UNITED STATES PATENT APPLICATION

For

NETWORKED DEFENSE SENSORS

INVENTOR:

JASON W. RUPE

Description

As we begin to recognize the value of our power and communication networks, physical security will get more attention. See this use case: https://interestingengineering.com/can-the-us-upgrade-its-infrastructure-to-defend-against-drone-attacks

This is a call to develop small sensors that can detect the use of drones in the area. By creating small sensors that can be on the communication network and complimentary sensors that can connect to the power network, we have redundant capabilities to sense when a drone is in the area, and thus can sound alarms, track information for post attach analysis, and enable fast reaction.

By combining audio sensors and RF sensors to catch drone control and information communications, the drone can be specifically identified, and then the information can be immediately relayed to authorities based on the information gathered. The attack signal itself can be used to add information about what type of attack was used and what to look for (hit on power, hit on communication network).

Someone who is not attacking but flying too close to the sensors which confirms flight too close to the power lines or communication lines can be reacted in one way. A swarm of drones would require a different reaction. Registered drones could be identified and if following flight plans or regulations allow to continue, or automatically ticket (with telemetry to confirm) if a violation occurs, or send authorities of a real threat is in order.

To expand the use and increase the value of the solution, it can be augmented to detect digging in the area as well and confirm that the location has had cable location done recently or not, and send authorities if not. There may be other attack types that can be identified in similar ways such as human voices, digging equipment, sound of a ladder rattling, etc. The signal can go to some core or edge logic for analysis to assess the threat and decide on action (potentially leveraging ProOps).

Note that simple augmentation of Gridmetrics 2.0 sensors and some additional back office logic may be sufficient, so this idea could be implemented as an extension to Gridmetrics.

Method Flow:

0) sensors in monitor mode, collecting baseline data and reporting it into a centralized, networked, or edge store and compute logic.

1) sensors in area pick up the signal indicating a drone, or other threat.

2) sensor information is sent to a centralized, networked, or edge store and compute logic that assesses the threat. If sensors or store or compute nodes need to share information, this happens now as needed using the logic set for assessment needs.

3) Information is collected, correlated, and assessed for likely attack vectors or threat types. A confidence level is given to each attack vector or threat type. Depending on the categorization of the information into threat vector logic, and the confidence in the assessment, a decision is made.

4) Decide on actions: if the decision is that the threat is likely real, a next level of logic determines which entities and systems and dashboards to alert and send information to. If the threat is low confidence, additional information may be collected to firm up the confidence or provide a soft alarm in case there are out of band opportunities to gather more information such as a policeman in the area already who can cheaply check out the potential threat. If the threat is high confidence but not clear what the attack vector is, such as multiple attacks potentially, then it may be that additional information is needed but certainty to alert some authorities is in order. The core logic for decision making may be sophisticated.

5) continue to collect information until the threat is cleared. use sensors to detect local action to mitigate the threats too.

6) if authorities alerted, and they indicate back that they are checking out the threat, continue to provide translated information to assist. Help with coordination by informing authorities in action who they may encounter.

7) After the threat is addressed, collect information about the threat type, and use that to train the logic further (either manually via rule based, or training of AI/ML) for continuous improvement.

8) make any repairs to the grid, network, or sensors as needed after recovery.

9) reset alarms and condition logs, and return to monitor mode.

Background

Problem described here: https://interestingengineering.com/can-the-us-upgrade-its-infrastructure-to-defend-against-drone-attacks

Abstract

Develop small sensors that can attach to the electric grid and the communication network in complimentary, redundant ways, to sense attack vectors from drones, and potentially construction in the area that is not permitted. It may be possible to do this as an augmentation to Gridmetrics 2.0.