JOURNAL OF ADVANCED INDUSTRIAL TECHNOLOGY AND APPLICATION
e-ISSN: 2716-7097

JAITA

Vol. 5 No. 2 (2024) 41-55
https://publisher.uthm.edu.my/ojs/index.php/jaita

Enhanced Wireless Control of Anti-Theft Solar Photovoltaic Modules Using Tree Topology

FCM Choong[1]*, K. Jia Jun[1]

[1] *Heriot-Watt University Malaysia, School of Engineering and Physical Sciences 1, Jalan Venna P5/2, Precint 5, Putrajaya, 62200, MALAYSIA*

*Corresponding Author: f.choong@hw.ac.uk
DOI: https://doi.org/10.30880/jaita.2024.05.02.004

Article Info

Received: 1 September 2024
Accepted: 22 November 2024
Available online: 8 December 2024

Keywords

Wireless, photovoltaic, anti-theft, solar farm, encryption system

Abstract

The increase in the market value of photovoltaic modules resulted in a growing number of solar panel thefts, causing tremendous losses to the owner of the solar farm. As a result, huge investments are needed to secure these solar panels. The current solution of using CCTV cameras and sensors requires high computational power, is expensive, and requires personnel to monitor it. This paper proposes an energy-efficient and cost-effective wireless encryption anti-theft solar photovoltaic system utilizing a radio frequency transceiver and a tree topology. The tree topology overcomes the limitation of a radio frequency transceiver by allowing a higher number of transmissions to be done simultaneously. A gyroscope module is used to detect theft by reading the rotational speed of the solar panel. Using the tree topology, the child node can transmit an error signal to the master node before calling the owner. The master node of the solar farm is responsible for transmitting a password to every child node to decrypt the circuit. If one of the solar panels is stolen, the circuit of the stolen panel will be encrypted if the password is not received within three minutes. A lithium-ion battery and a battery charger module are installed for energy storage to allow the system to operate in the absence of sunlight. The proposed system yielded a 39.3% reduction in power consumption and is a promising method for large-scale implementation in solar farms.

1. Introduction

Implementation of closed-circuit television (CCTV) cameras as a security system for solar farms is a common approach to prohibiting the activity of solar panel theft. However, such an approach consumes a lot of energy and has a high cost. Hence, several studies have looked to replace the anti-theft system using CCTV cameras. Though some of the research managed to secure the solar panel with great energy efficiency, their anti-theft system was not able to encrypt the solar panel. Other methods were too expensive and were not able to integrate well with the solar tracking system.

One way of detecting theft in a solar farm would be to measure the sudden drop in voltage in the system. For example, Viscontini and Paolo (2015) used a module to evaluate the overall string voltages of the system and looked for a critical drop in the voltage [1]. Another approach measured the electrical pulses generated by the photovoltaic module and an alarm is triggered if changes in the electrical pulses are detected [2]. However, the above approaches do not enhance the security of the solar panels, whereby stolen panels can still be sold to contractors before being sold back to customers again. One solution would be to use a relay or metal-oxide-semiconductor field-effect-transistor (MOSFET) together with a microcontroller to encrypt the circuit. For instance, Tan (2017) used a magnetometer to measure the orientation of the solar panel, and the circuit is

encrypted using a MOSFET when the change in orientation is detected [3]. The encrypted circuit will be decrypted via Zigbee [4], a wireless technology that is widely used in smart home systems [5]. However, the use of Zigbee modules in the solar panels will increase the manufacturing cost.

Several attempts have been made to implement a solar encryption system into the anti-theft solar system. Thiemann [2] and Viscontini and Paolo [1] have provided an inexpensive yet less power-hungry solution against theft by measuring the voltage and the impedance of the whole circuit. However, both solutions could not be implemented together with the solar module encryption system. The solar module and the theft detection system could not identify the identity of the user. Several anti-theft systems incorporating an encryption system into the theft detection system have been proposed [3, 6, 7, 8]. Goldack [6] has introduced an excellent and creative approach to the solar module encryption system in which the shapes and lengths of the electrical pulses were used as a key to decrypt the solar panel while encrypting the solar panel if none of the received pulses were the same as the key pulses. However, the alarm used to alert the owner can be sabotaged beforehand, making the theft unnoticeable. In other related work, Khan [8] and Tan [3] use the value read in a three-axis magnetometer as an indication to encrypt the solar panel. The decryption of the stolen solar module is achieved by a wireless controller, in that Tan [3] uses a Zigbee module as the wireless module to send encrypted commands to the encrypted solar module. The cons of this system would be the price of the Zigbee module, which might be quite expensive to implement into a security system, though it consumes very little energy during its operational state. Recent work has utilized Internet of Things (IoT) in the monitoring system [9, 10], supervised learning [11], and sensors integrated with a microcontroller [12] for monitoring systems and theft detection. However, more work must be done to find a cost-effective and energy-efficient integrated solution for theft monitoring and detection applied to large-scale solar farms [13].

The existence of a wireless solar module encryption system is crucial, and this work contributes by establishing an energy-efficient theft detection system that does not consume a high amount of energy and an inexpensive wireless communication system [14] for the encryption of solar panels in large-scale solar farms. A low-cost wireless encryption system using a radio frequency (RF) module is proposed to replace the Zigbee module. The RF module is programmed to mimic the characteristics of the mesh network possessed by the Zigbee module. The theft detection method comprises a wireless encryption system and a solar tracking system. A gyroscope module is used to detect tilting speeds that are outside the acceptable range. In addition, the decryption command of the transmitter is hidden in one of the solar modules to prevent the possibility of the alarm being sabotaged by theft.

2. Methodology

2.1 Overall Architecture

The high-level architecture of the overall system is shown in Fig. 1. The anti-theft system comprises four subsystems: a theft detection system, a wireless encryption system, a notification system, and a power supply system. The solar panel will extract solar energy from the sun and convert it into electricity to be injected into the power grid. The electricity will be transferred to the power supply system before powering up the anti-theft system. The electricity flowing into the power supply system will be used to charge the lithium-ion battery as well as supply it to the microcontroller to enable the overall system's operation. When the solar panel is unable to harvest energy from the sunlight during periods when sunlight is absent, the electricity stored in the power supply system will be able to supply electricity to the microcontroller. The microcontroller behaves as the brain of the theft detection system, solar encryption system, and notification system, in which the value obtained in the theft detection system will be processed by the microcontroller before sending any command to the encryption system or notification system to encrypt the circuit or notify the owner accordingly.

The wireless encryption system will be encrypting and decrypting the solar panel once any of the panel is stolen. One approach to detecting whether the solar panel is still within the area of the solar farm is by employing the master-slave topology or Global Positioning System (GPS) module in the solar panel. However, although the master-slave topology has its advantages in securing the solar panel on the roof, this solution has limitations on the number of solar panels to secure. This renders the system to be less feasible to apply to a large-scale solar farm. The latter approach, which involves inserting the GPS module into each solar panel to read the current location, might be a good idea to check if the panel is still in the solar farm. Nonetheless, considering the cost of installing all the solar panels in a large-scale solar farm, such an approach is not feasible. Hence, this paper presents an alternative approach to transmitting the password to the solar panel through a radio frequency transceiver to allow the output power to flow from the solar panel. For this approach to be implemented in a large-scale solar farm, the idea of tree topology must be implemented.

