SAFEZONE: A FRAMEWORK FOR DETECTING AND PREVENTING DRONES' MISUSE

AlHanoof A. AlHarbi[1], Fatima M. AlAmoudi[2], Razan A. AlBrahim[3], Sarah F. AlHarbi[4], Abdullah M. Almuhaideb[5], Norah A. Almubairik[6], Abdulrahman AlHarby[7], and Naya M. Nagy[8]

Department of Computer Science, College of Computer Sciences & Information Technology,
Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia.

Email: {alhanoofalharbi[1], fatimamo.amdi[2],razanalbrahim1[3], sfalharbi2[4]}@gmail.com, {amalmuhaideb[5], naalmubairik[6] aalharby[7], nmnagy[8]}@iau.edu.sa

(Presented at ICSC, 2019, KSA)

ABSTRACT*—*Recently, drones received a rapid interest in different industries worldwide due to its powerful impact. However, limitations still exist in this emerging technology, especially in privacy violation. As these aircraft, may threaten the security of entities, through entering restricted areas accidentally or on purpose. Therefore, This project aims to develop a mechanism to detect and prevent drones from invading people's privacy by accessing restricted areas. The proposed solution is a combination of detection and prevention methods, where a passive radar and radio frequency sensors will be joined in a centralized system; to detect and prevent drones from accessing others' property. The passive radar will have the ability to detect and identify a drone. Moreover, prevention techniques would be applied by sending jamming signals and forceful safe landing of the drone. We believe applying such mechanism will assist in limiting drones from violating the privacy of restricted areas in order to accelerate the drones' application and development.

Keywords— Privacy, Drone, Detection, Prevention, Jamming, Sensors, UAV.

INTRODUCTION

Recently, there has been a rapid interest around the world in Unmanned Aerial Vehicles (UAVs), often referred to as drones. A drone is an aircraft that operates without a human pilot onboard, remotely controlled or autonomously. They have been a focused subject in various industries [1]. This is due to their potential in a broad variety of applications, not only military and defense applications, but also civilian applications such as in traffic monitoring, movie making, popular events like concerts, examinations for industries such as oil fields and oil pipelines, surveillance, crime scene analysis, accident photography, delivering packages and many others application [1]. Hence, it has been estimated that by the end of this decade, the worldwide production of drones for all types and range would rise from $4 billion annually to $14 [2]. billion Thus, regulating the usage of drones, and proposing rules is just the start of a new era. Drones have several security issues as they have not been designed with a security perspective in mind, the evolution of drones for civilian functionality has burst into multiple issues related to safety, privacy, security, ownership of data, regulation, and business models [1]. One of the significant concerns is that drones threaten people's privacy by entering restricted areas where they are banned [3]. They can collect, store, and process data [4]. Privacy can be invaded by drones from two sides, by purpose, and by accident. Thus, this research paper aims to answer this question "How can drones' misuse be restricted using detection and prevention methods?" and ensure the privacy maintenance and data protection of citizens. The structure of this paper is as follows, It begins with discussing the related works. Then, followed by explaining the proposed solution. Finally, the conclusion will be given.

I. RELATED WORKS

This section illustrates different detection methods, then, it compares the related works to our proposed solution.

A. Drones' Detection Methods

In this section, several detection methods are discussed. Detection of drones would be the first step of preventing them from accessing restricted areas. There are four main detection methods that are used in prior works; detection using sound, computer vision, radar, and ambient RF signals. This research paper focus in

1. Passive Radar

There are two types of radar detection, active radar, and passive radar. Active radar operates by radiating an electromagnetic wave and receives the reflected wave from a target. Furthermore, an emitted wave would be directed by the transmitting antenna into an object, that will reflect it back to the receiving antenna as shown in Figure 1 [5]. On the other hand, passive radar contains a transmitting antenna and a receiving antenna, where the transmitting antenna will radiate a signal to objects. The receiving antenna will collect the radiated electromagnetic, reflected or scattered waves from a target directly, in addition, the time of the time delay will be calculated between the radiated signal directly from the transmitting antenna and the reflected signal from the object, Figure 2 defines the function of passive radar. [5] [6]

