Anti-theft and Anti-vandalism Design and Prospects for Solar-Powered Insecticidal Lamp IoT Nodes (Postprint)

Authors: Huang Kai, Shu Lei, Li Kailiang, Yang Xing, Zhu Yan, Wang Xiaohan, Su Qin

Date: 2023-02-17T00:00:00+00:00

Abstract

Solar insecticidal lamps can reduce pesticide application while effectively controlling pest populations. However, as deployment numbers increase, reports of theft and vandalism have become more frequent, seriously compromising pest control efficacy and causing substantial economic losses. To effectively address the issue of theft and vandalism of solar insecticidal lamp IoT nodes, this study takes the solar insecticidal lamp IoT as its application scenario and modifies the hardware design to obtain richer sensor information; it also proposes an auxiliary device—the drone-mounted insecticidal lamp—for emergency applications such as deployment, tracking, and inspection following theft or vandalism incidents. While these hardware-level modifications and auxiliary devices enable more comprehensive information gathering to determine the status of node theft and vandalism, the short duration of such incidents means that hardware modifications alone are insufficient for rapid and accurate detection. Therefore, this study further investigates six key research issues across three levels—internal hardware, software algorithms, and structural design: optimization design for anti-theft and anti-vandalism, establishment of judgment rules for anti-theft and anti-vandalism, rapid and accurate judgment of device theft and vandalism, emergency measures for device theft and vandalism, prediction and prevention of device theft and vandalism, and optimized calculation to reduce network data transmission load. Finally, it provides an outlook on the application of anti-theft and anti-vandalism technologies in the solar insecticidal lamp IoT scenario.

Full Text

Design and Prospect for Anti-theft and Anti-destruction of Nodes in Solar Insecticidal Lamps Internet of Things

HUANG Kai[1,2], **SHU Lei**[2,3*], **LI Kailiang**[2], **YANG Xing**[2], **ZHU Yan**[1], **WANG Xiaochan**[4], **SU Qin**[2]

[1]National Engineering and Technology Center for Information Agriculture, Nanjing 210095, China
[2]College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210031, China
[3]School of Engineering, University of Lincoln, Lincoln, LN67TS, U.K.
[4]College of Engineering, Nanjing Agricultural University, Nanjing 210031, China

Abstract: Solar insecticidal lamps (SILs) effectively control pests while reducing pesticide application. However, as deployment numbers increase, reports of theft and vandalism have grown substantially, severely impacting pest control efficacy and causing significant economic losses. To address this problem in the Solar Insecticidal Lamps Internet of Things (SIL-IoTs) context, this study proposes two complementary approaches. First, SIL hardware was retrofitted to acquire richer sensor information, incorporating a gated switch, voltage/current sensors, an emergency power module, and an accelerometer to detect tampering. Second, an auxiliary device—the unmanned aerial vehicle insecticidal lamp (UAV-IL)—was introduced for emergency deployment, tracking, and inspection after theft or destruction occurs. These hardware modifications provide comprehensive data for assessing SIL-IoT node status. However, given the rapid nature of theft and vandalism events, hardware improvements alone are insufficient for fast, accurate detection. Therefore, this study identifies six critical research issues spanning internal hardware, software algorithms, and structural design: (1) optimal anti-theft/anti-destruction device design; (2) establishment of judgment rules for theft and destruction; (3) rapid and accurate detection of theft and destruction events; (4) emergency response measures; (5) prediction and prevention of theft and destruction; and (6) optimized computation to reduce network data transmission load. The paper concludes with an outlook on anti-theft and anti-destruction technologies for SIL-IoT nodes.

Keywords: solar insecticidal lamp; anti-theft and anti-destruction; unmanned aerial vehicle insecticidal lamp; agricultural Internet of Things; node

---

1 Current Status of Theft and Destruction of Solar Insecticidal Lamps

Solar insecticidal lamps are widely used in agriculture, effectively reducing egg-laying by adult pests during field growth stages and decreasing subsequent fertil-

izer and pesticide usage while enabling pest monitoring to ensure food security [1]. However, mounting research and reports indicate that theft and vandalism of solar insecticidal lamps are severe problems (as shown in Figure 1 [Figure 1: see original paper]).