J. of Advanced Industrial Technology and Application Vol. 5 No. 2 (2024) p. 41-55

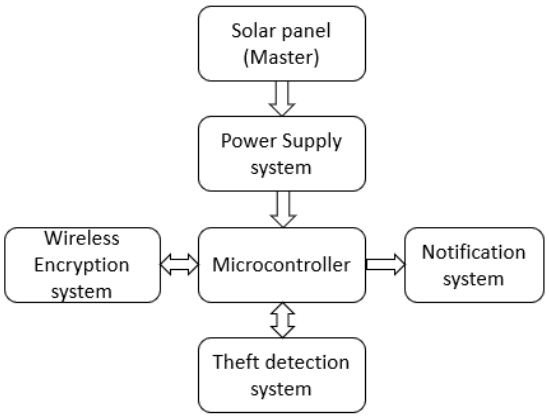


Fig. 1 *High-level architecture of the anti-theft system*

The overview of the tree topology implemented in the anti-theft system is shown in Fig. 2. The solar panel in level 0, being the master node, will transmit the password to each of the child nodes located in level 1. The nodes in level 1 will transmit the password to each of the child nodes located in a level below them, and the process will continue until all the child nodes have received the password from their parent node. The password received from their parents will act as a key to allow the child nodes to release the electricity harvested from the solar panel for three minutes. The circuit for the output power is connected to a normally open relay, where the circuit will be switched off if the password is not received within three minutes. This is usually the case when the panel has been successfully stolen, and the range is too far to receive the password from the master node.

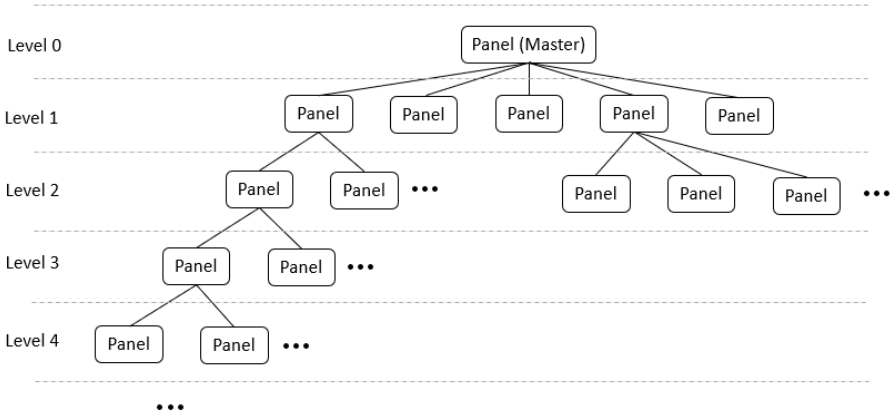


Fig. 2 *Tree topology of anti-theft system*

Hence, to safeguard the solar panel from theft, a theft detection system is implemented using a gyroscope module. In the event of detecting unauthorized use of the solar panel by one of the child nodes, an error signal will be transmitted from the child node to the master node through several parent nodes, which is like the transmission of a password but in the opposite direction. Once the master mode receives an error signal from the child nodes, the notification system will notify the owner via phone call.

2.2 Theft Detection System

A gyroscope can measure the angular velocity of an object and is used in the design of the theft detection system, in which a huge change in rotational velocity of a solar panel is considered as an unauthorized use of a solar panel and an error signal will be sent to the master node to notify the owner. The gyroscope module uses I^2C interface as the communication protocol between the module and the microcontroller, which is a two-wire interface comprised of signal serial data (SDA) and serial clock (SCL). It is also worth noting that the solar panel implemented with solar tracking system rotates in a very small angular velocity. Hence, a threshold angular velocity of a solar panel can be defined whereby any angular velocity larger than the threshold value will trigger the theft detection system to send an error signal to the master node. The theft detection system reads the rotational speed of the solar panel with the aid of a gyroscope module. The values read by the gyroscope are processed before printing them on the serial monitor for testing and verification. The values will then be compared

with the threshold value to ensure that the solar panel is in an idle condition where no external force is acting on it. When the gyroscope module in a solar panel reads a rotational speed greater than 10°/s, possibly due to a theft activity, an unusual rotational speed will be detected, and the error signal will be transmitted to the head of the network in the solar farm. Thus, taking advantage of the tree topology shown in Fig. 2, a global system for mobile communication (GSM) module is required to be installed only in the master node. If any of the child nodes need to inform the owner of the unusual rotational speed of the solar panel, they will need to transmit an error signal to the master node so that the master node will inform the owner on behalf of the child nodes. Like how the master node transmits passwords to the child nodes, the child nodes will transmit the error to the parent node, and the parent nodes will transmit the error to the master node through their respective parent nodes. Such an approach is cost-effective, as only one GSM module is required.

2.3 Wireless Encryption System

The wireless encryption system employs a relay to encrypt the circuit of the solar panel if any unauthorized use of the panel is detected. To detect unauthorized use of a solar panel, a wireless communication device, an RF transceiver, is installed inside the solar panel to check the location and determine if the panel is in the original position. Thus, a password will be sent to the solar panel through an RF transceiver and act as a key to decrypt the solar panel to allow the injection of output power to the grid. The solar panel responsible for sending the password to other solar panels serves as the master node, while the rest of the solar panels will act as the child nodes. In the case of a stolen solar panel, the panel will not be able to receive the password from the master node since it is too far away to receive the signal from the master node. As no password is received from the master node, the stolen panel will encrypt the circuit of the panel through the relay.

The RF transceiver is a single-chip radio transceiver operating at 2.4 GHz with a maximum baud rate of 2000 kb/s. This module can transmit data over a range of 100 meters and 10 meters in open space and indoors, respectively. However, despite having a wide transmission range, the transceiver can only communicate with up to five modules at the same time, which is not feasible for a large-scale solar farm with a huge number of solar panels. Hence, the idea of tree topology is introduced into the wireless encryption system to mimic the feature of a mesh network possessed by the Zigbee module. With the implementation of tree topology, the password from the master node will be able to be transmitted to all the child nodes. The master node is located at level 0, and the five child nodes of the master node are located at level 1. Each of the child nodes in level 1 has their own child node as well, which will be located at level 2. With the idea of tree topology implemented, the master node will first transmit the password to all the child nodes in level 1. The password received by the child nodes in level 1 will decrypt the circuit, and then the password will be passed down to their own child nodes in level 2. The process is repeated until every solar panel has received the password from their parent nodes.

The theft detection system in each solar panel will detect unusual rotational speeds using a gyroscope module. The medium through which the parent nodes communicate with their child nodes is known as a channel. There are two types of channels used in this wireless encryption system: one for the transmission of the password and another for the transmission of the error. Each channel is made up of a maximum of five-letter string addresses. The transmitting addresses for password and error are shown in Fig. 3 and Fig. 4, respectively. For the sake of simplicity, the address of each channel will be based on the location of the parent nodes. It should be noted that if a parent node is to transmit passwords to the child nodes, the receiving addresses of the child nodes must be identical to the transmitting addresses of the parent node. Conversely, if any of the child nodes needs to transmit an error to their parent node, the receiving address of the parent node must be the same as the transmitting address of the child node.