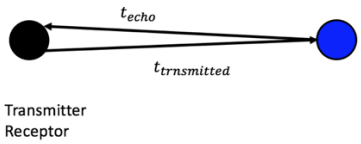

Figure 1 Active radar [5]

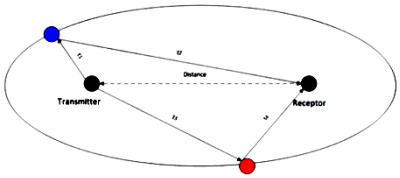

Figure 2 Passive Radar [5]

Studies showed that passive radars function more effectively than active radars. There are many features and advantages that passive radar has, but the most important ones are good detection ability for low-altitude targets, in the opposite of active radars, detecting covertness aircraft, longer detection range, and broad frequency coverage. As

there for features, they are: lighter in weight, lower cost, and smaller volume. [6]. Passive radars are developed in order to not change or modify the existing radar transmitters or installing new sensors [7].

On the other hand, as all technology has downsides, passive radars have some. They can be limited in channel bandwidth which will result in a poor range resolution, the detection range is restricted by the receiver design in addition to, there is a shortage in experimenting it with polarization combinations. In order to eliminate these disadvantages, a multi-static radar is more desired, which is a combination of active and passive radars. As a result of the combination, this would reduce the resilience on the illuminator, the waveform can be tailored to fit an interest, passive nodes can detect covert operations and increase data fusion chances. [7]

A lot of researchers prefer passive radars overactive in detecting UAVs. In [7], a multiple of passive radars was presented, types of passive radars were divided into detection/classification radars and detection radars. The classification feature in a detection radar is needed in order to prevent false positives. There are five proposed passive detection radars but only two a classification feature was included within.

The first classification/detection radar is commercial of the shelf (COTS) universal software radio peripheral (USRP), three experiments were applied each has different application; mobile phone illumination, micro base station, and base tower illumination. The test results were pleasant, where an accurate motion was generated from two types of drones: quadcopter and helicopter-style drones. The system has some limitation in classifying a drone in a further detection range than 100m, due to small RCS and path loss. [7]

The other classification/detection radar is based on doppler offset that was induced in orthogonal frequency-division multiplexing (OFDM). The proposed methodology wasn't tested on a real drone, but it can be implemented on any OFDM transmitter. The system would operate on fifth generation service where the frequency range from 3 and 4 GHz. [7]

2. Detecting Drones using Radio Frequency

The last type, Radio Frequency (RF) sensors, are low-costly and able to detect in a long detection range. Moreover, these RF sensors have the ability to spoof and jam drones by imitating a remote controller or spoofing GPS signals. A downside is that such sensors need prior training to identify/classify different drones. Additionally, they fail for fully/partially autonomous drone flights due to no/limited signal radiation from a drone/controller. One simple example of RF-detection is to monitor a wide range of RF, such as from 1 MHz to 6.8 GHz, and take any transmitter of unknown RF signals as a drone [8]. This method will induce a high probability of false alarms since an unknown RF transmitter is not necessarily a drone [9]. Another example of RF-detection which is a cost-effective and passive technique is Matthan detection system. Matthan depends on the unique physical signatures that persist across drones to detect and differentiate them from other moving objects. It recognizes drone by analyzing the drone's body shifting and vibration from drones related RF communication channel. [10]

3. Detecting Drones Using Audio

The third type is using audio detection. Sound detection is useful to overcome the limitations in other detection methods. Audio detection is passive, inexpensive for simple microphones and it doesn't get affected when it's night-time, as in some camera detections [8]. On the other hand, audio detection doesn't provide accurate results because of the noise factor that might result in many false-positives. Additionally, the range of detection depends on the type of audio sensor and environmental factors, such as wind and noise. Finally, audio detection requires a comprehensive database of audio signatures to make comparisons [8]. Audio detection was implemented in different projects and had different results. For example, [11] focused on analyzing and mining drone's sounds for an effective classification and detection of drones, this solution could overcome the failure of detecting UAVs using motion sensors, thermal sensors or high-resolution cameras at dark. The solution uses Hidden Markov Model for phenome analysis, which improved the efficiency of detection and classification and speeded up the analyzation process.

