5-1-2014

A Light-Weight Real-Time Privacy Protection Scheme for Video Surveillance by Unmanned Aircraft Systems

Surendra Shrestha
University of Nevada, Las Vegas

A LIGHT-WEIGHT REAL-TIME PRIVACY PROTECTION SCHEME FOR VIDEO SURVEILLANCE BY UNMANNED AIRCRAFT SYSTEMS

by

Surendra Shrestha

Bachelor of Technology (B.Tech.)
IEC College of Engineering and Technology
Uttar Pradesh Technical University, India
2008

A thesis submitted in partial fulfillment of
the requirements for the

Master of Science in Computer Science

Department of Computer Science
Howard R. Hughes College of Engineering
The Graduate College

University of Nevada, Las Vegas
May 2014

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

THE GRADUATE COLLEGE

We recommend the thesis prepared under our supervision by

Surendra Shrestha

entitled

A Light-Weight Real-Time Privacy Protection Scheme for Video Surveillance by Unmanned Aircraft Systems

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science

Department of Computer Science

Yoohwan Kim, Ph.D., Committee Chair

Laxmi Gewali, Ph.D., Committee Member

Ajoy Datta, Ph.D., Committee Member

Pramen Shrestha, Ph.D., Graduate College Representative

Kathryn Hausbeck Korgan, Ph.D., Interim Dean of the Graduate College

May 2014

Abstract

Unmanned Aircraft Systems (UAS) have raised a great concern on privacy recently. A practical method to protect privacy is needed for adopting UAS in civilian airspace. This thesis examines the privacy policies, filtering strategies, existing techniques, then proposes a new method based on encrypted video stream and cloud-based privacy servers. In this scheme, all video surveillance images are initially encrypted, then delivered to a privacy server. The privacy server decrypts the video using the shared key with the camera, and filters the image according to the privacy policy specified for the surveyed region. The sanitized video is delivered to the surveillance operator and anyone on the Internet who is authorized. In a larger system composed of multiple cameras and multiple privacy servers, the keys can be distributed using Kerberos protocol.

With this method the privacy policy can be changed on demand in real-time and there is no need for a costly on-board processing unit. By utilizing cloud-based servers, advanced image processing algorithms and new filtering algorithms can be applied immediately without camera software upgrade. This method is cost-efficient and promotes video sharing among multiple subscribers, thus it can spur wider adoption.

Acknowledgements

First and foremost I express my deepest gratitude to my advisor, Dr. Yoohwan Kim for his excellent guidance and assistance throughout my thesis. Without his ideas, advices and persistent help, this thesis would not have been possible.

I would also like to thank Dr. Laxmi P. Gewali, Dr. Ajoy K. Datta and Dr. Pramen P. Shrestha for their invaluable support. It is an honour to have them in my thesis committee. I am grateful to my parents for their warm support in every phase of my life. Lastly, my greatest appreciation goes to Binita Shakya for her untiring encouragement and motivation to complete my thesis.

Surendra Shrestha

University of Nevada, Las Vegas
May 2014

Table of Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION TO UAS

An Unmanned Aircraft (UA) can be simply defined as an aircraft without a human pilot on-board [1]. It is controlled either autonomously through the computer systems on the aircraft or by a human operator with a remote control outside the aircraft. It is also known by many other names including "drones", "Unmanned Aerial Vehicles (UAV)", "Remotely Piloted Vehicles (RPV)" and "Radio Control (R/C) aircraft". For a successful operation of an unmanned aircraft, an integration of a number of other systems are required. An Unmanned Aircraft System (UAS) is a system comprising of the UA and any other elements that are essential for the safe operation of the UA. These elements include control stations, communication data link, payloads, launch and recovery elements and the human element [2]. Figure 1.1 shows the combination of all the elements to create an UAS.