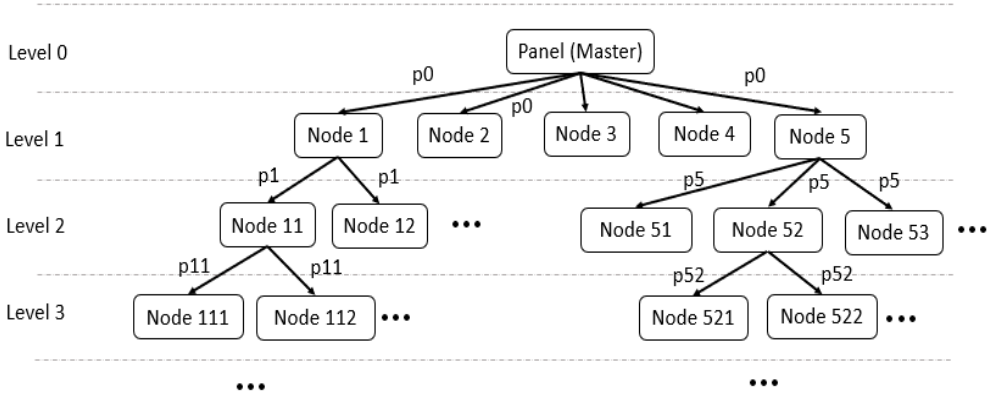


Fig. 3 *Transmitting address for password*

The numbering of each node is based on the level, parent, and index of the location. Based on Fig. 3, node 112 is the second child of node 11, hence it is numbered as 112. Node 53 is the third child of node 5; it is therefore numbered as 53. In short, the least significant bit indicates the position of the child, whereas the numbers next to it indicate the location of the parent node. Like the numbering of each node, the transmitting address of a channel is based on the data type and the numbering of the parent node. The leftmost letter suggests the data type, where letter '*p*' indicates password and letter '*e*' indicates error. The numbers next to the data type are the location of the parent node in a channel. The task of the master node is to transmit the password to the child nodes while standing by to receive errors from the child nodes. The task of all the child nodes would be trying to receive the password from their parents and errors from their own child nodes.

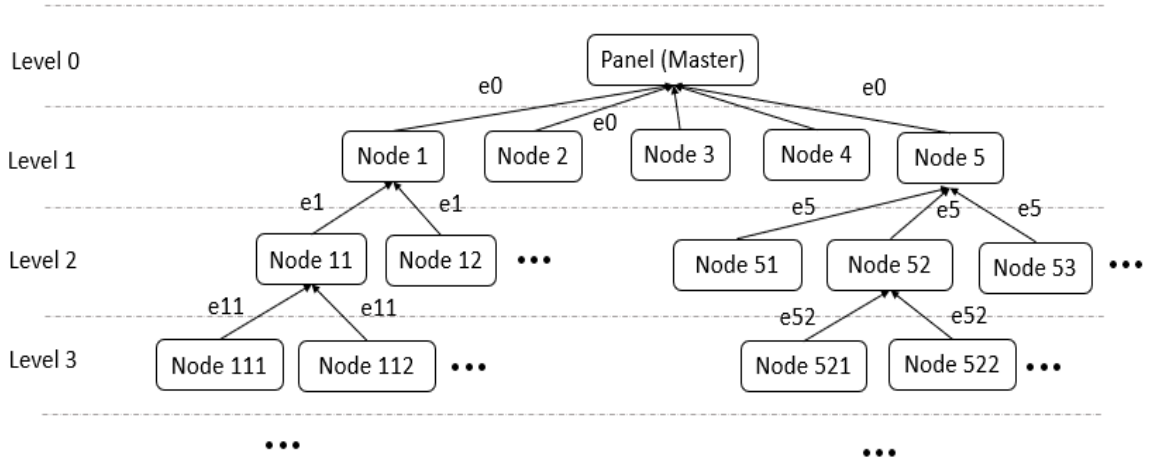


Fig. 4 *Transmitting address for error*

The block diagrams of the master node and child nodes are shown in Fig. 5 and Fig. 6, respectively. The master node is set to transmit the password every two minutes while waiting for incoming error signals from the child node. If an error is received or the gyroscope reads an unusual rotation, the master node will inform the owner by making a missed call. The child nodes, on the other hand, will check if the password is received within three minutes; otherwise, output power will be cut off through a relay. If the password is received by the child node, the counter will be reset, and the password will be passed down to their own child node. These child nodes will transmit errors to their parent nodes if an error is received by their own child nodes or the gyroscope in the panel reads unusual rotation, which in this case is greater than 10°/s.

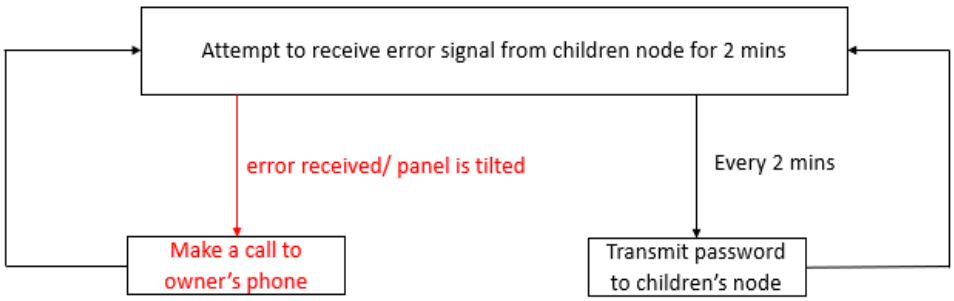


Fig. 5 *Block diagram of master node*

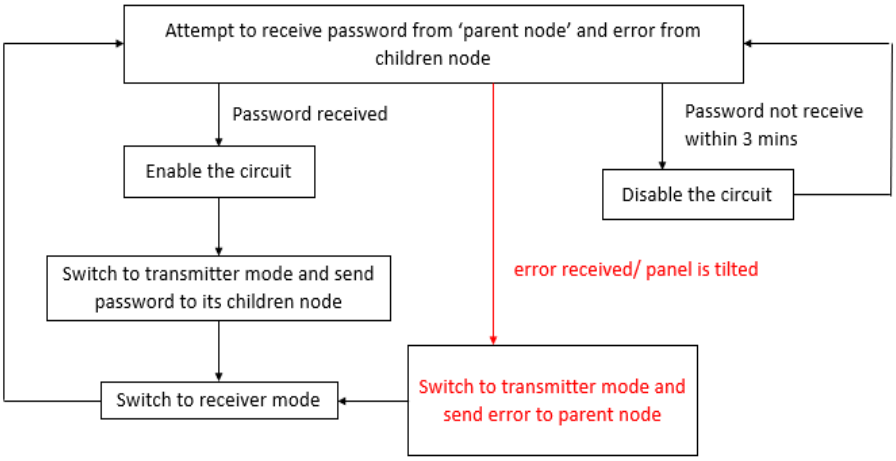


Fig. 6 *Block diagram of child nodes*

2.4 Notification System

The notification system is responsible for informing the owner when the master node of a solar farm has received an error signal from the child nodes. This is implemented using SIM900A module which allows short messaging services (SMS) or calls to the owner. The notification system is only implemented in the master node of the network to reduce the cost of the system. A 20-second call will be made to the owner if an error signal is received from any of the child nodes.

