Poster: PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems

Yan He
University of Oklahoma
heyan@ou.edu

Guanchong Huang
University of Oklahoma
guanchong.huang@ou.edu

Song Fang
University of Oklahoma
songf@ou.edu

Title: PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems

Authors: Yan He, Guanchong Huang, Song Fang

Venue: The Network and Distributed System Security (NDSS) Symposium 2026, San Diego, California

DOI: 10.14722/ndss.2026.231454

Full Reference [1]: Yan He, Guanchong Huang, and Song Fang. 2026. PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems. In *Proceedings of the Network and Distributed System Security (NDSS) Symposium 2026.* San Diego, CA, USA, pp. 1-18. https://doi.org/10.14722/ndss.2026.231454

Abstract: Wireless security surveillance systems are widely deployed due to their increased affordability. Motion detection is often integrated into them as the linchpin of the security they provide, detecting when someone is present in its range and then triggering the system to start recording or notifying the property owner. In this paper, we present *PhantomMotion*, a new attack framework to fool the motion detection function of those security systems. It can create fake motion stimuli stealthily by aiming laser beams into the motion detection range, and it confirms a response to the stimuli via sniffing wireless traffic. *PhantomMotion* does not require any professional equipment or to perform physical motion within the monitored area. It consists of a novel hardware platform integrating laser control and WiFi sniffing, and a new generative mechanism of motion injection. We develop a smartphone app to implement *PhantomMotion*, validating its efficacy against 18 popular wireless motion-activated security systems. Experimental results show that *PhantomMotion* can always generate fake motion to successfully trigger the systems, within an average of 12.8 seconds and via moving the laser spot for a mean distance of 1.1 m. Notably, we verify that *PhantomMotion* works from a distance of up to 120 meters.

NDSS 2026 Poster Submission Type: Type 2: Recently Published Research

References

[1] Y. He, G. Huang, and S. Fang, "PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems," in *Network and Distributed System Security (NDSS) Symposium 2026*. The Internet Society, Feb. 2026, pp. 1–18.

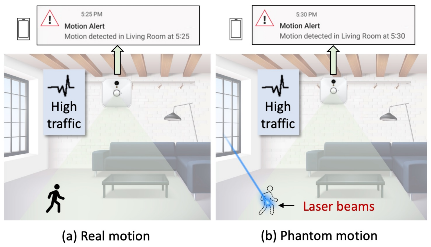
PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems

Yan He, Guanchong Huang and Song Fang
University of Oklahoma
{heyan, guanchong.huang, songf}@ou.edu

** This work has been accepted by NDSS'26 [1].*

Motivation

- **Ubiquitous Surveillance:** Booming wireless cameras market ($43.65B in 2024) leads to severe privacy risks (e.g., Hidden cameras in Airbnbs, hotels).
- **Current Limitations:** Existing camera detection/localization methods (e.g., MotionCompass [2], Lumos [3]) requires physical motion (waving/jumping) → labor-intensive and exposure-prone
- **Our Goal:** Trigger wireless security systems remotely without any human motion. Typical applications include:
  - Remotely triggering cameras to avoid being recorded;
  - Harassing or desensitizing users via a "cry wolf" effect;
  - Rapidly draining device batteries by repeatedly forcing high-power recording states.


5:25 PM
Motion Alert
Motion detected in Living Room at 5:25
High traffic
5:30 PM
Motion Alert
Motion detected in Living Room at 5:30
High traffic
Laser beams

(a) Real motion (b) Phantom motion

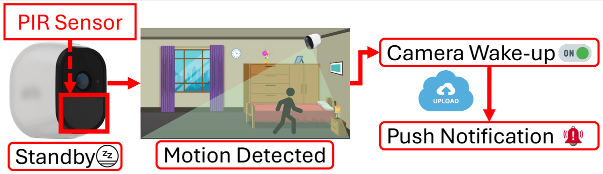
Camera Triggered by Phantom Motion.

Adversary Model

- **Two General Application Domains:**
  1) Attack: Targeting wireless security surveillance systems.
  2) Defense: Targeting spy cameras.
- **No Human Motion**: Avoid being caught or identified by hidden cameras.
- **WiFi Sniffing**: Determine if the camera is activated via wireless traffic analysis.
- **Line-of-sight**: Aim the laser at the target PIR sensor detection zone.