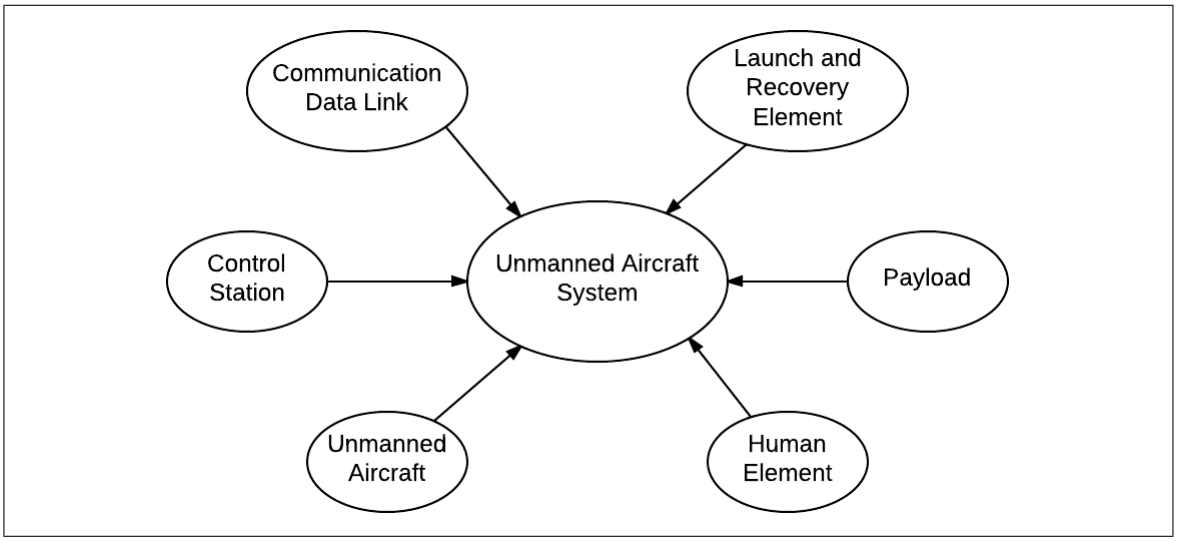

Figure 1.1: Elements of an Unmanned Aircraft System

1.1 Brief History

The concept of unmanned flight was first hypothesized by Nikola Tesla in the 1890s. Tesla shared his concept of remote-controlled torpedoes with Elmer Sperry. In October 1917, US Navy granted Sperry the first military contract for an unmanned flight system to develop an aerial torpedo. Sperry developed six test aircrafts for the US Navy, however, the aircraft could not fulfill its purpose fully though the models were launched successfully. The research on these aerial torpedoes were conducted until 1926 under Sperry. A modified N9 Navy seaplane was the first successful unmanned airplane to be flown by a radio remote control in September 1924 [3][4].

The US Army started its research on unmanned flight in 1918. In January 1918, Charles Kettering constructed a prototype UAV known as the "Bug" for the Army. The Army ordered around 100 Bugs, but before they could be used, the war had already ended. [4]. The invention of UAV started with its use in the battlefield and later it became an important tool for the US Army. The testing for UAVs started at the end of the World War I, and the Second World War embarked a milestone for its development. More than 15000 drones were built during that period for U.S. Military. The British conducted an initial test of UAVs in water and later in the deserts of Iraq. In 1942, US Navy conducted the test of UAVs that could carry weapons. During the 1940s, the UAVs were more popularly known as drones [5].

In 1955, the Army started using UAVs for military observations to locate an enemy. The development of High-altitude long-endurance (HALE) aerial vehicles started in 1968. The military UAS technology was continuously developed during the 1970s and the 1980s by the United States, Russia, Israel and some other European countries [6]. Only in 1990, Federal Aviation Administration approved the use of unmanned aircraft in national airspace for the first time [7]. The use of UAS flourished for military and civilian applications since 2000. With the development of more advanced technologies in computing, imaging and communication, the number of applications of UAS saw a huge growth after this period.

1.2 Classification of UAS

UAS can be classified based on the range or altitude in which they operate [8].