2.5 Power Supply System

The goal of having a power supply system is to ensure that the system operates in any weather conditions, especially in cloudy or rainy conditions and at night. The power supply system must be able to store adequate energy so that it is capable of supplying electricity for the overall system in the absence of sunlight. A rechargeable battery and battery charger are therefore the main components of this subsystem. The chosen capacity of the lithium-ion battery is 2000 mAh at 3.7 volts. The microcontroller that is implemented in this anti-theft system is the Arduino Nano, a microcontroller that requires at least 5V to operate. Hence, two 3.7V lithium-ion batteries will be employed together to provide an output voltage of 7.4V to the microcontroller. The lithium-ion battery charger that is used can charge the battery at a maximum current of 1A with a voltage of 5V. The circuit connection shown in Fig. 7 will allow the lithium-ion battery to be charged by the electricity generated from the solar panel while powering up the microcontroller. Such a configuration also enables the battery to supply electricity to the microcontroller if no electricity is generated by the solar panel in the absence of sunlight.

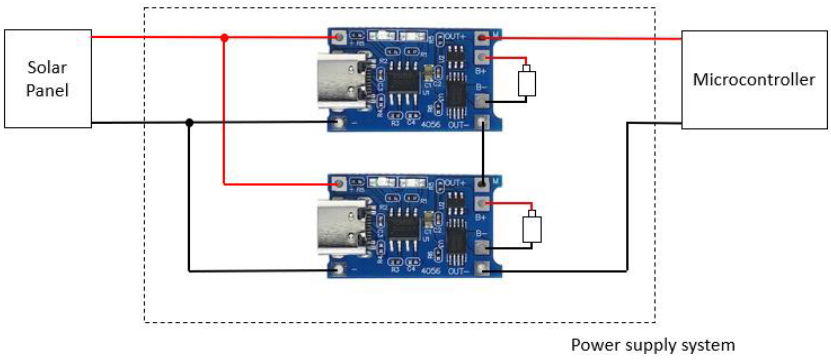


Fig. 7 *Circuit connection of power supply system*

2.6 Overall System

A simplified wire connection of the solar panel with the anti-theft system is shown in Fig. 8. It should be noted that the wire connection of the solar panel with the anti-theft system is the same for both the master node and the child nodes. The solar panel does not supply electricity directly to the microcontroller. Instead, the electricity

generated by the solar panel will be supplied to the power supply system before powering up the microcontroller. The power supply system will always store electricity in the lithium-ion battery to supply electricity to the microcontroller in the absence of sunlight. The output power of the solar panel is connected to the grid through a normally open relay. The relay is controlled by the wireless encryption system.

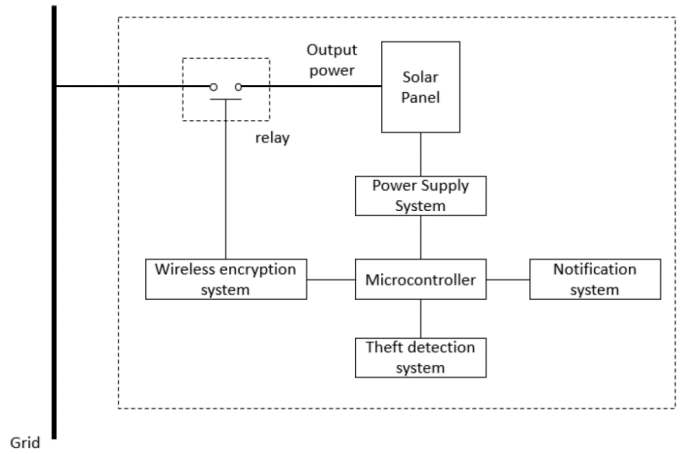
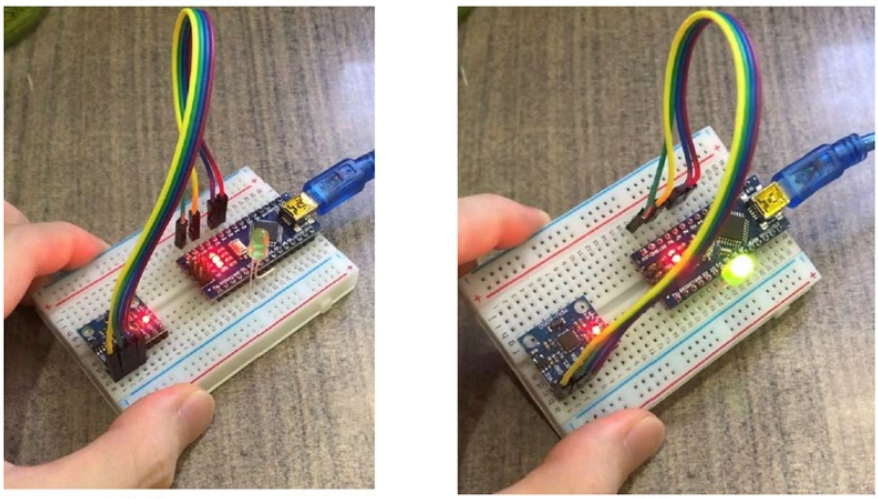


Fig. 8 *Simplified wire connection of solar panel with anti-theft system*

3. Results and Discussion

This section will discuss the results of the proposed system. The theft detection system, wireless encryption system, power supply system, and notification system were integrated together to implement a wireless solar panel anti-theft system.

For the theft detection system, the motion of tilting the gyroscope module is shown in Fig. 9(a) and Fig. 9(b), in which Fig. 9(a) shows the gyroscope module before tilting, and Fig. 9(b) shows the gyroscope module after tilting. It should be noted that the initial and final motion is captured, and a motion of 80°/s was experienced by the gyroscope module. The angular velocity when the gyroscope module is in tilting motion is recorded as shown in Fig. 10. As can be seen in Fig. 9(b), the LED has been lighted up, indicating that the angular velocity of gyroscope module has exceeded the threshold value, and hence an error signal is transmitted to the master node. Therefore, the theft detection system successfully detected the action of theft through readings recorded by the gyroscope. After the action of theft is detected, the circuit of the solar panel will not be encrypted. Instead, an error signal will be transmitted to the parent nodes and the master node.



(a) (b)

Fig. 9 *(a) Gyroscope module before tilting; (b) Gyroscope module after tilting*

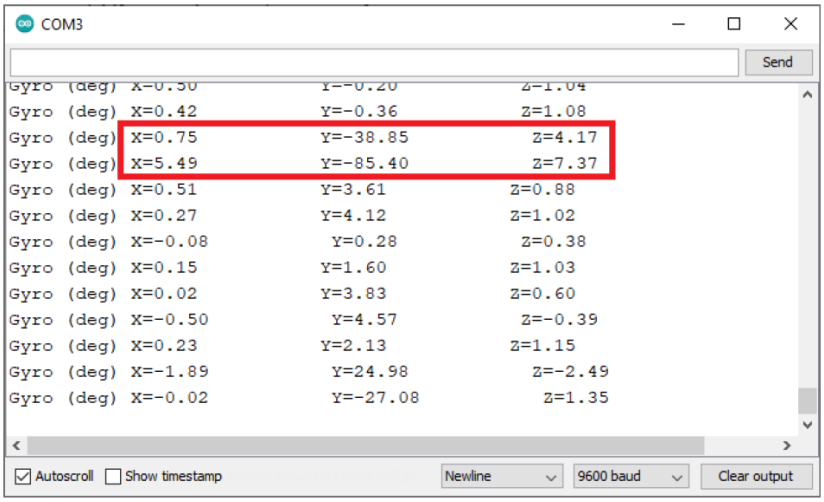


Fig. 10 *Angular velocity of gyroscope module in the motion of tilting*

The wireless encryption system can successfully encrypt and decrypt the solar panel while transmitting password and error between the parent node and child nodes. To illustrate the sending of password from the master node, a child node of master node 0 is placed next to it as shown in Fig. 11. With reference to Fig. 11, the module on the left is the master node, whereas the module on the right is the child node. As illustrated in Fig. 11, the green LED connected to child node is lighted up, which indicates that the password is transmitted from master node to child node. When the master node is disconnected from the power supply, the green LED of the child node turns off after three minutes as shown in Fig. 12. The green LED is used as an indication of the output power of a solar panel, and the child node shown in Fig. 11 is encrypted.