Figure 1 shows theft and destruction scenarios [2]. Table 1 summarizes relevant literature and reports on SIL theft and destruction. Analysis reveals the following primary causes:

(1) **High equipment value.** Analysis of 255 SIL products available online shows an average price of 2,039.5 RMB (range: 220.0–20,000.0 RMB) [23]. According to Li et al. [1], networked SIL products with anti-theft functions [25-29] face several scenarios when theft or destruction occurs: (a) entire lamp theft—if the complete, functional lamp is stolen, location tracking can identify the theft and enable recovery; (b) component theft—when components are stolen, the system only shows module faults without distinguishing theft from failure, and if the battery is stolen without backup power, the status cannot be determined; (c) entire lamp destruction—if all components (including battery) are destroyed without backup power, the status cannot be determined; and (d) component destruction—when components are destroyed, the system only shows module faults without distinguishing destruction from failure, and if the battery is destroyed without backup power, the status cannot be determined.

(2) **High surveillance costs.** SILs are often deployed in sparsely populated areas. Adding cameras and other monitoring equipment significantly increases hardware investment and costs, hindering widespread adoption, while the monitoring devices themselves face theft and vandalism risks [24].

(3) **Incomplete surveillance communication.** Existing SIL anti-theft functions primarily rely on GPRS modules [1], which only detect entire-lamp theft as shown in Figure 1(a) when the stolen lamp remains functional [2]. This approach cannot detect component theft or destruction and incurs ongoing data traffic costs.

(4) **Inadequate SIL management.** After node theft or destruction, lack of emergency response measures delays restoration, potentially leading to further losses.

Currently, SIL theft, destruction, and component failures all display as "fault" status in systems, making it difficult for maintenance personnel to determine the actual operational state. Table 1 documents numerous cases from literature and reports where SIL components were lost, damaged, or stolen, highlighting the severity of the problem.

If theft and destruction status could be accurately identified, maintenance personnel could respond quickly to minimize losses. However, current anti-theft functions require the precondition of a complete, functional lamp, indicating

that SIL anti-theft capabilities need substantial improvement.

Additionally, the authors reviewed the current state of IoT device security research (Table 2). The SIL-IoT scenario shares characteristics with three other device types but also has distinct differences. Existing countermeasures have limitations that can be addressed by combining approaches from these three scenarios to improve SIL theft and destruction responses.

Therefore, retrofitting current SIL-IoT nodes can achieve more comprehensive anti-theft and anti-destruction functionality. Based on the SIL-IoT proposed by the research team [1], this study considers two aspects of SIL anti-theft/anti-destruction design: (1) internal improvements—adding anti-theft sensors while considering cost and power consumption to provide data support for assessing component theft/destruction, with on-site alarms to minimize losses; and (2) external support—designing a highly mobile auxiliary device (UAV-IL) for emergency deployment to ensure normal network communication and provide effective evidence for theft/destruction cases.

2 Retrofit Design Requirements and Feasibility

2.1 Retrofit Design Requirements

SILs face theft and vandalism risks at all times, requiring monitoring solutions that address different time periods. Main SIL-IoT node components include: solar panels, batteries, insecticidal lamps, communication modules (antennas and wireless devices), control circuits, sensor modules, and mounting brackets. As shown in Figure 2 [Figure 2: see original paper], the retrofit adds voltage/current sensors to monitor solar panels, locks the battery cabinet with a door switch sensor to detect unauthorized opening, routes wiring inside brackets to prevent external damage, and integrates anti-theft hardware (backup power modules for communication, accelerometers) inside metal brackets for protection.

Different components require tailored anti-theft designs based on their operational characteristics:

(1) **Solar panels:** Current flows only during daylight, enabling daytime fault detection via current monitoring. At night, current cannot indicate status. However, theft or destruction typically involves violent shaking, falling, or movement of mounting brackets, making accelerometers effective for detection.

(2) **Batteries:** Batteries charge from solar panels during the day while powering communication modules, then power both lamps and communication modules at night. Current changes occur continuously. However, if stolen or destroyed, the entire node fails, necessitating emergency backup power to maintain communication. Battery cabinets are typically locked, requiring door switch monitoring.

(3) **Insecticidal lamps:** Powered by batteries, lamps operate at night with

current flow but are inactive during the day. Accelerometers can detect theft or destruction through bracket movement.

Current GPRS-based anti-theft only detects entire-lamp theft and cannot monitor all components continuously. Therefore, adding diverse sensors is essential for comprehensive information collection and accurate theft/destruction assessment.

2.2 Feasibility Analysis of Retrofit Schemes

Beyond sensors, video acquisition devices could provide richer information. Table 3 compares GPRS modules, video acquisition modules, and various sensors across multiple dimensions for SIL-IoT applications.

Cost includes initial investment and ongoing expenses. GPRS and video modules are more expensive than other sensors and incur continuous data traffic fees, significantly increasing application costs. Both modules also have high continuous power consumption, burdening battery output. Except for video modules requiring additional brackets, other sensors can be integrated into circuit boards, making video modules more exposed and vulnerable to theft/destruction.