1.2.1 High Altitude Long Endurance (HALE)

They operate in high altitude of over 15,000 m and generally have endurance of more than 24 hours. These are mostly used in military operations which require long range reconnaissance and surveillance.

1.2.2 Medium Altitude Long Endurance (MALE)

They operate in between altitude of 5,000 m and 15,000 m and have endurance of about 24 hours. These UAS are also able to operate in ranges of more than 500 km.

1.2.3 Tactical UAV

These UAVs operate at an altitude of around 5,500 m and have a range between 100 km and 300 km.

1.2.4 Close Range UAV

These UAVs generally operate at a range of 100 km.

1.2.5 Mini UAV

They operate at a range of about 30 km and are mostly used for civilian applications.

1.2.6 Micro UAV

These are generally launched by hand and have a wingspan of about 150 mm. They are generally used for short range applications.

1.2.7 Nano UAV

These are tiny UAVs which are generally used in groups for very short range surveillance.

1.3 Applications of UAS

UAS have been used in a wide range of applications ranging from military to research and surveillance. The use of UAS in various fields have been ever increasing, though its potential in many fields is yet to be exploited and used to maximum [9]. Basically, their applications can be divided into 2 main categories [8].

1.3.1 Military Applications

UAS have a lot of applications in army, navy or air force. Some of its applications in these fields can be listed as:

- Relay radio signals
- Protect ports from attacks
- Enemy activity surveillance
- Locate and Destruct land mines
- Eliminate unexploded bombs

1.3.2 Civilian Applications

UAS can put into a large number of civilian applications, some of which are listed below:

- Aerial Photography
- Fire Detection and Control
- Crime Surveillance
- Crop Monitoring and Spraying
- Search and Rescue Operations

1.4 Advantages of UAS

UAS are designed to perform particular type of roles and they possess an advantage over manned aircraft in these roles. UAS are basically suited for these type of operations [8].

1.4.1 Dull Operations

Some military or civilian operations require hours of continuous surveillance which is not possible through manned aircraft. UAS are more effective in these type of dull operations as it is cheaper and the ground-based operators can also work in shifts.

1.4.2 Dirty Operations

Monitoring environments such as nuclear clouds or chemical contamination can be highly hazardous to human health. For these types of operations, UAS are safer and more effective to use.

1.4.3 Dangerous Operations

Military Operations like reconnaissance over enemy territory are very dangerous to human lives. Due to its smaller size and greater stealth, UAS are more suitable to use in these operations without risking any human lives. Other examples of dangerous operations are forest fire control, operating in extreme weather conditions, *etc.*

1.4.4 Covert Operations

UAS are highly suited for covert operations because of their small size and quietly operating capability. It is very difficult for enemy to detect these UAS.

1.4.5 Research Operations

UAS are used in aeronautical field to carry our tests for research purposes. Small UAS models of larger manned aircraft are used to test various operations under realistic conditions.

1.4.6 Economic Reasons

UAS are cheap to operate and maintain. Because of this, it can be used in many civilian applications like local surveillance or delivery of small packets.

Chapter 2

PRIVACY CONCERNS

Privacy is a relatively broad term and there is no single definition to accommodate its various dimensions. There are several types of privacy, including "privacy of person, privacy of thought and feelings, privacy of location and space, privacy of data and image, privacy of behavior (and action), privacy of communication, and privacy of association including group privacy" [10]. Privacy is a subjective concept and different people react differently to it. It also varies by society or by era or generation. A privacy-invading incident may be perfectly acceptable for some, but it may be totally unacceptable to others. This complexity requires a method to apply different types of privacy protection mechanisms rather than one uniform strategy.

Right to privacy is one of our fundamental rights. The surveillance in public places and even in private places has decreased the degree of freedom and liberty. With the new emerging technologies, the right to privacy and data protection has been an important concern [11]. The right to data protection can be defined as "the individual's right to exercise a significant measure of control over the collection, use, and disclosure of one's own personal information" [12].

