Keyless Smart Lock (Secured Illini) Proposal

Andrew Ruiz, Sebastian Sovailescu, Bowen Cui
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana Champaign
Urbana, United States of America
TA: Sanjana Pingali

I. Introduction

A. Problem

Bike theft remains a major issue in urban and suburban areas, with millions of bicycles stolen annually due to the shortcomings of conventional locks. Despite the use of U-locks and chain locks, thieves easily bypass them using bolt cutters, angle grinders, and lock-picking tools. According to 529 Garage, over two million bikes are stolen each year in North America, discouraging cycling and undermining sustainable transportation efforts. Research by Sidebottom et al. (2009) highlights that even high-security locks can be compromised within minutes, exposing the need for more effective theft prevention measures. Additionally, improper locking techniques further contribute to the problem, leaving bicycles vulnerable. Addressing these security gaps is essential to protecting cyclists and promoting bicycle use as a reliable mode of transportation.

B. Solution

We propose a smart bike lock equipped with tracking, a keyless locking mechanism via Bluetooth, and an integrated siren that offers a comprehensive solution to the problem of bike theft. GPS/WiFi tracking ensures that stolen bikes can be quickly located and recovered, significantly increasing the chances of retrieval compared to traditional locks. The keyless locking mechanism eliminates vulnerabilities associated with physical keys or combinations, reducing the risk of lock-picking or brute-force attacks. By using Bluetooth connectivity, cyclists can securely lock and unlock their bikes through a smartphone app, adding convenience while maintaining security. Additionally, a built-in siren serves as an active deterrent by emitting a loud alarm when unauthorized tampering is detected, drawing attention and discouraging thieves. This multi-layered security approach not only makes theft more difficult but also increases the likelihood of intervention before a bike is stolen. By integrating these advanced features we will be helping to reduce bike theft rates and promote cycling as a secure and viable mode of transportation.

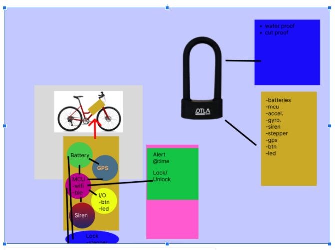

Fig. 1. Bike lock system interactions

C. High-level requirement list

- Electronic locking system that can be manually overridden with master key (or override code) that can withstand over 1000 lbs of force.
- A 90dB siren will sound for 10 seconds that is triggered by theft attempts when within a locked state. Theft attempts will be determined when excessive movement is detected which sensitivity will be experimented with.
- Can remotely communicate with a user's device when a registered device is within 10 feet of lock. Will register the device once for the operation of the keyless locking mechanism.
- 3.5V Indicator LEDs to indicate the lock's current state as well as power level. Will only turn on when motion is detected so as to not drain the battery.

II. Design

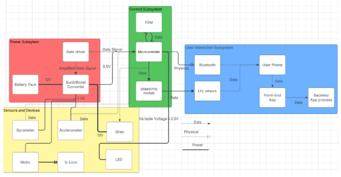

Fig. 2. Subsystem Block Diagram

A. Power Subsystem

Description: The power subsystem supplies power to all the components, ensuring long battery life and reliable connections. Most components, including the accelerometer/gyroscope and MCU, operate between 3.7 and 4.2 volts, while more power hungry sensors, such as the siren and the stepper motor, operate at a higher voltage, so we will utilize a buck converter to supply appropriate power from our 12V battery.

Components:

- Rechargeable Li-Po (3.7V)
- Voltage regulator
- Buck converter

Requirements:

- Battery must last at least one week on a full charge
- Provide current continuously to all sensors and the microcontroller.
- Output must be able to provide stable 3.7V, 4.2V, and 12V rails

B. Controls Subsystem

Description: Central control unit that acts as the "brain" of our smart bike lock. It processes accelerometer/gyroscope data, executes lock/unlock commands, controls the siren and manages wireless communication.

Interfaces:

- MCU Button : GPIO
- MCU LED : PWM GPIO
- MCU Siren : GPIO
- MCU Stepper Motor : I2C or SPI
- MCU WiFi/BLE : Integrated, so none.

State Name	Description
LOCKED	The accelerometer/gyroscope are ON and listening for anomalies. LED is yellow
UNLOCKED	The accelerometer/gyroscope are OFF. Cannot be triggered. LED is green.
ALARM ON	Siren is ON for 5 seconds. LED is blinks red for 5 seconds.
CONNECT	The MCU is looking for a connection to BLE/WiFi. LED turns blue.

TABLE I
FSM TABLE

Components:

- MCU

Requirements:

- Must lock/unlock the mechanism within **100ms**.
- **No** dead states.

C. Theft Detection Subsystem

Description: This subsystem triggers an alarm and notifies a user of unwanted tampering by monitoring the position of the bike using positional sensors. In the ALARM ON state, the siren plays for 5 seconds at over 100dB in an attempt to deter the thief. Simultaneously, a notification is sent to the user over WiFi and an LED blinks RED for 5 seconds.