Fig. 11 *Master node when password is transmitted*

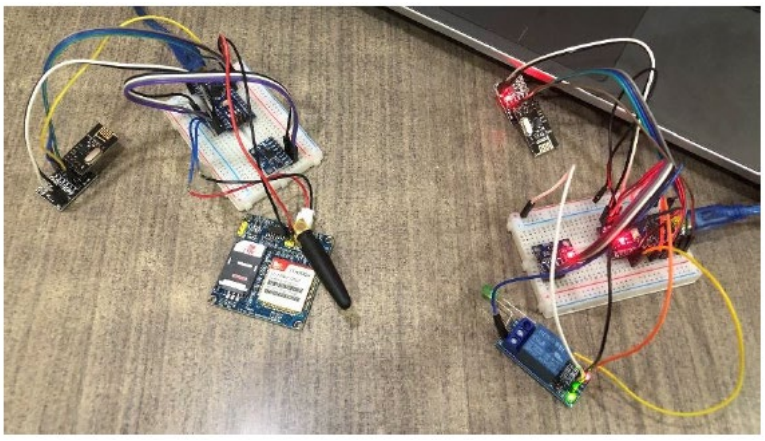


Fig. 12 *Master node when it is disconnected from power supply*

An error signal will be transmitted to the master node when any of the child node is tilted. The master node will make a call to the owner if an error is received from the child node. Fig. 13 shows the readings recorded on a serial monitor when an error is received. The error '999' was received when the counter is at n = 1149. Right after the error is received, the call function is made and the line 'calling' is printed on the serial monitor.

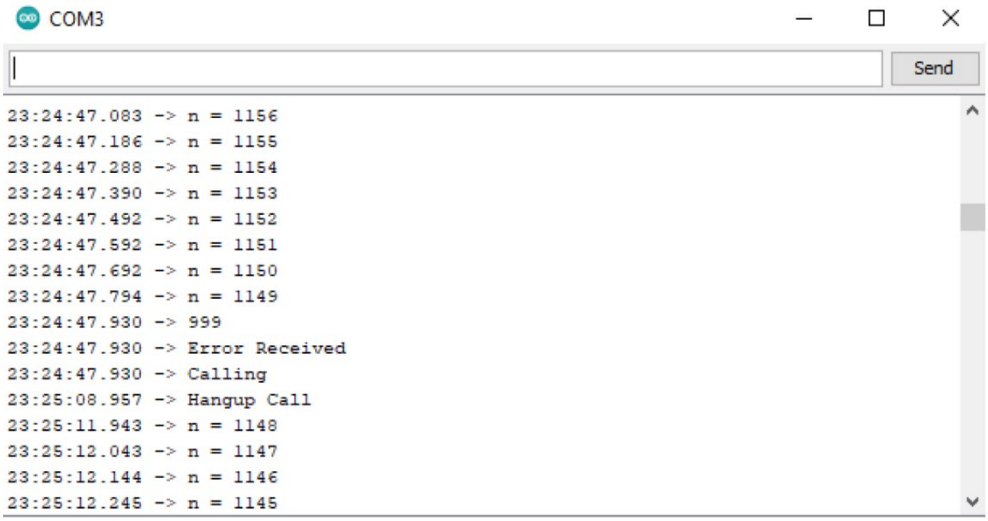


Fig. 13 *Serial monitor when error is received*

To illustrate the workings of the child nodes, Fig. 14 shows the serial monitor when node 1 receive a password. When data '1234' is received from the parent node, the counter *n* is reset to three minutes, which is shown as *n*=1800. Once the password is received, node 1 will transmit the password to the child nodes, indicated by the 'sending password' on the serial monitor. The transmission of data between solar panels have been achieved using the Arduino nRF24L01 module. The success of transmitting data wirelessly has made the encryption of solar panel possible through the relay. The generation of error signals due to tilting of solar panels is transmitted to the master node for further action.

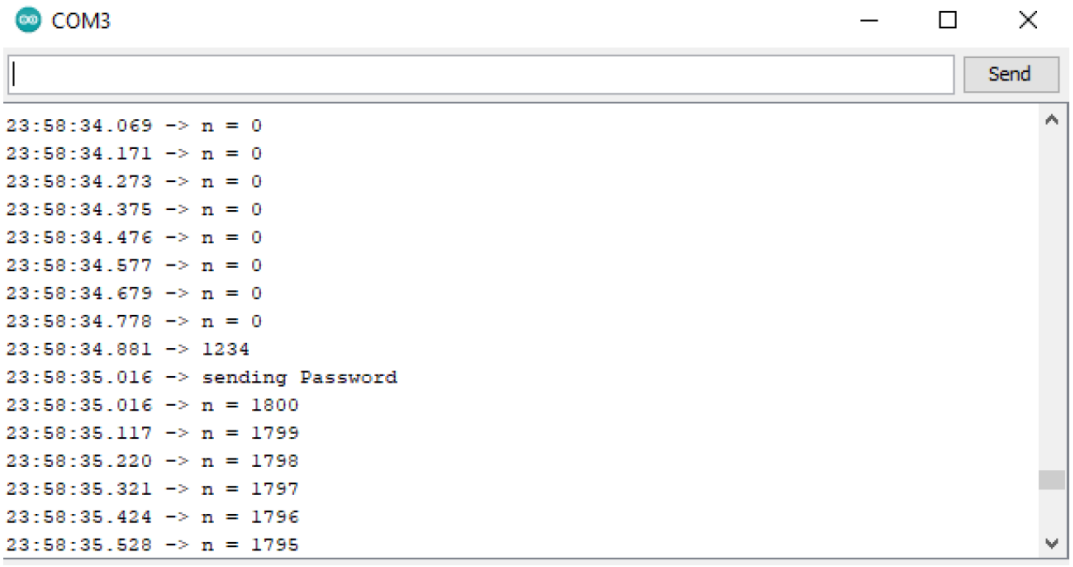


Fig. 14 *Serial monitor when child nodes receive a password*

To demonstrate the workings of the wireless solar panel anti-theft system, one master node and three child nodes were selected. Fig. 15 shows the anti-theft system prior to transmitting a password. The name of each node is labelled next to the module, and the network between each node is drawn. Nodes 11 and 12 are the child nodes of node 1, and node 1 is the child node of the master node. The green LED connected to the relay is dimmed, which indicates that the circuit is encrypted, and the password has not been received.