Another example of sound detection [12], which uses the correlation method, used in mathematics and signal analysis, and audio fingerprinting, that used in popular applications like Shazam. These solutions targeted the detection of small-sized drones. The first suggested solution, correlation method, compares the stored signal samples of the device' database to the recorded sample. First, the sample is recorded using a microphone or any recording device. Then, the recorded sample has to go through the Fast Fourier Transformation (FFT), which is a sound filtering process that reduces noise. Finally, the correlation process takes place to determine if it's a drone sound or not; through analyzing the similarity of the recorded sample and the sample stored in the database, which is the real drone's sound. This method was tested with different drones and a different set of sounds, and each got a different result and accuracy level. The results show that audio fingerprinting has a satisfying outcome according to the circumstances and the correlation method is adequate although there were some limitations, which were the small database size, inaccuracy of some results and testing non-real-time flying UAVs as all the tests were conducted in a closed place.

4. Detecting Drones Using Camera

The detection of a flying object is facing some unique challenges such as, differences in shapes and sizes that produce complex and changing backgrounds, distance range; potentially dangerous objects must be detected from long distance range, and the environment is fully three dimensional that makes the motions more complex for detection. A new detection method is proposed for detecting whether the object of interest poses danger or not by grouping 3D descriptors computed from spatiotemporal image cubes (st-cubes). These cubes are created by stacking motion- stabilized image windows over many consecutive frames, that give more information than using a single image. With the use of a regression-based motion-stabilization algorithm, this approach is becoming more practical and effective, unlike the one that relies on optical flow. This approach remains effective even when the shape and size of the object to be detected is barely visible or blurry. Moreover, it can be seen as a way to merge both the appearance and motion information to obtain effective detection in a very challenging condition. [13]

This approach of detection shows that temporal information from a sequence of frames plays a major role in the detection of small fast moving objects like UAVs or aircraft in complex environments [13]. Moreover, this approach obtains higher accuracy of detection compared to either appearance or motion-based methods individually. [13]

Thus, st-cubes is a new method of detecting drones using a camera that has high accuracy and can detect small drones in noisy environments, with the combination of motion features and appearance features comparing to the other existing methods which lack the high accuracy and they can be affected by the environments. [8, 9]

5. Hologarde

Hologarde aims to protect sensitive areas from explosive, chemical products, radioactive substances attacks. Hologarde existed solution combines three major technology to ensure that best practice of protection and accuracy is implemented. The first technology is radar, Hologarde uses pioneering 3D radar, that has already proven its capability to track and detect small objects. The software developed for this radar analysis the movement pattern of the target, in order to differentiate drones against the other object in the same range. The second technology is RF, which has the ability to detect the protocol used for data exchange between the drone and the pilot. Thus, combining RF with the radar technology approve that the target is a drone, not anything else such as a bird. The third and final technology is long range HD infrared cameras to provide visual confirmation of drones. [14]

6. Comparison Analysis of Drones Detection Methods

This subsection illustrates a comparison of existed related works, as shown in Table 1 below, it compares the detection techniques used to detect UAV. The comparison performed based on six optimal requirements: cost-effective, high accuracy, long range, convenience, unaffected by noise and generalization. To clarify, these specific requirements were chosen because they were discussed by the previous literature. It is noticeable that all mentioned literature have reached the high accuracy and cost effectiveness but each misses out some requirements or minor features. However, this research project seeks to implement what has been achieved in previous related works and combine existing technologies in one effective solution. The optimal requirements for the proposed solution are defined below:

- Cost-effectiveness: This requirement shall indicate the need for an affordable cost of the solution. The retrieval and implementation of the detection/prevention method must be a reasonable cost for small to medium entities.
- High Accuracy: This requirement means that the implemented solution must be able to successfully detect/prevent 80% of the flying drones.
- Long Range: This requirement is defined as the covered detection/prevention distance, as the solution is suspected to cover long range in detecting drones. The long acceptable range can cover from 1.5 to 2 km.
- Convenience: The requirement means that the implemented solution is easily used and doesn't require a long period of training to get familiar with its usage. The acceptable training period can be no longer than 2 to 3 weeks.
- Unaffected by noise: This requirement means that the chosen solution isn't affected by environmental or natural conditions and still maintains its high performance with stability.
- Generalization: This requirement means that the implemented solution must be able to perform and act to all types and sizes of drones.
-