2.1 Privacy Issues with UAS

One of the most useful applications of UAS is video surveillance. UAs can be equipped with powerful cameras that are able to take high-resolution pictures and videos of the geographic locations below [13]. R/C airplanes have raised some privacy concerns in the past. But their effect is generally limited for a few reasons. They fly under 400 feet with direct control under the operator within Line of Sight (LOS). Thus the operators are visible, and the attempt of privacy invasion can be easily spotted. UAs are much more capable than R/C airplanes, flying farther distance, possibly beyond line-of-sight (BLOS).

The surveillance image can be consumed by the surveillance operator, stored for later use, or broadcast on the Internet in real-time. This ability of the UAs has raised privacy concerns among the public [14][15][16]. For example, a UAS can take a video shot of people swimming in their back yard pool, or people in their home through the window as illustrated in Figure 2.1.

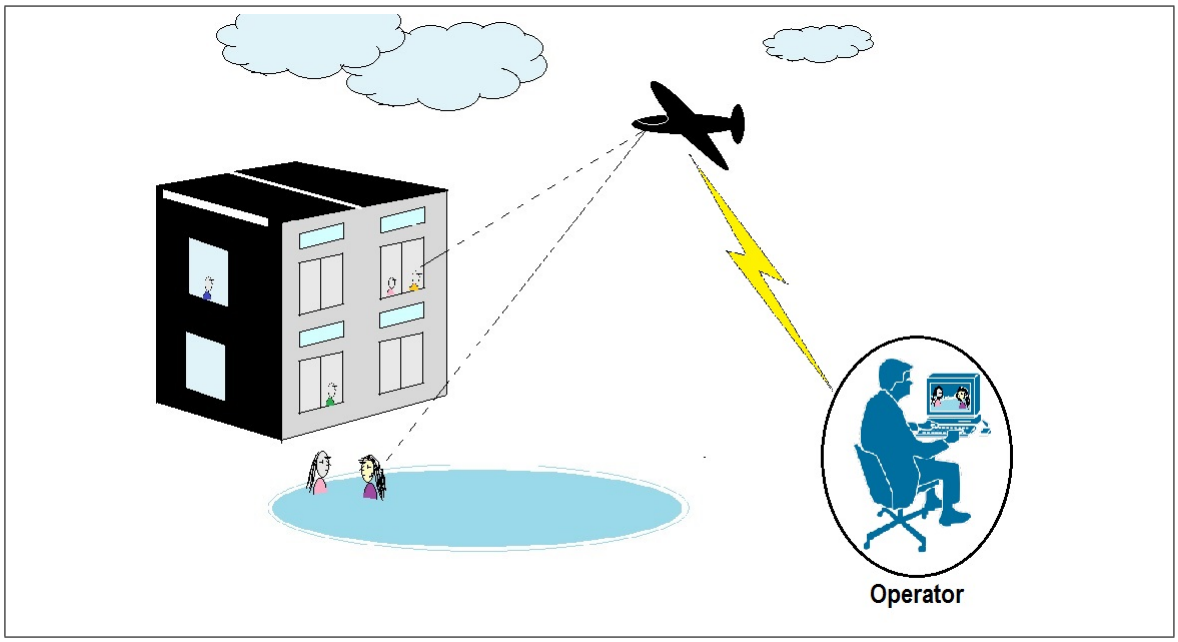

Figure 2.1: UAV Snooping

In particular, a video image streamed through the Internet in real-time can become available to millions of people instantly. Once the image is published on the Internet, there is no way to turn it back. Such inappropriate use of these technologies poses a serious threat to human rights for privacy and suggests a need for protection against these intrusions into privacy [17].

2.2 Need for Privacy

The wide use of UAS has ensured safety and security, but at the same time, privacy has been an important issue because of the surveillance from UAS. The regulations regarding the use of UAS should address these privacy concerns related with UAS. Many studies have analyzed the impact on privacy because of the use of UAS.

Cavoukian A. (2012) mentioned the necessity of addressing privacy while designing new technolo-

gies, including drones. The study emphasized that the privacy issues in drone technologies can be addressed by using "Privacy by Design (PbD)" framework. While using drones in public places, the public should be well informed prior to its use to maintain privacy of public. The camera and sensors in the drone should not collect information more than its required purpose [14].