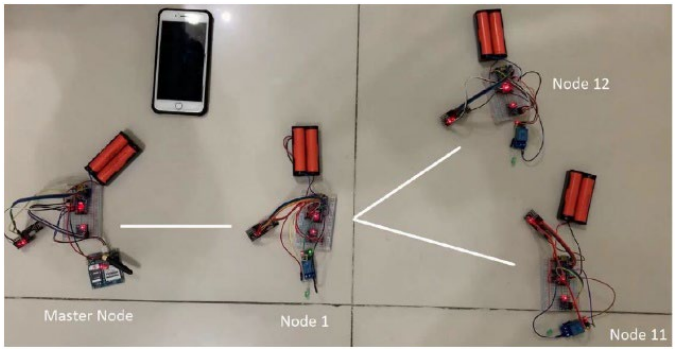


Fig. 15 *Anti-theft system before password is transmitted*

Fig. 16 shows that when a password is transmitted from the master node, the green LED of the child node is lit up to indicate that the password is received, and the circuit is decrypted. Though the transmission of the password cannot be observed, node 1 will be the first node to receive the password from the master node. The password received at node 1 will be further transmitted to the child nodes, which in this case are nodes 11 and 12. In the case where nodes 11 and 12 have their own child nodes, the password received will also be transmitted to the child nodes one level below them until every node has received the password to allow the output of generated power. This result suggests that the implementation of tree topology in an anti-theft system allows the child nodes to be monitored, even though the RF transceiver is only capable of communicating with a maximum of five nodes at the same time. With the idea of a tree topology with an RF transceiver, an infinite number of solar panels can be monitored and decrypted.

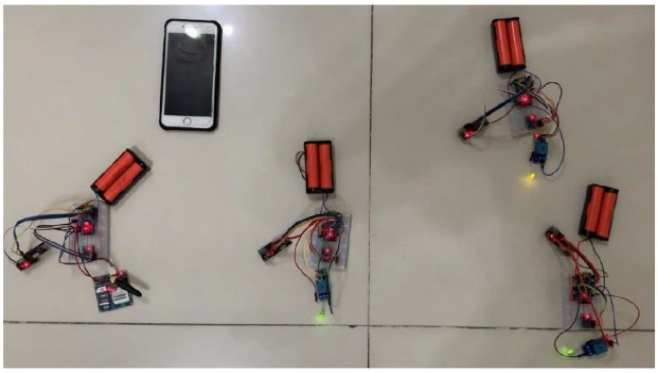


Fig. 16 *Anti-theft system after password is transmitted*

Fig. 17 shows the anti-theft system when the theft detection system of a child node is triggered. Node 12 is tilted gently to imitate the action of a thief who is attempting to remove the solar panel from its original position. Once the gyroscope module in node 12 reads an abnormal rotational speed, the microcontroller in node 12 will transmit an error signal to the parent node (node 1) through the RF transceiver. When node 1 receives an error signal instead of a password, the node will transmit this error to the master node. The master node, being the head of the network, will call the owner through the notification system, as shown in Fig. 18. This indicates that the gyroscope can read the rotational speed of the solar panel to detect if there is any theft activity.

To illustrate the encryption process of the solar panel, the master node is first disconnected from the power supply after the password is transmitted to the child nodes. Right after the password is sent, the counter on the phone starts to measure the duration taken for the child node to encrypt the circuit. Fig. 19 shows the moment when the password is transmitted, and the counter is started. After three minutes of not receiving any password from the master node, all child nodes are encrypted, as shown in Fig. 20, where the green LED is no longer lit up. This scenario shows that a solar panel is successfully stolen from the solar farm, and the solar panels do not receive any password from the master node to allow the output power flow of the solar panel. As a result, these encrypted solar panels must be returned to their owner for decryption of the circuit, which in turn prevents the panel from flowing into the black market for resale since the encrypted solar panel will be treated as a ruined panel.

J. of Advanced Industrial Technology and Application Vol. 5 No. 2 (2024) p. 41-55

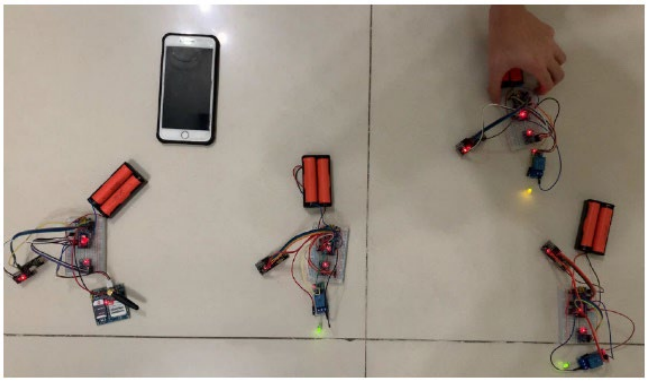


Fig. 17 *Anti-theft system when theft detection system is triggered*

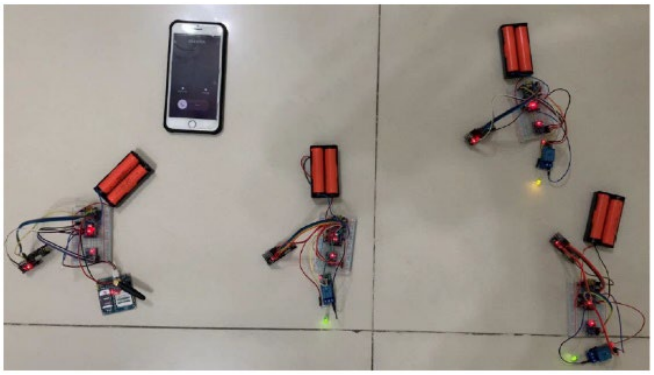


Fig. 18 *A phone call is received from Master node*

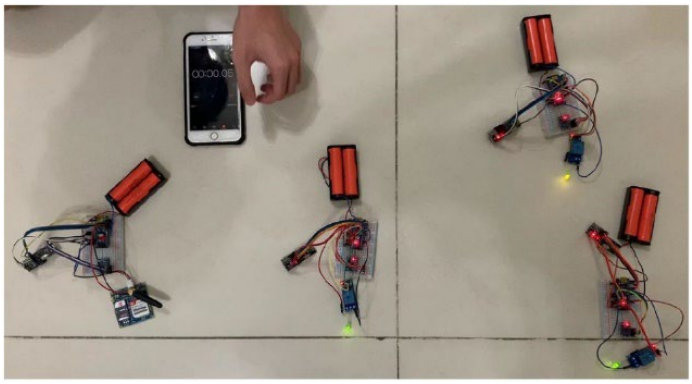


Fig. 19 *Counter when password is transmitted from master node*

The role of the notification system is to give a call to the owner to inform them of the action of theft, and this task is accomplished using the SIM900A module with an activated SIM card. The *MakeCall()* function will be called when an error is received from the children node. Fig. 21 demonstrates that a phone call is successfully made after tilting one of the nodes. As the number of the SIM card is saved as SIM900A, the phone has received a call from SIM900A. The phone call will end after 20 seconds. The SIM900A module is also able to send SMS messages to the owner.

