IAES Journal of Electrical and Electronics Engineering
Vol. 5, No. 2, December 2018, pp. 25~28
ISSN: 2338-7432, DOI: 10.11591/jeee.v5i2.pp25-28

Beyond motion detection: design, reliability, and communication challenges in PIR-based anti-theft alarm systems

Octa Wisnu[1], Tri Wahono[2]
[1]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received May 6, 2017
Revised Apr 15, 2018
Accepted Jun 8, 2018

Keywords:

Anti-theft alarm
False alarm
Home security
Intruder detection
Passive infrared sensor
PIR
Wireless sensor network

ABSTRACT

Passive infrared (PIR)-based anti-theft alarms offer an affordable way to detect human movement without continuously recording images. Their appeal comes from low power consumption, privacy-friendly operation, simple interfacing, and compatibility with microcontrollers and wireless communication modules. However, a motion event is not automatically evidence of burglary, and practical systems remain vulnerable to false alarms, blind spots, environmental variation, power interruption, and communication failure. This review examines PIR sensing principles and the design of alarm systems that combine sensor placement, signal processing, embedded control, local warning devices, and remote notification. Literature published up to 2017 is synthesized to trace the development from single-sensor alarm triggers to distributed PIR networks and connected intrusion-detection architectures. Particular attention is given to detection range, movement direction, outdoor limitations, alarm verification, energy management, and wireless security. The review finds that dependable protection requires more than a sensitive PIR module: it depends on coverage planning, robust decision logic, fail-safe alert pathways, and secure communication. A practical design framework and research priorities are proposed for improving reliability while retaining the low cost and simplicity that make PIR systems attractive for residential and small-business security.

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

Residential and small-business security systems are increasingly expected to provide timely warnings when unauthorized movement occurs inside a protected area. Conventional security arrangements, such as mechanical locks and standalone sirens, offer limited information about an intrusion and may not notify property owners who are away from the premises. Electronic alarm systems address this limitation by combining sensors, processing units, warning devices, and communication modules. Among the available sensing technologies, passive infrared (PIR) sensors are attractive because they detect changes in infrared radiation without actively transmitting energy or continuously capturing images [1], [2].

Despite their simplicity, PIR-based alarms face an important technical problem: detecting movement does not necessarily mean detecting an intruder. A passing animal, an authorized occupant, changing thermal conditions, or an unsuitable sensor position may produce an unwanted alarm or prevent detection. These limitations can reduce user confidence and make an otherwise inexpensive security device ineffective in practice. This review therefore examines PIR-based anti-theft alarms as integrated systems, focusing on sensing performance, embedded processing, alarm activation, communication reliability, and practical deployment.

2. REVIEW SCOPE AND PIR SENSING PRINCIPLES

This review considers research published up to and including 2017, with emphasis on PIR-based intrusion detection, human movement analysis, connected alarm prototypes, and wireless sensor network security. The selected literature includes journal articles and conference papers with traceable publication records and DOI identifiers. Studies of PIR-based human tracking are included because their findings help explain detection range, movement direction, and sensor coverage, even when their original applications are not explicitly anti-theft alarms. Research on wireless sensor networks is also considered because remote notification introduces communication and security requirements beyond the PIR sensing element itself.

A PIR sensor detects variations in infrared radiation received from objects within its field of view. Human bodies emit thermal radiation, and movement across the sensor's detection zones produces changes in the differential signal generated by its pyroelectric elements. A Fresnel lens is commonly used to divide the monitored area into multiple detection zones and concentrate infrared energy onto the sensing element. The sensor's output is then conditioned and interpreted by an electronic circuit or microcontroller to determine whether a motion event has occurred [3], [4].

The characteristics of a PIR sensor strongly influence the reliability of an alarm system. Detection performance depends on the distance and direction of movement, the thermal contrast between the target and its surroundings, the lens configuration, and the sensor's installation height. Yun and Lee [3] demonstrated that PIR signals contain information related not only to movement detection but also to direction, distance, and speed. Zappi *et al.* [4], [5]. similarly showed that multiple PIR nodes can be used to improve spatial awareness beyond a simple binary motion indication.

3. ARCHITECTURE OF A PIR-BASED ANTI-THEFT ALARM

A practical PIR-based anti-theft alarm can be organized into five functional stages: sensing, signal processing, decision-making, local warning, and remote notification. The PIR module provides the initial motion signal, while a microcontroller evaluates that signal according to the system's armed status and programmed response conditions. When an intrusion event is accepted, the controller activates a buzzer or siren and may switch on a warning light. A GSM, Wi-Fi, or other communication interface can then transmit an alert to the property owner or a monitoring station.

