УДК 004.934.2

ГІРОФОН – РОЗПІЗНАВАННЯ МОВИ ПО СИГНАЛАМ ГІРОСКОПА

І. В. Христюк[1, a], В. М. Степаненко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В роботі показано, що гіроскопи MEMS, що встроєні в сучасних смартфонах, досить чутливі для реєстрації акустичних сигналів, що знаходяться поблизу телефону. Отримані на виході MEMC-датчиків сигнали містять лише низькочастотну інформацію (<200 Гц). Тим не менш, застосовуючи обробку сигналів та машинне навчання, можна використовувати цю інформацію для ідентифікації мовця та для синтаксичного аналізу мови. Оскільки iOS та Android не потребують спеціальних дозволів для доступу до гіроскопа, виявляється, що програми та активний веб-вміст, що не мають прав доступу до мікрофона, можуть підслуховувати мовлення поблизу телефону.

Ключові слова: Аналіз мови, MEMS

Вступ

Сучасні смартфони та мобільні пристрої мають безліч датчиків, що забезпечують розширений спектр можливостей для користувачів. Зазвичай їх використовують для вимірювання, сигналізації, регулювання, керування приладами та процесами. Але іноді вони можуть використовуватися як об'єкти витоку інформації, якою користувач не планує ділитися. Хоча ризики конфіденційності, пов'язані з деякими датчиками, такими як мікрофон (прослуховування), камера чи GPS (відстеження), очевидні та добре зрозумілі, деякі ризики все ж залишаються під контролем користувачів та розробників додатків. Зокрема, доступ до датчиків руху, таких як гіроскоп та акселерометр, не обмежується мобільними операційними системами. А саме, кожна програма, встановлена на телефоні, і кожна веб-сторінка, яка переглядається , може мати доступ до цих датчики, не повідомляючи про це користувача.

1. Характеристики гіроскопа як мікрофона

Через акустичну сприйнятливість MEMS [1] гіроскопа можна сказати, що показання гіроскопа – це ніби звукові зразки, що надходять до мікрофона. Звертаю увагу, що частота звукового сигналу перевищує 20 Гц, тоді як у загальних випадках частота зміни кутової швидкості мобільного пристрою нижча ніж 20 циклів в секунду. [2], [3]

Отже, можна фільтрувати високочастотні показання, щоб зберегти лише ефекти звукового сигналу, навіть якщо мобільний пристрій рухається. Тим не менш, слід зазначити, що ця фільтрація може призвести до певної втрати акустичної інформації, оскільки деякі зовнішні частоти можуть бути відфільтровані.

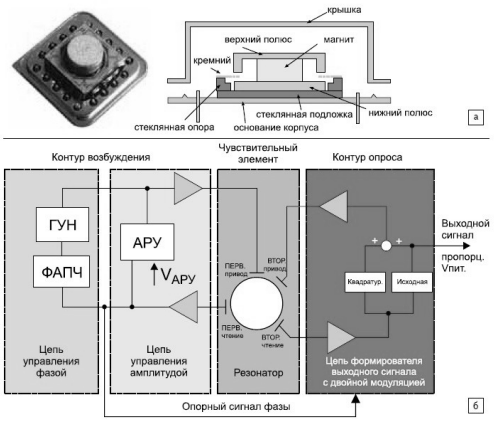

Рис. 1. Гіроскоп: а) конструкція; б) блок-схема

2. Налаштування експерименту

Експериментальна установка складається з набору гучномовців, які включають сабвуфер та два високочастотні динаміки (зображено на рис.2). Сабвуфер є важливим для експериментів з низькочастотними тонами нижче 200 Гц. Гучність відтворення звукових сигналів складає 75 дБ, щоб отримати якомога більше співвідношення сигнал/шум (SNR) для більшої якості розпізнавання звуків. Це означає, що для більш обмежувальних сценаріїв атак (надалі джерело) буде необхідність обробки низького SNR, можливо, фільтруючи шум або застосовуючи якусь іншу попередню обробку для виділення мовного сигналу. [4]

3. Експериментальні дані

Через низьку частоту дискретизації гіроскопа, розпізнавання загальної мови, що не залежить від мовця, могло б займати багато часу. Тому в роботі, ідентифікація мови обмежена словником, розпізнавання якого все одно даватиме значну приватну інформацію. Було зосереджено увагу на словнику цифр, який

[a] iren02.07.2000@gmail.com

Рис. 2. Експериментальна установка

включає слова: нуль, один, два ..., дев'ять та "о". Розпізнавання таких слів дозволить зловмиснику підслуховувати особисту інформацію, таку як номера кредитних карток, номера телефонів тощо. Ця інформація може прослуховуватись, коли жертва говорить поруч із телефоном. [3]

4. Основні методи захисту

В роботі розглянуті деякі способи зменшення потенційних ризиків. Для надійної конструкції потрібен загальний розгляд всієї системи та оцінка можливостей зловмисника, проти якого ми захищаємось. Для захисту від зловмисника, який має лише доступ користувача до пристрою (додаток або веб-сайт), може бути достатньо застосувати фільтр низьких частот до вихідних зразків, наданих гіроскопом. Спираючись з частоти дискретизації, доступної для браузерів на базі Blink та WebKit, досить пропустити частоти в діапазоні $0 - 20$ Гц. Якщо цієї швидкості достатньо для більшості програм, фільтрування може виконувати драйвер або ОС, унеможливлюючи будь-яку спробу підслуховування більш високих частот, які розкривають інформацію про оточуючі звуки. Якщо певна програма вимагає незвично високої частоти дискретизації, вона повинна з'являтися у списку дозволів, які вимагає ця програма, або вимагати явного дозволу користувача. Для захисту від зловмисників, які отримують доступ, такий вид фільтрації слід виконувати на апаратному рівні. Звичайно, це накладає обмеження на частоту дискретизації, доступну для додатків. Іншим можливим рішенням є акустичне маскування. Його можна застосовувати лише навколо датчика або на корпусі мобільного пристрою.

Висновки

Показано, що акустичний сигнал, виміряний гіроскопом, може розкрити приватну інформацію з навколишнього середовища телефону, наприклад, про те, хто говорить у кімнаті, і певною мірою про те, про що йдеться. Для цього використано обробку сигналів та машинне навчання для аналізу мовлення з дуже низьких частот. Подальша робота над низькочастотною обробкою сигналів цього типу повинна мати можливість ще більше підвищити якість інформації, вилученої з гіроскопа.

В результаті роботи виявлено несанкціонований канал витоку конфіденційної інформації, спричинений необмеженим доступом до гіроскопа: програми та активний веб-вміст, що працює на телефоні, можуть підслуховувати звукові сигнали, включаючи мовлення, поблизу телефону. Розроблено кілька стратегій пом'якшення наслідків:

- фільтрація
- доступ до всіх датчиків повинен контролюватися системою

дозволів, розмежовуючи низьку та високу частоти дискретизації.

Вони можуть бути прийняті постачальниками мобільного обладнання для блокування цієї загрози.

Перелік використаних джерел

1. MEMS for Cell Phones and Tablets http://www.i–micronews.com/upload/Rapports/Yole–MEMS–for–Mobile–June–2013–Report–Sample.pdf, July 2013
2. 3-axis digital gyroscopes: http://www.st.com/st–web–ui/static/active/en/resource/sales–and–marketing/promotional–material/flyer/fl3axdigitalgyro.pdf.
3. Меркуренко И. В. Динамика микромеханического и волнового твердотельного гироскопов
4. Василенко М. В. Теорія коливань: Навчальний посібник. — К. : Вища школа, 1992.