In conclusion, GPRS and video modules entail continuously increasing costs, and video modules are prone to theft/destruction. Integrating other sensor modules (voltage/current, accelerometer, door switch) offers lower cost without additional fees and ensures security. Therefore, this study selects voltage/current sensors, accelerometers, and door switch sensors.

2.3 Overall System Design

The anti-theft/anti-destruction system retrofit is illustrated in Figures 3 [Figure 3: see original paper] and 4 [Figure 4: see original paper]. The system uses an Arduino module (model ARMEGA328P) to receive signals from voltage/current modules, accelerometer, door switch, and power modules, interfacing with Raspberry Pi Zero and CC2538 communication modules:

(1) Four voltage/current modules monitor battery, solar panel, lamp tube, and metal mesh, returning digital signals to Arduino.

(2) The power module supplies all components; the backup power module provides emergency power if the main battery is cut off.

(3) The accelerometer module returns digital signals when SIL shaking occurs.

(4) The door switch module returns 0/1 signals.

(5) The CC2538 communication module receives Arduino signals and issues control commands.

(6) Raspberry Pi Zero receives Arduino data and issues control commands.

2.4 Functional Feasibility Verification

Sensor functionality must be verified before SIL installation. Tests confirm all four sensors operate normally:

(1) **Door switch:** System receives corresponding high/low level signals when opened/closed.

(2) **Voltage/current sensors:** Real-time voltage/current changes for different components (e.g., "12.01 V, 3.9 mA").

(3) **Backup power:** Wireless communication modules continue operating after battery disconnection, with duration depending on battery capacity without restart.

(4) **Accelerometer:** Captures signals when SIL shakes and uploads them to the system.

These modules provide data supporting SIL status assessment.

3 UAV-Based Anti-theft and Anti-destruction Auxiliary Equipment

While sensors provide richer information for theft/destruction detection, limitations remain: (1) insufficient detail for investigation and recovery after incidents; (2) lack of rapid node replacement measures, potentially causing network communication paralysis; (3) inability to perform insecticidal functions when nodes are destroyed. Therefore, auxiliary equipment is needed.

3.1 Target Requirements

After SIL retrofitting, the anti-theft system can collect richer information for more accurate theft/destruction detection. Users need: (1) risk reduction before incidents; (2) recovery of stolen components or entire lamps or valuable investigation clues after incidents; (3) rapid-response auxiliary equipment for emergency pest control due to the time-consuming and costly nature of SIL redeployment. UAVs, as highly mobile devices, effectively meet emergency needs.

UAVs are widely used in agriculture for soil monitoring [55,56], mapping [57,58], artificial pollination [58,59], crop phenotyping [60,61], precision agriculture [62-64], irrigation [65,66], pesticide spraying, pest monitoring and control [67-69], crop monitoring, and plant identification [70,71]. Safety applications include police UAVs [72] and power line inspection UAVs [73]. However, no research has applied UAVs for agricultural equipment anti-theft/anti-destruction.

Thus, UAVs can be adapted for the SIL-IoT scenario to enhance effectiveness. This study proposes the unmanned aerial vehicle insecticidal lamp (UAV-IL) for both pest control and anti-theft/anti-destruction support.

3.2.1 Structural Composition

The UAV-IL consists of a UAV with its power supply and an insecticidal lamp with its own power source (Figure 5 [Figure 5: see original paper]).

(1) **UAV:** A customized UAV (brand: datonhooya) [74] with 5.0 kg payload capacity, equipped with GPS, image transmission system, and 2.4 GHz wireless communication. The bottom bracket is customized for lamp installation. Based on findings that insecticidal discharge interferes with nearby wireless communication [75], the bracket maintains separation between UAV and lamp communication modules to avoid interference.

(2) **Insecticidal lamp:** The Shenbu solar insecticidal lamp [76,77] weighs 3.5 kg. Considering UAV payload, a small lithium battery powers the lamp, making UAV-IL operating duration differ from SIL.

The two systems have independent communication systems and power sources: UAV uses high-density lithium polymer battery (16,000 mAh), while the lamp uses standard lithium battery (12V, 8400 mAh). Communication protocols between UAV-IL and SIL-IoT nodes can be configured based on application requirements.

3.2.2 Flight Tests with Lamp and Simulated Insecticide Tests

Feasibility tests evaluated lamp-carrying flight capability and operating duration.

(1) **Lamp-carrying flight test:** A custom bracket secured the lamp to the UAV. Tests confirmed the UAV could carry the lamp (Figure 6 [Figure 6: see original paper]), though bracket design requires optimization for improved takeoff/landing stability.