Carr E. B. investigated privacy issues related with UAS and questioned Federal Aviation Administration (FAA) on three important issues of UAS, such as command and control of UAS, detection and recognition of other aircraft by UAS, and the privacy of individuals [6]. Villasenor J. also conducted study in the origin of drones, regulatory and privacy issues related with the use of drones [3].

Many research and studies have been conducted to identify privacy related issues aroused from emerging technologies [18]. Finn *et al.* (2013) examined the privacy impacts of new technologies. Among various types of privacy, UAS have impacted "privacy of behavior and action, privacy of data and image, privacy of location and space and privacy of association" [10].

In the recent years, the number of UAS being operated has risen greatly and is expected to rise further in the coming years [3]. With the high quality video surveillance cameras being used in the UAS to monitor the activities happening in the ground, the chance of inadvertent privacy invasion is increasing. Night operation poses a greater threat, as it is nearly impossible to locate a UAS at night due to its low visibility and silent operation, while it is now possible to view the night images in high definition with full color instead of gray IR video [19].

Video surveillance is not a new concept. We are already living in a world where we are constantly being watched [20]. There are CCTV cameras nearly in every public places, roads, campuses, bars, bus stations, office buildings, *etc.* This prevalence of CCTV image has actually helped to track down the suspects in Boston Marathon Bombing attack in 2013 [21]. There are Google Street View that is available to the general public, and numerous satellite images in search engines such as Google or Bing. However, all of those images are taken in public places and the chance of privacy violation is low. In case of Google street view, the images are not available in real-time, and it is carefully censored to blur the car plate numbers or people's faces. In case of those image providers, tracking the company violating the privacy law is not a problem, as it is readily available, in case there is any privacy-violating incident.

However, in case of UAS, the surveillance operator is not easily traceable. The video can go viral

instantly on the Internet as it happens, and worse, people responsible for this cannot be identified. This is a serious threat to general public, and a number of states have already created anti-UAS law reflecting the fear against the privacy invasion by UAS [22][23][24]. Without answering these concerns in a trusted manner, both from policy/legal and technical side, a wide adoption of UAS for civilian usage could be hampered.

Chapter 3

RELATED WORK

Although the privacy invasion is a serious threat from the UAS, there has been very few published works on this topic. This section discusses possible solutions that are being discussed informally in the research community.

3.1 Increasing visibility

One of the problems with UAS-based surveillance is that the public who is monitored is generally unaware of it because of it low visibility. They are small, and they generate very low noise [2]. By mandating a flashing light, and sound warning (*e.g.*, beeping), people can become aware of them. While taking video, additional warning may be given, like blinking red light similar to camcorder.

3.2 Geo-Fencing

Geo-fencing is a feature in a software program that uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries [25][26]. A geo-fence creates a virtual barrier so that a moving object cannot enter or exit across the virtual wall. A geo-fence can be a predefined set of boundaries, like school attendance zones or neighborhood boundaries, or it could be dynamically generated. Figure 3.1 shows an example of geo-fencing.

The virtual fence can be set up through the co-ordinates of the GPS positions forming a polygonal shape. A pre-defined location can be set up as the return point if the UAS crosses the boundary [27]. The geo-fencing concept is not new in airspace control. Airplanes may not enter a restricted airspace. The geo-fencing concept is now being applied to UAS in fine-grain [28].

However, the concept of geo-fencing may be too rigid for an efficient operation of UAS. Not all privacy-protected airspace is a restricted airspace. It may require unnecessary detour. If a surveillance region is surrounded by geo-fence, the region is not accessible even if it allows video surveillance.

