczną inteligencję, który analizuje te minimalne zmiany sygnału w postaci informacji o stanie kanału.

zrecenzowany, że cechy biometryczne, takie jak kształt ciała, wzrost i ruch, są „wyodrębniane z informacji o stanie kanału (CSI) i przetwarzane przez modułową głęboką sieć neuronową (DNN)” za pomocą specjalnego kodera [Zespół pisze w artykule, który nie został jeszcze niezależnie](#). Sieć neuronowa jest trenowana z wykorzystaniem funkcji uczenia kontrastowego w celu identyfikacji solidnych i uogólnialnych sygnatur biometrycznych. To podejście pomaga modelowi dowiedzieć się, które punkty danych są podobne („pozytywne”), a które niepodobne („negatywne”).

W kontekście urządzeń Wi-Fi, CSI odnosi się między innymi do informacji o amplitudzie i fazie transmisji elektromagnetycznych. Według badań pomiary te oddziałują na ludzkie ciało w sposób, który prowadzi do zniekształceń specyficznych dla danej osoby.

Dokładność rozpoznawania ponad 95 procent

Naukowcy wprowadzili do sieci, która zasadniczo działa jak mały komputerowy mózg, informacje z zestawu danych NTU-Fi. Jest on rutynowo wykorzystywany do wykrywania obecności ludzi za pomocą sygnałów Wi-Fi. Według badania, ich własne eksperymenty pokazują, że to podejście „osiąga konkurencyjne wyniki w porównaniu z najnowocześniejszymi metodami i potwierdza swoją skuteczność w identyfikacji osób za pomocą sygnałów Wi-Fi”. System może zatem wykryć, czy ktoś znajduje się w pomieszczeniu i kim jest ta osoba, z dokładnością do 95,5%.

Technologia ta działa bez widocznego nadzoru i bez wiedzy osób, których dotyczy. Teoretycznie system ten mógłby służyć do identyfikacji osób wszędzie tam, gdzie jest dostęp do Wi-Fi – w domach, biurach czy budynkach użyteczności publicznej.

Rozpoznawanie twarzy: zawodne

Naukowcy opisują tę metodę jako alternatywę dla konwencjonalnego rozpoznawania biometrycznego, które do tej pory opierało się głównie na obrazach z kamer. Metoda ta zasadniczo mierzy unikalne cechy biologiczne lub behawioralne danej osoby i porównuje je z przechowywanymi danymi. Zautomatyzowane systemy nadzoru biometrycznego, takie jak rozpoznawanie twarzy i chodu, wykorzystują kamery i specjalistyczne oprogramowanie do identyfikacji osób w czasie rzeczywistym w większym otoczeniu, bez konieczności interakcji z systemem.

Jednak systemy wizualnego rozpoznawania twarzy lub chodu są wrażliwe na czynniki zewnętrzne. Słabe warunki oświetleniowe, zasłonięte twarze, zmieniające się kąty widzenia lub niska jakość obrazu mogą poważnie wpłynąć na dokładność. Tradycyjne metody biometryczne są zatem „zawodne”, uważa zespół. Nowa biometria bezprzewodowa jest bardziej niezawodna, ponieważ wykorzystuje unikalne zniekształcenia sygnału. Wynikają one nie tylko z cech zewnętrznych, ale także ze struktur wewnętrznych, takich jak kości i narządy. Prowadzi to do zakłóceń, które mogłyby posłużyć za indywidualny podpis. W kolejnym kroku te cechy biometryczne są porównywane ze znanymi danymi referencyjnymi w celu jak najdokładniejszej identyfikacji osób.

Surowe dane powinny być anonimowe

Chociaż badania w tej dziedzinie są wciąż na wczesnym etapie, ich rozwój już teraz rodzi poważne pytania dotyczące ochrony danych: gdzie leży granica między postępem technologicznym a prawem do prywatności, skoro nawet niewidzialne sygnały wewnątrz i wokół ludzi mogą być wykorzystywane do inwigilacji? Aktywiści ostrzegają już [przed masową inwigilacją obywateli za pomocą automatycznego rozpoznawania twarzy](#), która w przyszłości może przybrać zupełnie inny wymiar.

Sami naukowcy podkreślają jednak, że surowe dane Wi-Fi gromadzone w celu identyfikacji osób są z natury anonimowe. Oznacza to, że jeśli wpadną w niepowołane ręce, będą bezużyteczne dla atakujących. Bez specjalnie opracowanego modelu sztucznej inteligencji i powiązanego z nim systemu, nie da się zidentyfikować żadnej osoby.

Na przestrzeni lat naukowcy odkryli, że sygnały Wi-Fi mogą być wykorzystywane do różnych celów, m.in. [do widzenia przez ściany](#), wykrywania upadków, wykrywania obecności człowieka i rozpoznawania gestów, w tym języka migowego.