(2) **Operating duration test:** The Shenbu lamp normally operates 5 hours nightly when fully powered. This test verified whether the lithium battery could sustain 5 hours of continuous discharge. Instead of field testing, a simulated discharge module [78] was used at 4 discharges/second. Discharge effectiveness was determined by detecting level jumps in nearby components, as high-voltage pulses cause level changes associated with actual insecticidal discharge. Monitoring these jumps during 5 hours of continuous operation confirmed the battery meets nightly requirements.

3.3 Comparison between UAV-IL and SIL

Table 4 compares UAV-IL and SIL across multiple dimensions. UAV-IL offers high mobility for rapid deployment but has shorter duration due to battery limitations. SIL provides longer operation via solar charging but is fixed and time-consuming to install. UAV-IL can temporarily replace stolen nodes and assist in tracking, while SIL provides stable, long-term pest control.

3.4 Potential Applications of UAV-IL

As SIL-IoT auxiliary equipment, UAV-IL has six potential applications:

(1) **Green pest control:** As a new agricultural device, UAV-IL can attract and kill migratory pests when deployed, reducing pesticide use.

(2) **Deployment testing:** UAV-IL enables rapid pre-deployment testing of multiple configuration schemes in SIL-IoT networks, reducing deployment workload and optimizing communication and pest control effectiveness compared to fixed SIL testing.

(3) **Emergency use:** For sudden pest outbreaks beyond SIL-IoT capacity or when conditions prevent pesticide spraying (e.g., high winds), UAV-IL can provide emergency pest control in critical areas, reducing pesticide application. If an entire SIL is stolen, UAV-IL can temporarily replace it to maintain pest control and communication functions while tracking the stolen device. For component theft, UAV-IL deployment depends on specific circumstances (e.g., solar panel theft at night requires no deployment).

(4) **Pest attraction:** In SIL-IoT networks, if one node faces high pest pressure while neighboring nodes have lower pressure, UAV-IL can fly at night without killing to gradually attract pests to lower-density areas for elimination, reducing regional pesticide use and preventing excessive energy consumption at high-pressure nodes. In areas without SIL deployment but with migratory pests, UAV-IL can attract pests to SIL-equipped regions.

(5) **Security warning:** If SIL or UAV-IL is stolen or destroyed, intelligent decisions from coordinated devices enable early warning and tracking. Periodic targeted patrols by UAV-IL can deter theft and enable traceability.

(6) **Network monitoring:** In pest monitoring, integrated radar networks (large-scale) and ground-based lamps, aerial lamps, and pheromone traps (small-scale) enable precise tracking of pest migration dynamics with real-time network publication [79]. With high mobility and integrated monitoring/control, UAV-IL can reduce manpower requirements, coordinate with ground lamps (intelligent SIL-IoT nodes, aerial lamps, pest monitoring lamps) to collect pest information, and support production and research.

4 Key Research Issues and Prospects

4.1 Key Research Issues

SIL-IoT node retrofitting and UAV-IL auxiliary equipment provide important hardware support for anti-theft/anti-destruction. However, sensor data alone is insufficient for rapid, accurate detection. For example, when door switch opens, accelerometer responds, and voltage/current sensors show normal readings, single-node data cannot definitively indicate theft versus component fail-

ure. Better anti-theft/anti-destruction functionality requires consideration of software, hardware, and structural design across six key issues:

(1) **Optimize device anti-theft/anti-destruction design:** Considering cost constraints, current SIL-IoT nodes only have basic sensors (door switch, accelerometer, backup power). Enhanced security could add GPS sensors (tracking), redundant safety designs, and voltage/current sensors at more critical locations. Structural improvements could include higher-security electrical cabinets and anti-theft mounting holes on solar panel support beams [80].

(2) **Establish judgment rules:** Current SIL anti-theft relies primarily on location changes. Multi-sensor, information-fusion-based solutions for SIL anti-theft/anti-destruction are lacking. Unlike industrial equipment, SILs feature wide deployment ranges, low density (2–4 hm^2/lamp), and difficult real-time maintenance. Their operating mechanisms must also be considered. Therefore, selecting appropriate sensors and establishing a multi-source information fusion rule base for theft/destruction detection is critical. Researching causal relationships between theft, destruction, and different faults is also essential.

(3) **Rapid and accurate theft/destruction detection:** Based on current SIL-IoT information, rapid and accurate detection remains challenging. Fault diagnosis techniques [75] can only identify possible scenarios, not definitive conclusions. Waiting for manual inspection or extended monitoring may enable accurate judgment but can cause significant losses (e.g., unrecoverable stolen equipment). Therefore, rapid and accurate detection is paramount.