Table 1 Detection Comparison Analysis

		Solution Requirement					
Technology	Reference	Cost Effective	High Accuracy	Long Range	Convenience	Unaffected by noise	Generalization
Radar	[7] [8] [15]	√	√	≡	≠	√	≡
Audio	[11] [12] [13]	√	≡	≡	≠	χ	≡
Camera	[9] [10] [11]	≠	√	√	≠	≡	√
RF	[11] [10] [14]	√	√	√	≡	≡	≠
Hologarde	[15]	χ	√	√	√	√	√

√ Completely applicable χ Not applicable ≡ Partially applicable ≠ Not mentioned in the paper

To conclude, in order to distinguish the important requirements that are needed in these detection methods a comparison analysis was conducted, and shown there are some shortages in each and every detection method.

B. Drones' Prevention Methods

The second step of catching a drone is prevention, where this section is discussing the implemented methods of prevention. Preventing drones from accessing a restricted area would reduce the invasion of privacy. A number of solutions were implemented, there are practical solutions and impractical solutions. Prevention methods are applied by entities for different reasons.

The practical solutions that are employed by enterprises are NFZ and PITBULL, these methods are more flexible and can be implemented by every entity. The impractical solutions were catching a drone by a larger drone, eagle, or a gun, these solutions are impractical due to it requires cost and time for training.

A proposed solution that was by one of the riding companies, DJI, whereas they addressed this problem by No-Fly Zone (NFZ) technology in their developed drones "Phantoms". NFZ can address the problem by restricting or forcefully landing the drone, but it lacks invading the privacy where the drone could not move but still transmit

data to the owner. In addition to, the drone's camera can still record and take footages of the restricted area. Another shortage of the solution that it could be disabled through the request to unlock the zone. Moreover, the solution is only implemented on the DJI Drones but neglects the other drone vendors. [16]

Another solution was to implement wearable jammers "PITBULL" to soldiers that detect and defends against malicious drones. The solution covers the distance 1000 meters and can work manually or autonomously. PITBULL covers the 2.4GHz, 5.8GHz and GNSS frequency bands and requires external antennas to cover additional frequency bands. The solution is limited; where it focuses on helping soldiers to focus on the mission and covers limited frequency bands and space area, which won't be an effective solution for securing restricted areas. [17]

The impractical solutions were catching a drone by a larger drone, where it was implemented by a police department in Tokyo. The solution implementation is based on warning the drone's pilot that the drone entered a restricted area if the pilot refuses to retreat it will be trapped and interrogated. [4]

Another technique of catching a drone is by training an eagle. The Scotland metropolitan police started to train eagles in order to catch a drone by tutor them that a drone is their prey. [4]

The last solution is catching a drone by a gun. There are two types of gunshots, the first method is a net will be shot in order to catch a drone. After catching the drone's rotors get knotted a parachute will release in order to ensure a safe landing of the drone [4]. The other method is shooting signals, where the signals will jam the communication between the drone and its pilot, and provide a safe vertical landing on the spot. [18]

The solutions proposed are lacking certain essential requirements. The two practical solutions are considered as acceptable solutions, nonetheless, they lack the detection feature. The other part of the implemented solutions, the impractical solutions, needs a more efficient detection method to be applied. Depending on the eye watch which is cannot be reliable nor accurate in addition some of the detectors cannot detect at night or it can detect at a short range.

1. Comparison Analysis of Drones Prevention Methods

This subsection demonstrates a comparison of existed related works to drone prevention, as shown in Table 2 below, it compares the prevention techniques used nowadays to prevent UAV from accessing restricted areas. The comparison performed based on the same requirements shown in the detection method before. Moreover, this research project aims to reach an optimal solution for both detecting and preventing drones.

As stated, a comparison analysis was also conducted based on the existing prevention methods. There was a lack of implemented prevention methods in several aspects. The practical solutions, NFZ and PITBULL, were not covering both sides detecting and preventing drones. The other solutions were impractical since they rely on living creatures that cannot detect at night or another drone that can be misled. As a result, there was not a whole solution that covers both sides detecting and preventing drones in one centralized system.