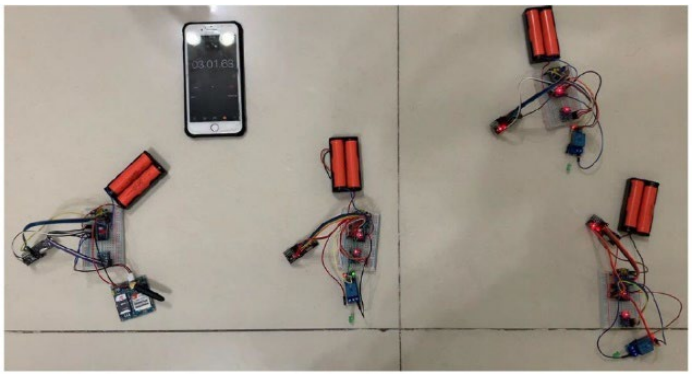


Fig. 20 *Counter when child nodes are encrypted*

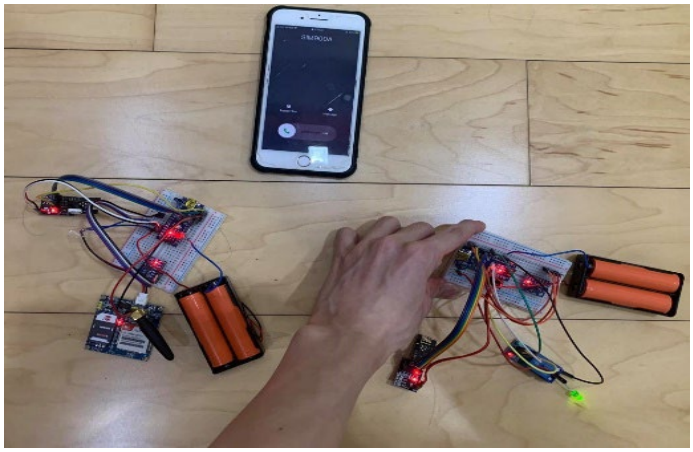


Fig. 21 *Call triggered when error signal is received from child node*

The power supply system is made to enable all subsystems to work, and in the absence of sunlight, the battery used must be capable of supplying the overall system for a minimum of 24 hours, considering the worst-case condition. The power consumption of every component is therefore critical when calculating the maximum period that a battery can supply. According to the datasheet of each component, the average power consumption for an Arduino Nano, nRF24L01 module, gyroscope module MPU-6050, and SIM900A module (idle) is 19 mA, 12.3 mA, 3.6 mA, and 22 mA, respectively. It is found that the resultant current consumption for a master node is 46.9 mA, whereas the current consumption for all child nodes would be 24.9 mA. The capacity of the lithium-ion battery used in the subsystem is 2000 mAh. With an average current consumption of 46.9 mA, the master node can operate for 42.6 hours with a fully charged lithium-ion battery. The child node, on the other hand, can operate for 80 hours in the absence of sunlight. The prototype of the power supply system is illustrated in Fig. 22. The battery charger TP4056 module is mounted at the back of the battery. The voltage output of the power supply system when charging is shown in Fig. 23. At 8.02 V, it is enough to power up the whole system. The TP4056 module is charged using a USB-C to illustrate the charging of the battery using a solar panel. Nonetheless, the result should be the same as when charging is done using power generated from a solar panel.

Based on the results obtained, an evaluation of the overall system is carried out. The cost and energy efficiency of the proposed system are calculated and compared with the conventional approach, which is the use of CCTV cameras. The power consumption of a typical DVR CCTV camera is 40 W. Assuming that eight security cameras are installed in a large-scale solar farm consisting of 1000 solar panels, the total power consumption used for the security cameras would be 320 W. On the contrary, the proposed system will draw 24.9 mA at 7.8 volts for the child nodes, so the power consumption per solar panel would be 194.22 mW. Assuming that the anti-theft system is implemented on 1000 solar panels, the total power consumption of the proposed system is therefore 194.22 W. The decrease in power consumption when replacing the CCTV cameras with the proposed anti-theft system is calculated using Equation (1):

$$\%\ \boldsymbol{decresase\ in\ power\ consumption} = \frac{\mathbf{320 - 194.22}}{\mathbf{320}} \times \mathbf{100\%} = \mathbf{39.3\%} \quad (1)$$

A decrease of 39.3% in power consumption can be seen when the anti-theft system is implemented in a large-scale solar farm. However, one should also note that the footage recorded by the CCTV cameras should be stored on a computer. If the power consumption of a computer is considered, the decrease in power consumption calculated above will be more significant. In addition, CCTV cameras require personnel for continuous monitoring.

Assuming four personnel were hired to monitor the security cameras, and given that the average monthly salary is RM2000, a total of RM8000 will have to be spent every month to have the security system working. On the other hand, the total cost of the proposed anti-theft system is only RM50 for each module. Having it implemented on 1000 solar panels will cost about RM50,000 in total. Comparing the price of using CCTV cameras and the proposed anti-theft system, it can be shown that despite the anti-theft system's greater initial cost, the overall cost is still a lot cheaper than using CCTV cameras in the long run.

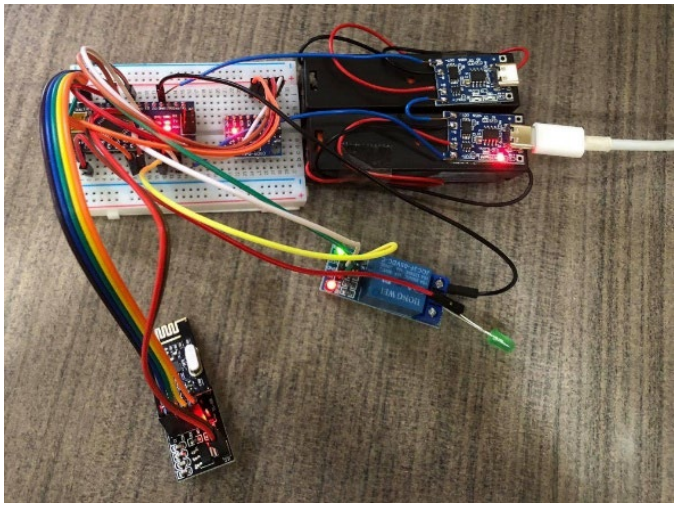


Fig. 22 *Power supply system*

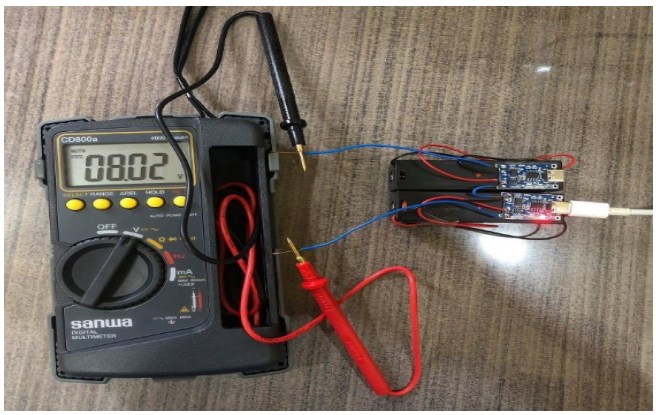


Fig. 23 *Power supply system output*

To quantitatively compare the performance of the proposed system with other methods, Table 1 presents the performance analysis. The proposed system overcomes some of the limitations found in previous works such as limited capability to encrypt the solar panel, limited alert functionalities and scalability. Furthermore, the proposed system allows the master node to be hidden among its child nodes as the appearance of the master solar panel is no different from all the child solar panels. Therefore, it is impossible for theft to locate the master node among thousands of solar panels in a solar farm, which prevents theft from bypassing the anti-theft system by sabotaging the master node of a solar panel. Such a design was able to solve the issue encountered by Bertolodo *et al.* [15] in their anti-theft alarm system, where the transmitter of the master node has the possibility of being sabotaged by theft. Finally, having a tree topology in the design of the anti-theft system requires only one notification system to be implemented in one of the solar panels, which in this design is the master node. This implementation will greatly reduce the cost, as all the child nodes do not need to have individual notification systems installed in the system. Through the transmission of an error signal from one node to the other, the master node can notify the owner on behalf of the child node, which initiated the error signal due to the theft. The

proposed system is energy-efficient and low cost incorporating wireless communication system using radio frequency and tree-topology for the encryption of solar panels that can be easily extended to large-scale solar farms applications. In addition, the proposed system integrated well with a solar tracking system.