(4) **Emergency response measures:** If critical nodes are stolen or destroyed and backup power cannot support full functions (discharge, pest monitoring), the entire SIL-IoT network fails. Nodes cannot operate lamps or monitor pests, preventing real-time pest assessment. Backup power may also be unable to monitor some components, leaving them vulnerable. Therefore, rapid emergency deployment is essential. SIL installation workload makes quick node replacement difficult, requiring UAV-IL for emergency deployment. Research on deploying limited UAV-ILs across multiple failed nodes to maintain basic pest monitoring and communication is crucial.

(5) **Theft/destruction prediction and prevention:** SIL-IoT nodes in remote locations face high theft/vandalism risks. Historical data analysis of theft patterns (components stolen, node location, post-theft movement direction, final location) can build predictive models. Combined with UAV-IL' s all-weather, automated, intelligent operation, this enables targeted patrols of high-risk nodes and rapid tracking after incidents, improving prevention.

(6) **Optimize computation to reduce network load:** First, theft/destruction

is rare, making daily monitoring data repetitive; real-time transmission increases network load. Second, SIL deployment in harsh environments can cause accelerometer false positives. Testing is needed to determine optimal communication frequency and improve detection accuracy.

4.2 Prospects

Anti-theft/anti-destruction design for SILs and UAV-IL auxiliary equipment can effectively reduce theft/vandalism risks, ensure node functionality, minimize economic losses, and promote technology adoption. Figure 7 [Figure 7: see original paper] illustrates future applications at network and node levels.

(1) **Network level:** After hardware retrofitting, SIL-IoT enables rapid and accurate detection of theft, destruction, and faults when SIL functions fail. Highly integrated UAV-IL and SIL systems support collaborative operation, providing a "safety net" for network nodes and ensuring operational security—encompassing both agricultural information security [81] and equipment safety.

(2) **Node level:** Network-level task allocation enables UAV-IL as backup nodes for emergency deployment and insecticidal operation. UAV-IL can also perform patrol and tracking tasks. As anti-theft/anti-destruction technology advances, UAV-IL nodes—whether ground-deployed or airborne—will receive appropriate protection, reducing theft/vandalism risks for all nodes.

Future agriculture will increasingly adopt IoT technology, showing trends toward unmanned, intelligent smart agriculture [82]. This requires deploying extensive agricultural equipment. The anti-theft/anti-destruction technology for SIL-IoT nodes can be extended to other agricultural IoT scenarios, safeguarding agricultural production equipment through software, hardware, and structural design.

References

[1] LI K, SHU L, HUANG K, et al. Research and prospect of solar insecticidal lamps Internet of Things[J]. Smart Agriculture, 2019, 1(3): 13-28.
[2] JIANG G. Physical insecticidal lamps successfully control pests—whose cheese is moved[EB/OL]. (2017-05-30) [2021-03-10]. http://blog.sciencenet.cn/blog-475-1057890.html.
[3] WANG X, WENG X. Application of frequency vibration insecticidal lamps in garden pest control[J]. Plant Protection, 2001(3): 47-48.
[4] LIU Z. Experiment on controlling pine caterpillar with frequency vibration insecticidal lamps[J]. Forestry of Shanxi, 2003(6): 32.
[5] LIU Z. Analysis on the effect of frequency vibration insecticidal lamp on controlling larch sheath moth[J]. Forestry of Shanxi, 2004(2): 29.
[6] DU J, WU J, WANG D. Occurrence status and control techniques of apple pests in Yichuan county[J]. Shaanxi Journal of Agricultural Sciences, 2010,