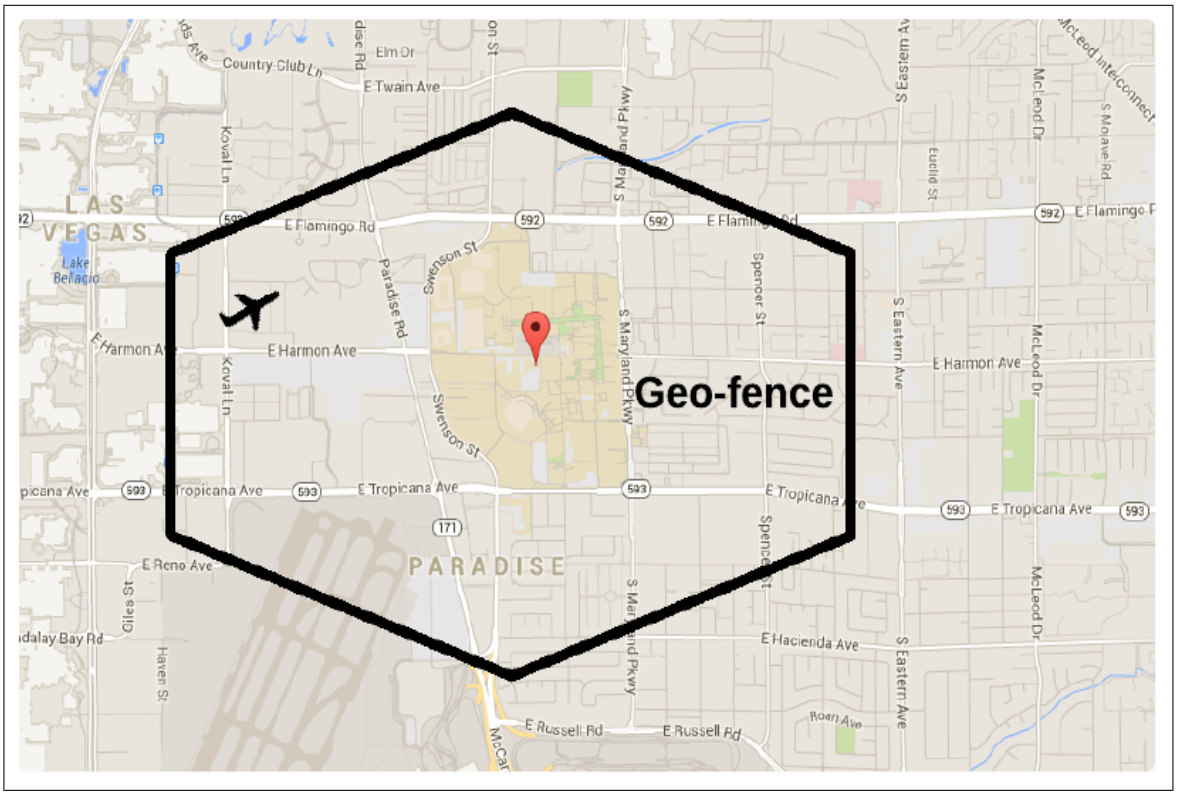

Figure 3.1: Geo-fencing

Therefore a softer alternative is desirable.

3.3 Blanking Technique

The blanking technique erases a certain portion of the video if the portion is privacy-protected. The camera and the on-board processing system determine whether the region is protected, and, if protected, blanks out the section of the video before transmitting the video to the ground station (Figure 3.2). So an accidental release of the privacy-protected video is prevented as the decision is made by the on-board processing unit before the surveillance operator can view it. This method requires an on-board processor with a pre-loaded privacy map of the surveyed geographical region. The privacy map contains detailed information about which region should be blanked out. Although blanking technique is currently the most intuitive and viable solution, there are some shortcomings.