Table 1 *Comparative performance analysis*

Method	Parameters						
	Cost	Power	Number of transmissions	Encryption system	Alert notification	Solar tracking system	Scalable
Goldack, D. [6]	Low	Low	Low	Yes	Yes	Yes	Yes
Energy, T. [7]	Low	Low	Low	No	Yes	Yes	Yes
Bertoldo et al [15]	Low	Low	Low	No	Yes	No	Yes
Thiemann, C. [2]	Low	Low	Low	No	Yes	No	Yes
Paolo & Viscontini [1]	Low	Low	Low	No	Yes	Yes	Yes
Khan, W. A. [8]	Low	Low	Low	Yes	Yes	No	Yes
Tan, Y. S. [3]	High	Low	Low	Yes	Yes	No	No
Proposed system	Low	Low	High	Yes	Yes	Yes	Yes

4. Conclusion

A wireless encryption anti-theft system that is energy efficient and cost-effective is proposed in this paper. The anti-theft system can encrypt the circuit of the solar panel and notify the owner in the event of a theft. This has, in turn, avoided the need to employ security guards to monitor CCTV cameras to monitor theft activity. A 39.3% reduction in power consumption is observed when the proposed system is used to replace the conventional security system using CCTV. The proposed anti-theft system utilizes a radio frequency transceiver and tree topology to reduce the cost of the system. The limited number of transmissions that can be done simultaneously, which is the weakness of a radio frequency transceiver, was offset using tree topology. The action of theft can be detected as soon as possible using the gyroscope module in the theft detection system. Implementation of a gyroscope instead of a magnetometer would allow the anti-theft system to work seamlessly with the solar tracking system. Such an anti-theft system would help investors secure the solar panels in the solar farm, thereby encouraging investment in large-scale solar farms to generate electricity for ancillary services. Besides, the proposed anti-theft system would allow investors to generate greater profit by reducing the power loss and cost spent on CCTV cameras as well as personnel.

Further studies can be carried out to optimize and improve the performance of the system. Firstly, a feature that allows the owner to change the password or the address of the channel can be included. The owner can change the address of the child nodes to receive a password from their grandparent nodes. Without the function of changing the address of the channel, a new solar panel will have to be installed to replace the stolen one. Next, a detection mechanism to detect which child node has initiated the error signal can be added to recognize the solar panel that has triggered the theft detection system, allow the owner to know the location of the thief, and take prompt action. Next, a conditioning monitoring system can be embedded on the solar panel to evaluate the health of the electronic components used in the anti-theft system. As the electronic components are subjected to failure and degradation, the failure of the anti-theft system may result in unexpected encryption of the solar panel when it fails to receive a password from the parent node. Therefore, conditional-based maintenance is required to be carried out to extend the lifespan of the anti-theft system while avoiding a sudden drop in the output power of the solar panel. With a conditioning monitoring system implemented, earlier detection of faults is possible, and maintenance of components can be carried out during the night without affecting the capacity factor of the solar farm. Finally, a GPS module can be installed in the master node to track the location of the module, which will allow the owner to track the location of the thief.

Acknowledgement

The authors appreciate the support from Heriot-Watt University Malaysia for providing the facilities, and financial support for this research.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *FCM Choong, K. Jia Jun;* ***data collection:*** *K. Jia Jun;* ***analysis and interpretation of results:*** *FCM Choong, K. Jia Jun;* ***draft manuscript preparation:*** *FCM Choong. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] Viscontini, P. & Paolo, C. (2015) Intelligent system for monitoring and control of photovoltaic plants and for optimization of solar energy production, *IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*, 1933-1938, https://doi.org/10.1109/EEEIC.2015.7165468
[2] Thiemann, C. (2010) Alarm system for photovoltaic modules as well as method for protecting a photovoltaic installation from theft, United States Patent 20100207770.
[3] Tan, Y. S. (2017). Wireless control of anti-theft solar photovoltaic module. [Undergraduate dissertation, Universiti Tunku Abdul Rahman, Malaysia].
[4] Zhang, K., Si, C., Zhu, Z., Guo, C., & Shi, Q. (2018) A two-dimensional solar tracking stationary guidance method based on feature-based time series, *Mathematical Problems in Engineering, 2018*, 1-12, https://doi.org/10.1155/2018/3420649.
[5] Reaz, M.B.I., Assim, A., Choong, F., Hussain, M.S., & Mohd-Yasin, F. (2006) Prototyping of smart home: a multiagent approach, *WSEAS Transactions on Signal Processing*, *2(5)*, 805-810, ISSN: 1790-5022.
[6] Goldack, D. (2003) Protective system for a solar module, United States Patent 6650031.
[7] Energy, T. (2015) Anti-theft system and method using a multiple radio frequency signal for solar panel system, United States Patent 9000919.
[8] Khan, W. A. (2018) A novel anti-theft security system for photovoltaic modules. [Undergraduate dissertation, Universiti Tunku Abdul Rahman].
[9] Rattanawichai, P., Fangsuwannarak, T., & Laohawiroj, S. (2021) Monitoring system of smart cassava farm with solar energy by using internet of things, *2021 International Conference on Power, Energy and Innovations (ICPEI),* 146-149, https://doi.org/10.1109/ICPEI52436.2021.9690659
[10] Hassan, S., Bari, S., Shuvo, A. S. M. M. B., & Khan, S. (2021) Implementation of a low-cost iot enabled surveillance security system, *7th International Conference on Applied System Innovation (ICASI)*, pp. 101-104, https://doi.org/10.1109/ICASI52993.2021.9568426
[11] Khan, Z.A., Adil, M., Javaid, N., Saqib, M.N., Shafiq, M., & Choi, J.G. (2020) Electricity theft detection using supervised learning techniques on smart meter data, *Sustainability, 12(19)*, 8023-8033, https://doi.org/10.3390/su12198023
[12] Chowdhury, I., & Ahmed, T. (2021) Design and prototyping of sensor-based anti-theft security system using microcontroller, *International Journal of Engineering Research & Technology (IJERT), 10(3)*, 58-66, https://doi.org/10.17577/IJERTV10IS030019.
[13] Gorjian, S., Ebadi, H., Trommsdorff, M., Sharon, H., Demant, M., & Stephan, S. (2021) The advent of modern solar-powered electric agricultural machinery: a solution for sustainable farm operations, *Journal of Cleaner Production, 292(126030)*, 1-23, https://doi.org/10.1016/j.jclepro.2021.126030
[14] Chew, K.W., Pang, W.L., Choong, F., & Chua, F.Y. (2008) VHDL modelling of the wireless audio transceiver through IEEE802.3 and IEEE802.11, *6th International Conference on Electrical Engineering, 6(6)*, 1-12, https://doi.org/10.21608/iceeng.2008.34225
[15] Bertoldo, S., Lucianaz, C., & Allergretti, M. (2012) A wireless sensor network ad-hoc designed as anti-theft alarm system for photovoltaic panels, *Wireless Sensor Network, 4,(1),* 107-112, https://doi.org/10.4236/wsn.2012.44014