56(2): 229-231.
[7] LI G, LI W, MENG W. Trapping and killing corn borer with new insecticidal lamps[J]. Chinese Horticulture Abstracts, 2011, 27(4): 183-184.
[8] Dazhong Network. Insecticidal lamps frequently suffer "black hands" : Municipal authorities say theft and improper use are harmful[EB/OL]. (2011-06-30) [2021-03-10]. http://sd.dzwww.com/dongying/201106/t20110630_{6442237}.htm.
[9] Nanguo Metropolitan Daily. Sanya government freely installed thousands of insecticidal lamps—hundreds destroyed after two months[EB/OL]. (2011-12-26) [2021-03-10]. http://www.hinews.cn/news/system/2011/12/26/013866708.shtml.
[10] QI Y. Study on application effect of solar intelligent insecticidal lamps[J]. Modern Agricultural Science and Technology, 2012(2): 148.
[11] LIN W, REN H, LIU W. Experiment on controlling orchard pests with solar insecticidal lamps[J]. New Agriculture, 2012(15): 25.
[12] LIN X. Analysis of insecticidal lamps promotion in Guangzhou[J]. Guangdong Agricultural Sciences, 2013, 40(14): 103-104, 108.
[13] KONG D, SUN M, ZHAO Y, et al. Actively strive for public financial support and solidly promote green prevention and control of pests and diseases[J]. China Plant Protection, 2013, 33(3): 63-65.
[14] Rural Masses. 16,500 insecticidal lamps help 300,000 mu of peanuts bid farewell to pesticide history[EB/OL]. (2014-08-05) [2021-03-10]. http://paper.dzwww.com/ncdz/content/20140
[15] KONG D, SUN M, ZHU X, et al. Practice and effect of integration of specialized unified control of crop diseases and pests and green prevention and control in Zoucheng city[J]. China Plant Protection, 2015, 35(4): 85-87.
[16] WANG X. Analysis on the transformation from chemical control to physical control—application of solar insecticidal lamps[J]. Science & Technology Information, 2015, 13(33): 226-227.
[17] YUN T, ZHANG L. Trapping effect of solar energy pest-killing lamp on vegetable pests[J]. Northern Horticulture, 2016(18): 118-121.
[18] YAN S, KONG D, ZHAO Y, et al. Practice and thinking of full coverage green prevention and control of peanut diseases and pests[J]. China Plant Protection, 2018, 38(1): 73-77.
[19] ZHAO D, FAN J, LIANG X, et al. Application status, problems and strategies of solar insecticidal lamps in Wenshanzhou[J]. Agriculture and Technology, 2018, 38(12): 7.
[20] ZHANG Y, YU F. Preliminary study on trapping and killing effect of solar insecticidal lamps on corn pests[J]. Agriculture and Technology, 2018, 38(4): 36.
[21] WANG D. Insecticidal lamps must not be wasted in agricultural production[J]. Pesticide Market News, 2018(22): 56-57.
[22] JIANG B, ZHAO T, JIA S. Promotion and application of solar insecticidal lamps in agricultural production[J]. Farm Machinery, 2020(10): 85-88.
[23] WANG K, GAO Q, LI L, et al. Current development status of agricultural insect-pest light trap in China[J]. Insect Research in Central China, 2020, 16(00): 116-125.
[24] Jiangsu Provincial Public Security Department. Surveillance doesn' t mean "everything is safe" —cameras can also be stolen[EB/OL]. (2020-08-26)

[2021-02-03]. http://www.cn/Bqb/20000412/GB/4216%5ED0412B1401.htm.
[25] Henan Yunfei Technology Development Co., Ltd. Smart IoT insecticidal lamp[EB/OL]. [2021-02-03]. http://www.tynpzs.com/cpzx/tynpzs/273.html.
[26] Zhejiang Longhao Agricultural Technology Co., Ltd. IoT solar insecticidal lamp[EB/OL]. [2021-02-03]. http://www.dwdds.com/product/283.html.
[27] Shanghai Feixin Environmental Protection Technology Co., Ltd. IoT solar insecticidal lamp[EB/OL]. [2021-02-03]. http://www.xxscled.cn/product/20180228161404.html.
[28] Henan Sailan Instrument Equipment Manufacturing Co., Ltd. Smart IoT solar insecticidal lamp[EB/OL]. [2021-02-03]. http://www.slyqa.com/a/cp/fz/tynscd/473.html.
[29] Changzhou Jinhe New Energy Technology Co., Ltd. IoT insecticidal lamp[EB/OL]. [2021-02-03]. http://www.jinhexny.com/news/27.html.
[30] LENCWE M, CHOWDHURY S, OLWAL T. Detection of underground power cable theft: Strategies and methods[C]//2018 IEEE PES/IAS PowerAfrica. Piscataway, New York, USA: IEEE, 2018: 1-9.
[31] CHRISTOPHER A, SWAMINATHAN G, SUBRAMANIAN M, et al. Distribution line monitoring system for the detection of power theft using power line communication[C]//2014 IEEE Conference on Energy Conversion (CENCON). Piscataway, New York, USA: IEEE, 2014: 55-60.
[32] PATIL Y, SANKPAL S. EGSP: Enhanced grid sensor placement algorithm for energy theft detection in smart grids[C]//2019 IEEE 5th International Conference for Convergence in Technology (I2CT). Piscataway, New York, USA: IEEE, 2019: 1-5.
[33] GAO Y, FOGGO B, YU N. A physically inspired data-driven model for electricity theft detection with smart meter data[J]. IEEE Transactions on Industrial Informatics, 2019, 15(9): 5076-5088.
[34] ZHENG Z, YANG Y, NIU X, et al. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids[J]. IEEE Transactions on Industrial Informatics, 2018, 14(4): 1606-1615.
[35] ZHENG K, CHEN Q, WANG Y, et al. A novel combined data-driven approach for electricity theft detection[J]. IEEE Transactions on Industrial Informatics, 2019, 15(3): 1809-1819.
[36] SALINAS S, LI P. Privacy-preserving energy theft detection in microgrids: A state estimation approach[J]. IEEE Transactions on Power Systems, 2016, 31(2): 724-733.
[37] GAO Y, ZHOU C, SHANG D. A smart phone anti-theft solution based on locking card of mobile theft phone[C]//2011 International Conference on Computational and Information Sciences. Piscataway, New York, USA: IEEE, 2011: 971-974.
[38] CHANG S, LU T, SONG H. SmartDog: Real-time detection of smartphone theft[C]//2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Piscataway, New York, USA: IEEE, 2016: 223-228.
[39] HUSSAIN M, LU L, GAO S. An RFID based smartphone proximity absence alert system[J]. IEEE Transactions on Mobile Computing, 2017, 16(5): 1246-1257.