Table 2 Prevention Comparison Analysis

		Solution Requirement					
Technology	Reference	Cost Effective	High Accuracy	Long Range	Convenience	Unaffected by noise	Generalization
Larger Drone	[19]	≡	√	≠	≠	√	√
Gun	[19]	≠	≡	χ	≠	χ	√
PITBULL	[17]	≠	√	χ	√	√	√
DJI (No-Fly-Zone)	[16]	χ	√	√	χ	χ	χ
Eagle	[19]	χ	√	√	≠	χ	√
Jamming Gun	[18]	≠	≡	√	√	≠	√

√ Completely applicable χ Not applicable ≡ Partially applicable ≠ Not mentioned in the paper

II. PROPOSED SOLUTION

This section covers the system requirements that are used in the proposed framework. The framework suggests implementing sensors that would help in securing the area; where it would detect and prevent invading drones as shown in Figure 3. This section includes an explanation of the functional and non-functional requirements. The proposed solution functional requirements are divided into two sections detection and prevention functions/requirements.

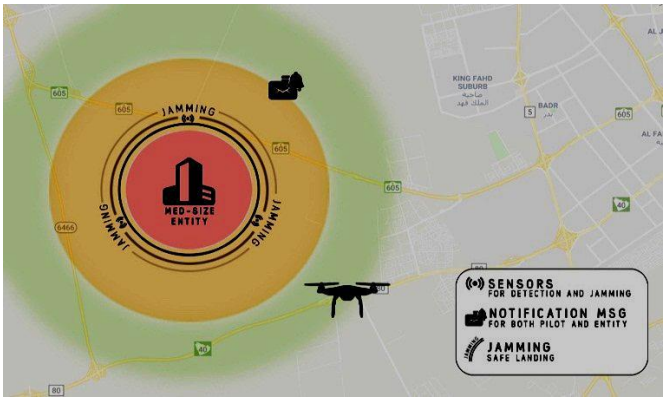

Figure 3 Illustration of The Proposed Framework

A. Functional Requirements

1. Detection Requirements

- Sensing:

The applied sensor should effectively sense the area for any object that hovers over the property or the restricted area. There are two zones where the sensor should distinguish between them, red and yellow zones. In each zone, a specific action will be taken. The identification function fully depends on the sensing function. Once the sensor has sensed that there's a drone the identification phase would initiate.

- Identification:

In order to catch a drone, the sensor must identify objects and differentiate between them. A sensor should specify the objects, whether it is a bird or a drone in order to determine or identify the drone by tracing its MAC address since every drone has the feature of broadcasting it's MAC address. The government has to have a database with all registered drones in the country and the associated MAC address, owner, owner's personal information.

- Sending Notification Message:

A message should be sent to the entity which is the owner of the restricted area, and as well to the pilot which is the drone's owner. This function will be initiated once the drone has crossed the yellow zone. This function cannot be accomplished unless the drone is identified. A database at the entity's side would record every entered drone along with its MAC addresses. If the drone has crossed the yellow area the entity would be notified and they can call the police for further investigation or actions.

2. Prevention Requirements

- Jamming:

The proposed solution will have to be notified if the drone has crossed the red zone area. Once a drone has crossed it the sensor will jam the drone's signal in order to disconnect it from the pilot's controller. This function is important in order to guarantee that the captured data are not sent or disclosed to the pilot or any other third party.

- Safe Landing:

The proposed solution will implement a safe land for a drone after crossing the red zone area. The sensor will be alerted that a drone has been detected in the red zone area and it will take the action of safe landing it. This will guarantee the entity to know what kind of information is being stored in the drone and transmitted to the attacker, in addition, it can help in identifying the attacker's identity.

B. Non-Functional Requirements

- Accuracy

Accuracy defines how often does our model gives correct prediction, thus the proposed solution of detecting and preventing drones misuse shall be reliable, which aims to eliminate the number of false alarm and ensure high confidence detection and prevention.

- Range

The proposed solution shall work within the range specified by the entity requirements.

- Speed

Due to the importance of detecting a drone, the proposed solution shall be performed in a timely manner that leads to achieving the effectiveness and efficiency of the solution.

- Cost-effectiveness

The proposed solution needs to maintain a low total cost that is affordable to mid-sized entities.

