SurFi: Detecting Surveillance Camera Looping Attacks with Wi-Fi Channel State Information

Nitya Lakshmanan*, Inkyu Bang†, Min Suk Kang*, Jun Han*, Jong Taek Lee#

*National University of Singapore, †Agency for Defense Development, #Electronics and Telecommunications Research Institute

+ research done while working in NUS
Surveillance cameras are now everywhere

China to have 626 million surveillance cameras within 3 years

Nov 22, 2017  |  BY FRANK HERSEY

Consumer Video Surveillance Market to Top $1 Billion in 2018, IHS Markit Says

Acceptance of video surveillance for the home has grown, in part because people now have more control over their surveillance systems

Nov 08, 2018
Surveillance camera looping attack

Place of interest

valuable

Surveillance system

Security guard

Video shows a normal activity!

Video feed
Surveillance camera looping attack

Place of interest

- valuable

Surveillance system

- video feed

security guard

Video shows a normal activity!

No activity

Surveillance camera looping attack

Place of interest

- valuable

Surveillance system

- video feed

security guard

Video shows a normal activity!

No activity
Surveillance camera looping attack

Place of interest
valuable

Surveillance system
security guard
Video shows a normal activity!

video feed
looped!

No activity
Looped
Surveillance camera looping attack

**Place of interest**

![Diagram of a place of interest with valuable items and a red figure representing a robbery.]  

**Surveillance system**

- **Video feed:** The video feed is *looped!*
- **Security guard:** The surveillance system shows *a normal activity!*

**Reality vs. Seen by the guard**

- **Reality:** Robbery is visible.
- **Seen by the guard:** The video is looped, indicating no activity.

Video shows a normal activity!
Surveillance camera looping is a *reality now*

Exploiting Surveillance Cameras
Like a Hollywood Hacker
BlackHat 2013

Loopping Surveillance Cameras
like in the movies
DefCon 2015

Live video → Replayed image → Modified timestamp
**Mitigation** of camera looping attack is **hard**

Can we mitigate the camera looping attack effectively at no extra hardware cost?

- Incur prohibitive cost
- Not robust against an adversary who can **manipulate** the video

**Surveillance camera with integrity protection**

**Video frame comparison**

Live (3 pm)  
This morning (10 am)
SurFi (Surveillance with Wi-Fi) detects camera looping attack

SurFi achieves attack detection accuracy of 98.8% and false positive rate of 0.1%
System model: *indoor space* under *video surveillance*

- ✓ Place of interest such as bank or jewelry store
- ✓ Field-of-view of the camera
- ✓ CSI measurement cannot be compromised
Threat model: adversary can *loop* surveillance video feed

- ✓ Manipulate video feed
- ✓ Evade detection of his unauthorized activities
Challenge: *video* and *CSI* signals are *different*

How to find **common attributes** for reliable comparison of two **different sensing modalities**?

- ✓ Displacement of body keypoints (e.g., wrist, elbow)
- ✓ Amplitude of subcarriers
Main intuition: Both signals capture the similar **timing** and **frequency** components

- **Timing components**: Start and end time of the activity
- **Frequency component**: Prominent frequency

Reliable detection observed consistently across **different activities, people, and times**
System design of SurFi

Data Pre-processing module
- Live video feed
- Wi-Fi CSI signal
- OpenPose
- Denoise

CSI event detector module
- New Event (i) detected

Attribute extraction module
- Video attributes
- CSI attributes

Comparison module
- Compute similarity score \( S(i) \)

Decision module
- Event(1), \( S(1) \)
- Event(i), \( S(i) \)
- Event(N), \( S(N) \)

looped or not?
1) Data preprocessing module: 
*Preprocesses* the raw video and CSI signals
1) Data preprocessing module: **Preprocesses** the raw video and CSI signals

- **Raw video signal** → **OpenPose** → **Processed video signal**
- **Raw CSI signal** → **Denoise** → **Processed CSI signal**

- ✓ Filter high frequency noises
2) CSI event detector module:
Uses the *motion energy* to detect the *start of a new event*
3) Attribute extraction module: Extracts *common attributes*
4) Comparison module:
Computes the **per-event similarity score** of a single event

\[
\sum_{i=0}^{3} \text{Per-event similarity score } S(i)
\]
5) Decision module:
Outputs *looped or not* after observing *multiple events*

The more the events seen, the higher the confidence for the final decision
Experiment setup

• Redmi Note 4 phone camera (13-Megapixel)

• Wi-Fi transmitter receiver pair set up on Thinkpad laptops running Linux 802.11n CSI tools

![Diagram of experiment setup]

Place of interest

- 2.6-meter
- 4.9-meter
Three events

(E1) stand/arm waving

(E2) sit/fist thumping

(E3) sit/clapping
Clear difference in the per-event similarity

![Bar chart showing per-event similarity scores for Legit and Attack categories across tested events E1, E2, and E3. The chart illustrates a clear difference with Legit having high similarity scores and Attack having low similarity scores.]
Multiple events are observed for a duration of time

Example:
Attack detection accuracy *increases* with more events.

- 5 events: 98.8%
- 1 event: 36%
Future improvements

• Stronger adversary
  • Performs criminal activities while replicating start + end times, prominent frequency of legitimate events
  • Future work: Investigate more attributes

• Multiple events in sequence
  • Future work: Activity recognition techniques
Deployment consideration

• **Threshold calibration**
  • Adjust to the new environment

• **Placement of the receiver**
  • Strategically placing the receiver way from the wall
Conclusion

• First *practical system* to detect surveillance camera looping attack in real-time

• Defense technique requiring *no additional hardware deployment*

• Attack detection accuracy of *98.8%* with false positive rate of *0.1%*

• *Future work*: more diverse events, sophisticated adversary model
Questions?

nityalak@comp.nus.edu.sg
Activities *behind-the-wall* may degrade the performance of SurFi.

Conduct experiments to test behind-the-wall activities.
Strategically placing the receiver at a certain distance from the wall will minimize false alarms.

✓ Varying motion energy may lead to false detection of an activities.

✓ Activities are not detected since the corresponding motion energy is close to zero.