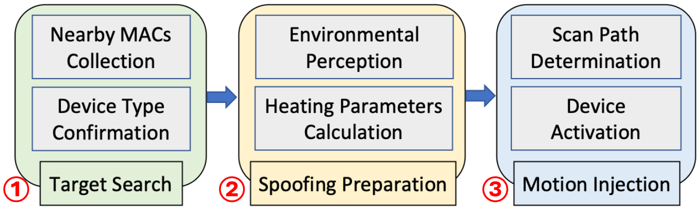
Attack Principle

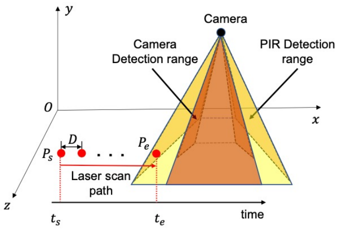
- **Modern Camera Design:** PIR-based motion activation mechanism extends battery life from hours to months by replacing continuous recording.
- **PIR Sensor**: Passive Infrared (PIR) sensor detects motion by sensing temperature differences between an object and the background. It is widely used in wireless security systems with low price (~$3).
- **Laser Motion Injection**: Using a laser to heat a specific spot in the detection zone to match human body temperature (~37^{o}C).



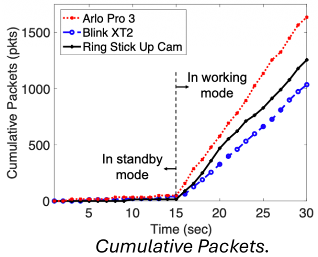
PIR-based Wireless Camera Motion Detection Workflow.

System Design





Outside-in Scanning.



Cumulative Packets.

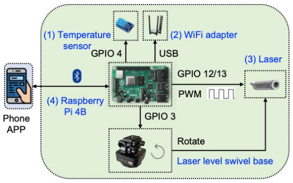
①: Sniff ambient WiFi traffic to identify potential wireless security devices.

②: Measure environmental temperature and calculate the required laser heating parameters for specific materials (e.g., wood, bricks).

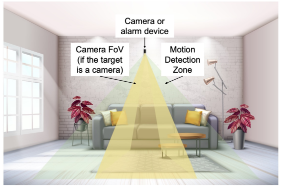
③: User a laser to scan a path, heat points sequentially. The system correlates laser heating with traffic bursts to confirm successful triggering.

Experimental Evaluation

- **Metrics**: Success Rate, False Positive (FP) Rate, Operation Time, Scan Distance.
- **Overall Attack Impact**: Achieved 100% success rate for 18 devices (100 trials per device) with 0 FP (operation time: 8.1–14.7 s; scan distance: 0.8–1.3m).



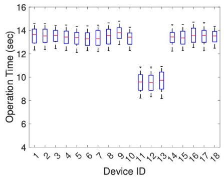
The Testbed of PhantomMotion.



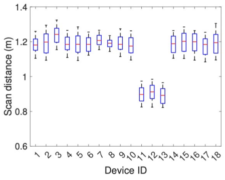
Experiment Environment

ID	Model	WiFi Chipset	PIR Amount
1	Arlo Pro 2	Cypress	1
2	Arlo Pro 3	Cypress	1
3	Blue by ADT	Cypress	1
4	Blink XT2	TI	1
5	eufyCam E	Hisilicon	1
6	Google Nest Cam	Ambarella	1
7	Google Nest Doorbell	Ambarella	1
8	IHOXTX DF22 Cam	MediaTek	1
9	LaView N15 Cam	MediaTek	1
10	Reolink Argus 2	MediaTek	1
11	Ring Spotlight	TI	2
12	Ring Spotlight Pro	TI	2
13	Ring Stick Up Cam	TI	2
14	Simplisafe Cam	Telit	1
15	Wyze Cam Outdoor v2	Ingenic	1
16	Arlo Home Security System	Cypress	1
17	Ring Alarm System	Quectel	1
18	Simplisafe Safety Alarm	Espressif	1

Tested Wireless Security Devices



Overall Operation Time.



Overall Scan Distance

- **Robust Adaptability**: Achieved 100% success rate and 0 FP across diverse materials (brick, aluminum, wood, stone) and environmental temperatures (5^{o}C-30^{o}C).
- **Long-Range Attack**: Achieved 100% success rate and 0 FP at 120 m, bounded by the maximum WiFi sniffing range of 500 feet in an open area.
- **Severe Battery Drain**: For 15 wireless security cameras, continuous attacks accelerate depletion, fully draining batteries in 6.2–15.7 hours, compared to >97% capacity retention under normal usage after 16.5 hours.

References

[1] Y. He, G. Huang, and S. Fang, "PhantomMotion: Laser-Based Motion Injection Attacks on Wireless Security Surveillance Systems," in Network and Distributed System Security (NDSS) Symposium 2026. The Internet Society, Feb. 2026, pp. 1–18.

[2] Y. He, Q. He, S. Fang, and Y. Liu, "MotionCompass: Pinpointing wireless camera via motion-activated traffic," in Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services, ser. MobiSys '21. ACM, 2021, p. 215–227.

[3] R. A. Sharma, E. Soltanaghaei, A. Rowe, and V. Sekar, "Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment," in 31st USENIX Security Symposium. USENIX Association, Aug. 2022, pp. 1095–1112.