- Convenience

The proposed solution must integrate a conventional centralized system that manages the sensor information with an easy-to-use operator interface, to enhance the situational awareness and decision making.

- Generalization

The proposed solution shall be applicable for multiple classifications of drones to be used on different types of drones.

- Unaffected by noise

The solution must maintain stable and operate under different conditions such as a natural condition.

Thus, the solution is believed to be one of the strongest prevention and detection systems of drones. The implemented solution achieves the specified requirements from several aspects.

III. SOLUTION DESIGN

This section visualizes the proposed solution in detail. It points out to the system flowcharts which illustrate the workflow of the system. Also, it shows the design consideration of the hardware and software where interaction between the drone's user and the drone's system occur.

A. System Architecture

The main purpose of this system is that an admin which is the owner of the property has full control of the flying drones on his area. The admin can monitor every movement, and the system can define whether it's a drone or not. Furthermore, prevention techniques will be applied in order to protect the privacy of the property's owner graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates). Figure 4 illustrates the functions performed by the user "admin" and the relations between the functions and actors.

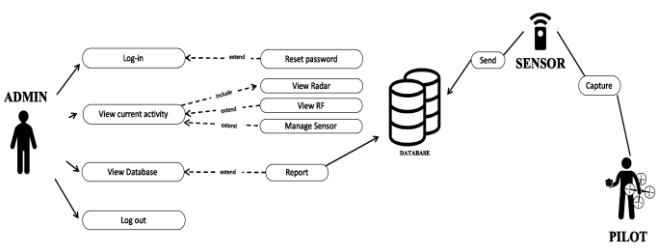

Figure 4 Admin use-case

B. System Flowchart

This subsection demonstrates the flow charts of the proposed solution, starting with the entire system flow chart that illustrates how our system will react once the drone reaches the restricted area, it will take actions on both sides yellow and red zone. The yellow zone means the drone is flying near the borders of the restricted area so only a notification will be sent to the pilot to warn him, unlike the red zone, the drone accessed the restricted area so a preventative action will be taken such as, jamming and safe and force landing as shown in Figure 5.

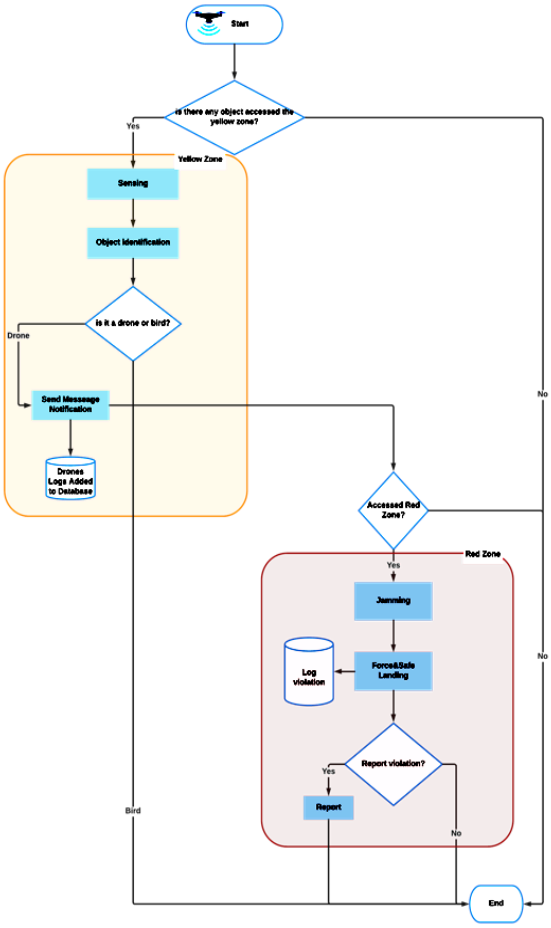

Figure 5 Accessing SafeZone system flow chart.

C. Design Consideration

- Hardware

A combination of passive radar and radio frequency sensors connected to the centralized system, in addition to, a drone. Table 3, illustrates the quantity and a little description for each hardware needed.

Table 3 Hardware Details

No.	Component	Quantity	Description
1	Passive Radar	1-3	Range = 150 Km
2	Radio Frequency	3-4	The covered frequencies = 915 MHz, 433 MHz, 2.4 GHz, 5.8 GHz
3	Drone	1	Small/Medium size

- Software

The software used is implemented using the Java object-oriented programming language. MySQL workbench program tool would be used to design the architecture of the required database.