[40] YANG L, GUO Y, DING X, et al. Unlocking smartphone through hand-waving biometrics[J]. IEEE Transactions on Mobile Computing, 2015, 14(5): 1044-1055.
[41] REN Y, CHEN Y, CHUAH M, et al. User verification leveraging gait recognition for smartphone enabled mobile healthcare systems[J]. IEEE Transactions on Mobile Computing, 2015, 14(9): 1961-1974.
[42] AFMAN J, CIARLETTA L, FERON E, et al. Towards a new paradigm of UAV safety[EB/OL]. arXiv preprint arXiv:1803.09026, 2018.
[43] HU J, LI J, LI G. Automobile anti-theft system based on GSM and GPS module[C]//2012 Fifth International Conference on Intelligent Networks and Intelligent Systems. Piscataway, New York, USA: IEEE, 2012: 397-400.
[44] SREEDEVI A, NAIR B. Image processing based real time vehicle theft detection and prevention system[C]//2011 International Conference on Process Automation, Control and Computing. Piscataway, New York, USA: IEEE, 2011: 1-6.
[45] MOHANASUNDARAM S, KRISHNAN V, MADHUBALA V. Vehicle theft tracking, detecting and locking system using open cv[C]//2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). Piscataway, New York, USA: IEEE, 2019: 1075-1078.
[46] KWAK B, HAN M, KIM H. Driver identification based on wavelet transform using driving patterns[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2400-2410.
[47] ARTONO B, LESTARININGSIH T, YUDHA R, et al. Motorcycle security system using SMS warning and GPS tracking[J]. Journal of Robotics and Control (JRC), 2020, 1(5): 150-155.
[48] ZALA D. Bike security with theft prevention[C]//2018 3rd International Conference on Inventive Computation Technologies (ICICT). Piscataway, New York, USA: IEEE, 2018: 640-643.
[49] LIU Z, WANG M, QI S, et al. Study on the anti-theft technology of museum cultural relics based on internet of things[J]. IEEE Access, 2019, 7: 111387-111395.
[50] HAN Y, CHEN Z, GUO T. Design of equipment anti-theft tracker based on wireless sensor network[C]//2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS). Piscataway, New York, USA: IEEE, 2017: 1-5.
[51] DING W, HU H. On the safety of iot device physical interaction control[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS' 18). New York, NY, USA: ACM, 2018: 832-846.
[52] JIN W, XIANG X. Design of insecticidal lamp monitoring system based on zigbee and gprs technology[J]. Journal of Zhejiang University of Science and Technology, 2017, 29(6): 433-441.
[53] MA Q, TIAN M, TANG W. Research and design of distributed remote control system of solar insecticidal lamps based on WSN[J]. Internet of Things Technologies, 2017, 7(2): 77-79, 83.
[54] ZHU C. Research on intelligent management system of plant protection