Microcontroller-based designs are particularly suitable for low-cost security applications because they combine input monitoring, timing, and output control in a compact platform. Godbole *et al.* [1] reviewed a theft-prevention concept integrating PIR sensors, a Raspberry Pi, a camera, a buzzer, a relay, and GSM notification. Sahoo and Pati [2] presented an IoT-based intrusion detection architecture using PIR sensors, ZigBee communication, an ESP8266 module, and GSM alerts. These examples illustrate how a basic motion detector can be extended into a connected security system that provides both immediate local warnings and remote information.

The alarm controller should distinguish between the system's armed and disarmed states before responding to a motion event. During the armed state, a valid detection can initiate an alarm sequence, while the disarmed state should prevent routine occupant movement from triggering an alert. Entry and exit delays can also be introduced to allow authorized users to operate the system without activating the siren unintentionally. Yuliza and Sujatmoko [6] described a GSM-connected residential security concept in which PIR detection activates a local siren and sends a message through the mobile network.

4. DETECTION PERFORMANCE AND FALSE ALARM REDUCTION

Detection reliability is one of the most important challenges in PIR-based anti-theft systems. A sensor may fail to detect an intruder who moves slowly, remains outside the effective detection zones, or generates insufficient thermal contrast against the background. Conversely, environmental changes or movement from non-human objects may produce signals that resemble an intrusion event. A dependable system must therefore balance detection sensitivity with the ability to reject irrelevant motion.

Sensor placement is a practical factor that directly affects detection coverage. Installing a PIR unit near an entrance or corridor can improve the probability of detecting movement through a predictable access route, but a single sensor may leave blind spots in a large room. Zappi *et al.* [5] investigated the use of PIR sensor networks to improve the spatial resolution of presence detection, demonstrating the value of combining information from multiple sensing locations. Lee *et al.* [7] also explored a PIR-based indoor location-aware system for smart-home applications, supporting the use of distributed sensing when a single detection point is insufficient.

Signal processing can improve the distinction between meaningful movement and unwanted disturbances. Instead of relying exclusively on a binary output, a controller may examine signal duration,

pulse patterns, amplitude, and the sequence of detections from multiple sensors. Yun and Lee [3] demonstrated that PIR signal features can support the classification of movement direction, distance, and speed, providing a basis for more informative detection decisions. Zappi *et al.* [4] further showed that feature extraction and sensor fusion can improve movement interpretation in distributed PIR networks.

Outdoor deployment introduces additional difficulties because the thermal background can change considerably with weather and time of day. Aldalahmeh *et al.* [8] examined PIR-based intrusion detection at extended ranges and proposed a signal-processing approach that considered the intruder's trajectory and sensor field-of-view geometry. Their work highlights the importance of analyzing the actual PIR signal rather than treating the sensor output as an infallible motion indicator. Choubisa *et al.* [9] investigated the use of an optical camera as a complementary sensing modality for outdoor PIR-based intrusion classification, addressing situations in which environmental temperature conditions weaken PIR performance.

5. COMMUNICATION, ENERGY, AND SYSTEM SECURITY

Remote notification is valuable because an alarm that sounds only inside an unattended building may not produce an effective response. GSM-based communication can deliver short-message alerts without requiring the property owner to remain connected to a local network. Internet-connected architectures can provide additional functions, such as event logging, remote status checking, and integration with other smart-home devices. However, each communication method introduces dependencies on network availability, power consumption, and the security of transmitted information.

Wireless sensor networks provide a useful framework for connecting multiple PIR nodes across a protected property. Their distributed architecture can improve spatial coverage, but wireless communication also creates potential vulnerabilities involving unauthorized access, message manipulation, and denial of service. Alrajeh *et al.* [10] reviewed intrusion-detection approaches for wireless sensor networks and discussed the security challenges associated with distributed sensor communication. Yang *et al.* [11] examined security technologies for wireless sensor networks, including authentication, key management, and secure routing, which are relevant to connected alarm installations.

Energy management is another important consideration, especially for battery-powered sensors and remote installations. Continuous sensing, frequent wireless transmissions, and persistent camera operation can shorten battery life and increase maintenance requirements. Ghosal and Halder [12] reviewed energy-efficient intrusion detection in wireless sensor networks, emphasizing the need to balance security functions with the limited resources of sensor nodes. For PIR-based alarms, event-driven communication and selective activation of higher-power components can reduce unnecessary energy consumption while maintaining an active detection function.

The security of the alarm system itself must not be overlooked. A system that sends alerts through an unsecured wireless channel may expose sensitive information or allow an attacker to interfere with event reporting. Authentication, protected communication, access control, and secure configuration are therefore important even in relatively simple residential devices. Abduvaliyev *et al.* [13] discussed key research areas in wireless sensor network intrusion detection, providing a broader security context for systems that rely on distributed sensing and wireless communication.