Components:

- MCU
- Accelerometer
- Gyroscope
- Siren

Interface: The MCU will collect accelerometer and gyroscope data at predefined intervals. If an abnormality is detected, the FSM will enter a triggered state in which the alarm will begin sounding for a fixed amount of time. The user will also receive an alert on their phone app over WiFi.

Requirements:

- LED must be RED for 5 seconds during ALARM ON state.
- Siren is ON for 5 seconds.
- App must send 1 notification and 1 log.

D. Locking Mechanism Subsystem

Description: This subsystem controls the locking mechanism through an app or a button. A hidden metal bar is moved back and forth by a stepper motor in order to secure the lock. We can transition from the LOCKED to the UNLOCKED state either through bluetooth or by pressing a button combination. The states are represented by the LED colors described in the FSM table.

Components:

- MCU
- Metal piece
- Stepper motor
- Button/ keypad
- LEDs

Requirements:

- The lock must open or close securely and timely based on password entry.
- The user must understand the state the lock is in.

E. User Interaction Subsystem

Description: This subsystem allows the user to utilize the full capabilities of WiFi and BLE. Once connected to either, the ESP32 chip can send and receive data, improving our system's connectivity. Once connected to Bluetooth or WiFi, the ESP32 microcontroller will transmit our data readings to a cloud-based backend, such as Firebase. We will collect timestamps, accelerometer/gyroscope values, and various state signals to log detected tampering and decrease fake alarms. We can also use Google's API to triangulate the device's location. We will be able to control the lock from our app.

Components:

- Frontend (Python/NextJS)
- Backend (Python/ Firebase)

Requirements:

- Receive app alert within **15 second**s of incident
- Record **5** incidents

F. Tolerance Analysis

1) Battery life: ssuming we use a 12V 5-10 Ah battery, we calculate the battery life using the formula : Battery life = Battery Capacity / Total Current Draw. Based on the ESP32-S3-WROOM datasheet, we made the following assumptions about each subsystem's average current consumption

Component	Average Current
MCU	25mA
BLE/WiFi	20mA
Accelerometer/Gyroscope	3mA
Siren	0.1mA
Stepper Motor	0.1mA
LED	0.001mA
Total Current Draw	48.2001mA

TABLE II
Component Average Power Draw

Total battery time = [5000 [mAh]/ 48.2001[mAh] = 103.734 [h] /24 = 4.32 days , 10000/ 48.2001 = 207.468 = 8.64]. In order to reach a battery life of one week we would likely need a 10000mAh cell or multiple smaller cells with a total capacity over 10000mAh

2) Lock Force Tolerance: With the locking mechanism, we have a quarter-inch diameter, 3 inch long steel bar that is held by two supports on the top when force is applied upwards. The U-bar itself is focused on a 1/4 inch section at the center of the bar so the tolerance is how much force can be applied across this section. Since the force is applied at the center of the quarter-inch diameter (0.25 inches) steel pipe, with support at both ends, we can model this as a uniformly distributed load (UDL) over a small length. The primary failure mode to consider is bending stress. For a simply supported beam with a point load at the center, the maximum bending moment Mmax is given by: $Mmax = F(L - a)/4$ with "F" being applied force and "L" being the effective length of the beam (span between supports) which ends up being about an inch and "a" being the 0.25in length of the U-bar. The maximum bending stress in a circular cross-section is given by:$MmaxC/I$ with "C" being the outer radius 0.25/ 2 = 0.125in and "I" being equal to$I = (pid^4)/64$ The lock will fail when the maximum stress exceeds the yield strength of the steel which is about 53,700 psi. Given all of this we calculated that the maximum force the lock can withstand before bending is approximately 1,757.3 lbs. If the applied force exceeds this value, the lock will begin to deform permanently, reducing its effectiveness. We found that this value was more than acceptable because it would be very hard to manually apply this much force without industrial grade tools.

III. Ethics and Safety

Developing a smart bike lock with tracking, Bluetooth locking, and an alarm system presents several ethical and safety considerations, particularly in line with the IEEE Code of Ethics and the ACM Code of Ethics. Privacy is a major concern, as location tracking must be handled responsibly to prevent misuse. To ensure user data security, we will require explicit consent for location tracking. Additionally, reliability is crucial, as a malfunction could leave a user stranded. Following ethical guidelines to "avoid harm," we will integrate redundant unlocking mechanisms, such as backup PIN entry or an emergency override. In addition to ethical considerations, our design must comply with safety and regulatory standards. Since our smart lock utilizes Bluetooth and GPS, it must meet FCC Part 15 regulations for radio frequency emissions and comply with UL 437 security standards to ensure resistance to physical attacks like cutting or drilling. Additionally, we must consider state laws regarding electronic tracking devices, ensuring that location data remains private and is accessible only to the owner. Potential safety concerns, such as false alarm activations will be addressed by implementing adaptive sensitivity settings. By adhering to these ethical and safety standards, we can develop a secure, reliable, and compliant smart lock that effectively reduces bike theft while minimizing risks to users.