insecticide lamp based on internet of things technology[D]. Hefei: Anhui University, 2019.
[55] POPESCU D, STOICAN F, STAMATESCU G, et al. A survey of collaborative UAV-WSN systems for efficient monitoring[J]. Sensors, 2019, 19(21): 1-40.
[56] AYAZ M, AMMAD-UDDIN M, SHARIF Z, et al. Internet-of-things (IOT)-based smart agriculture toward making the fields talk[J]. IEEE Access, 2019, 7: 129551-129583.
[57] Michael P A. International climate protection[M]. Cham: Springer International Publishing, 2019: 93-97.
[58] JEONGEUN K, SEUNGWON K, CHANYOUNG J, et al. Unmanned aerial vehicles in agriculture: A review of perspective of platform, control, and applications[J]. IEEE Access, 2019, 7: 105100-105115.
[59] MADDIKUNTA P K R, HAKAK S, ALAZAB M, et al. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges[J]. IEEE Sensors Journal, 2021: 1-12.
[60] BOURSIANIS A D, PAPADOPOULOU M S, DIAMANTOULAKIS P, et al. Internet of things (IOT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review[J]. Internet of Things, 2020. (in Press)
[61] SHEN B, FAN Y, YANG Y, et al. Research of multi-rotor aircraft application based on crop phenotyping acquisition[J]. Equipment Manufacturing Technology, 2019(8): 10-12, 29.
[62] ALZAHRANI B, OUBBATI O S, BARNAWI A, et al. UAV assistance paradigm: State-of-the-art in applications and challenges[J]. Journal of Network and Computer Applications, 2020, 166: 1-44.
[63] SONG Q, ZHENG F. Potential and methods of wireless communications for Internet of things based on UAV[J]. Chinese Journal on Internet of Things, 2019, 3(1): 82-89.
[64] JIA H, YANG L, ZHENG J. Advances of uav remote sensing applied in forest resources investigation[J]. Journal of Zhejiang Forestry Science and Technology, 2018, 38(4): 89-97.
[65] TANG P, TIAN J. Application and development of uav in future agricultural machinery[J]. China Southern Agricultural Machinery, 2020, 51(16): 53-54.
[66] YAN Z, YANG Z, WANG L, et al. Research status of markov theory in unmanned systems[J]. Chinese Journal of Ship Research, 2018, 13(6): 9-18.
[67] XIAO Q, WANG Z, GUO H. Application and development prospect of plant protection UAV in tea garden[J]. China Tea, 2019, 41(4): 16-18.
[68] HE D, DU X, QIAO Y, et al. A survey on cyber security of unmanned aerial vehicles[J]. Chinese Journal of Computers, 2019, 42(5): 1076-1094.
[69] HE Y, WU J, FANG H, et al. Research on deposition effect of droplets based on plant protection unmanned aerial vehicle: A review[J]. Journal of Zhejiang University(Agriculture and Life Sciences), 2018, 44(4): 392-398.
[70] CHEN P. Applications and trends of unmanned aerial vehicle in agriculture[J]. Journal of Zhejiang University (Agriculture and Life Sciences), 2018,

44(4): 399-406.
[71] FU T, DENG Y, HAN Z. Application of uav in modern agricultural production[J]. Science and Technology of Tianjin Agriculture and Forestry, 2017(4): 14-15.
[72] SHANG Y, LIU R, WEN W. Practical application and existing problem analysis of police unmanned aerial vehicle[J]. Wireless Internet Technology, 2020, 17(10): 15-17, 29.
[73] SUI Y, NING P, NIU P, et al. Review on mounted uav for transmission line inspection[J]. Power System Technology, 1-15.
[74] Datonhooya. Heavy payload UAV[EB/OL]. [2021-02-03]. https://item.taobao.com/item.htm?id=61603535
[75] YANG X, SHU L, HUANG K, et al. Characteristics analysis and challenges for fault diagnosis in solar insecticidal lamps Internet of Things[J]. Smart Agriculture, 2020, 2(2): 11-27.
[76] SHUANG K, LI K, SHU L, et al. High voltage discharge exhibits severe effect on zigbee-based device in solar insecticidal lamps Internet of Things[J]. IEEE Wireless Communications, 2020, 27(6): 140-145.
[77] Shenbu. Solar insecticidal lamp[EB/OL]. [2021-02-03]. https://item.taobao.com/item.htm?id=5632774940
[78] HUANG K, LI K, SHU L, et al. Demo abstract: High voltage discharge exhibits severe effect on zigbee-based device in solar insecticidal lamps Internet of Things[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway, New York, USA: IEEE, 2020: 1266-1267.
[79] People' s Daily Overseas Edition. Insect radar helps "snatch grain from insects'mouths"[EB/OL]. (2020-08-17) [2021-02-03]. http://paper.people.cn/rmrbhwb/html/2020-08/17/content_{2003608}.htm.
[80] XING L, FAN F, CHEN Q, et al. Anti-theft positioning structure of solar panel: China, CN201927618U[P]. 2011-08-10.
[81] YANG X, SHU L, CHEN J, et al. A Survey on smart agriculture development modes, technologies, and security and privacy challenges[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(2): 273-302.
[82] FRIHA O, FERRAG M A, SHU L, et al. Internet of things for the future of smart agriculture: Comprehensive survey of emerging technologies[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(4): 718-752.

(Visit www.smartag.net.cn for free full-text electronic version)

Note: Figure translations are in progress. See original paper for figures.