6. INTEGRATED DESIGN RECOMMENDATIONS AND FUTURE RESEARCH

A reliable PIR-based anti-theft alarm should be designed around the physical characteristics of the protected location rather than around the sensor module alone. The design process should begin with identifying likely entry routes, room dimensions, possible obstructions, and the expected movement patterns of occupants. Sensor placement should then be selected to minimize blind spots and provide suitable coverage of vulnerable access points. Where one sensor cannot provide adequate coverage, multiple PIR units or complementary sensing technologies should be considered.

The controller should use a structured decision process to reduce false alarms without introducing excessive detection delays. A practical implementation can combine an armed-state check, signal-duration filtering, a short confirmation interval, and multi-sensor agreement where available. Local siren activation should remain possible even when the communication network is unavailable, while remote notification should be treated as an additional response channel. Backup power and a clear indication of system status are also important because a security device must remain dependable during ordinary power interruptions.

Future research should prioritize standardized testing under different indoor and outdoor conditions. Evaluation should report detection probability, false-alarm rate, detection latency, communication delay, and power consumption rather than relying only on demonstrations that the buzzer or message function operates. More attention is also needed on the effect of pets, thermal background changes, sensor ageing, and deliberate attempts to bypass or disable the detection unit. These measures would provide a more realistic

basis for comparing PIR-based alarm designs and assessing their suitability for long-term security applications.

7. CONCLUSION

PIR-based anti-theft alarms provide a practical and relatively inexpensive approach to detecting movement in residential and small-business environments. Their effectiveness, however, depends on more than the sensitivity of the sensing element, because sensor placement, signal interpretation, controller logic, power management, and communication reliability all influence the final security outcome. Research up to 2017 demonstrates a progression from simple motion-triggered alarms toward distributed PIR networks and connected intrusion-detection systems. The literature also shows that false alarms, outdoor thermal conditions, limited coverage, and wireless vulnerabilities remain important challenges. A dependable design should therefore combine careful coverage planning, appropriate signal processing, independent local warning, secure remote notification, and backup power. With these considerations, PIR technology can serve as a useful foundation for accessible and maintainable anti-theft alarm systems.

REFERENCES

[1] S. Godbole, S. Deshpande, N. Barve, and S. Galim, "Review on theft prevention system using raspberry Pi and PIR sensor," *International Journal of Computer Applications*, vol. 155, no. 11, pp. 8–11, 2016, doi: 10.5120/ijca2016912026.

[2] K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor," in *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, 2017, pp. 1641–1645. doi: 10.1109/RTEICT.2017.8256877.

[3] J. Yun and S. S. Lee, "Human movement detection and identification using pyroelectric infrared sensors," *Sensors (Switzerland)*, vol. 14, no. 5, pp. 8057–8081, 2014, doi: 10.3390/s140508057.

[4] P. Zappi, E. Farella, and L. Benini, "Tracking motion direction and distance with pyroelectric IR sensors," *IEEE Sensors Journal*, vol. 10, no. 9, pp. 1486–1494, 2010, doi: 10.1109/JSEN.2009.2039792.

[5] P. Zappi, E. Farella, and L. Benini, "Enhancing the spatial resolution of presence detection in a pir based wireless surveillance network," in *2007 IEEE Conference on Advanced Video and Signal Based Surveillance, AVSS 2007 Proceedings*, 2007, pp. 295–300. doi: 10.1109/AVSS.2007.4425326.

[6] Yuliza and J. Sujatmoko, "Design and Modeling of a Residential Security Control System Using a GSM Network," *Universitas Mercu Buana ISSN*, vol. 8, no. 2, p. 142932, 2017, [Online]. Available: https://jte.mercubuana.ac.id/publications/142932/

[7] S. Lee, K. N. Ha, and K. C. Lee, "A pyroelectric infrared sensor-based indoor location-aware system for the smart home," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 4, pp. 1311–1317, 2006, doi: 10.1109/TCE.2006.273150.

[8] S. Aldalahmeh, A. Hamdan, M. Ghogho, and D. McLernon, "Enhanced-range intrusion detection using pyroelectric infrared sensors," in *2016 Sensor Signal Processing for Defence, SSPD 2016*, 2016, pp. 1–5. doi: 10.1109/SSPD.2016.7590597.

[9] T. Choubisa *et al.*, "An optical-camera complement to a PIR sensor array for intrusion detection and classfication in an outdoor environment," in *Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017*, 2017, pp. 44–52. doi: 10.1109/LCN.Workshops.2017.63.

[10] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: A review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 167575, 2013, doi: 10.1155/2013/167575.

[11] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," *Journal of Sensors*, vol. 1, p. 842392, 2015, doi: 10.1155/2015/842392.

[12] A. Ghosal and S. Halder, "A survey on energy efficient intrusion detection in wireless sensor networks," *Journal of Ambient Intelligence and Smart Environments*, vol. 9, no. 2, pp. 239–261, 2017, doi: 10.3233/AIS-170426.

[13] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013, doi: 10.1109/SURV.2012.121912.00006.