IV. CONCLUSION

This section concludes what was previously stated about SafeZone system, by mentioning the findings and contributions; which focuses on the system outcomes and how it helps in protecting the privacy against intruding drones, and it points out the recommendations for future works.

A. Findings and Contributions

After the conduction of comparison and research, it was found that all existing solutions don't include the combination of detection and prevention in their proposed solutions. Moreover, most existing prevention methods depend on living creatures, which isn't effective in all conditions. It was found that the combination of passive radars and RF sensors is the most significant solution that matches the optimal requirements.

This project contributes to protecting the privacy of small to medium entities. The solution provides the entities of constant detection and prevention against intruding drones, which will help in keeping the entity's privacy and security under control. Moreover, the cost of implementing the solution is reasonable for small to mid-sized entities which would help them to secure themselves within a limited budget. Finally, the solution helps some countries that ban the use of drones, to consider allowing the use of drones since there would be constant monitoring and protection of privacy against unwanted drones.

B. Recommendations For Future Works

As a continuation of this project, the implementation phase is left for future work, and it is recommended that the encryption of communication between drones and pilots is implemented; since the communication is easily intercepted and lacks encryption mechanisms. In addition, it is suggested as a future that the system covers a wider range so that it includes the detection and prevention for large entities.

REFERENCES

[1] P. Blank, S. Kirrane and S. Spiekermann, "Privacy-Aware Restricted Areas for Unmanned Aerial Systems," in *IEEE Security & Privacy*, 2018.

[2] B. Canis, "Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry," in *Congressional Research Service*, 2015.

[3] B. Rao, A. G. Gopi and R. Maione, "The societal impact of commercial drones," *Technology in Society*, vol. 45, pp. 83-90, 2016.

[4] V. Dey, V. Pudi, A. Chattopadhyay and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, Pune, India, 2018.

[5] R. Creutzburg, J. Pleban and R. Band, "Investigations for improving the security of a toy," in *The*

International Society for Optical Engineering, Brandenburg, 2014.

[6] Nutaq, "Active vs. Passive Radar," [Online]. Available: https://www.nutaq.com/blog/active-vs-passive-radar. [Accessed 20 Oct 2018].

[7] H. You, X. Jianjuan and G. Xin, Radar Data Processing With Applications, wily, 2016.

[8] J. S. Patel, F. Fioranelli and D. Anderson, "Review of radar classification and RCS characterisation techniques for small UAVs or drones," *IET Radar, Sonar & Navigation*, vol. 12, no. 9, pp. 911-919, 2018.

[9] A. Rozantsev, V. Lepetit and P. Fua, "Detecting Flying Objects Using a Single Moving Camera," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2017.

[10] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68-74, 2018.

[11] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu and D. Matolak, "Detection, Tracking, and Interdiction for Amateur Drones," *IEEE Communications Magazine*, vol. 56, no. 4, p. 2018, 2018.

[12] M. Nijim and N. Mantrawadi, "Drone classification and identification system by phenome analysis using data mining techniques," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 2016.

[13] J. Mezei, V. Fiaska and A. Molnar, "Drone Sound Detection," in *16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI)*, 2015.

[14] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han and T. Vu, "Cost-Effective and Passive RF-Based Drone Presence Detection and Characterization," *Mobile Computing and Communications*, vol. 21, no. 4, pp. 30 - 34, 2018.

[15] A. D. Chadwick, "Micro-Drone Detection using Software-Defined 3G Passive Radar," in *International Conference on Radar Systems (Radar 2017)*, 2017.

[16] "DRONESHIELD," 2018. [Online]. Available: https://www.droneshield.com/dronegun-tactical/.. [Accessed 2 Dec 2018].

[17] M. Dursun and İ. Çuhadar, "Unmanned Air Vehicle System's Data Links.," vol. 4, no. 3, pp. 189-193, 2016.

[18] C. Pauner, I. Kamara and J. Viguri, "Drones. Current challenges and standardisation solutions in the field of privacy and data protection," in *Trust in the Information Society*, 2015.