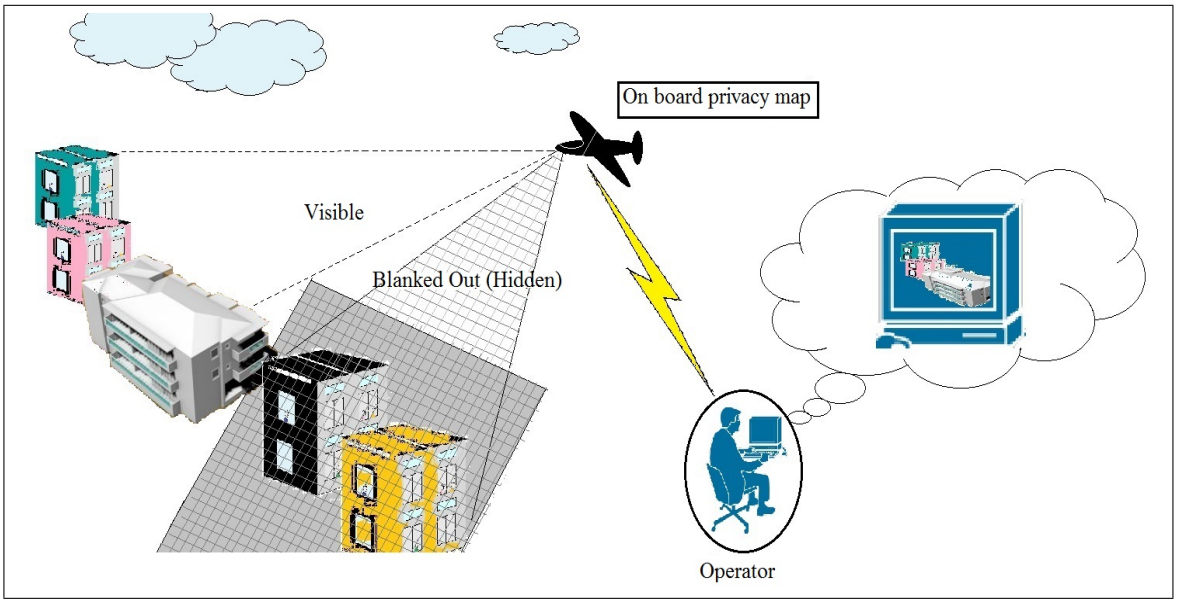

Figure 3.2: Blanking Technique

3.3.1 Need for an on-board map and processing system

This technique requires specialized maps and high-performance on-board computing system. While it is not impossible, there are some undesirable consequences. The need for larger memory and high-performance computing system increases the cost, which directly impacts the affordability of the system and slows the adoption rate. Furthermore, those added equipment consumes more power and reduce the battery life. The increased weight also reduces the speed, range, and flight duration of the UA.

3.3.2 Static privacy map

The on-board privacy map is static and not updated in real-time. It is a snapshot of the privacy requirements, and the map is frozen until next update. If a person spots a UAS flying and taking a video over his house, there is no way to stop it because on-demand request in real-time is not easily supported. Secondly, updating the map and on-board software is the responsibility of the UAS operator. But with a large UAS fleet, it takes significant time and effort to update the privacy maps and software in all UAs, and thus it may be neglected.

3.3.3 Non-compliant usage

Use of the blanking algorithm is purely voluntary. The operators can turn off the algorithm, and take the video freely in the private regions. It is difficult to check whether the algorithm is being

used as required or audit it afterwards. Even if an audit can be done afterwards, the video may have been already released to the public by the time it is audited. The lack of audit feature hurts not only the subjects being surveyed, but also the surveillance operator. If there is any criminal charge or lawsuit related to privacy against the operator, the operator needs to prove that the blanking algorithm was properly used. This feature may not be possible.

Chapter 4

PROPOSED SCHEME

The proposed scheme is a lightweight real-time privacy protection scheme with multiple levels of privacy. This scheme uses a cryptographic process to encrypt the video from the UAS and decrypt it at a trusted third party server. Since the privacy filtering operation is done in a powerful cloud-based server on the ground, the UAS doesn't need to carry sophisticated computing equipment as in blanking technique. The privacy detection algorithm, privacy map, filtering software can be upgraded separately from the camera system. Thus the same camera can be used for a longer period without upgrading.

4.1 Architecture

The architecture is shown in Figure 4.1. The video taken by the UAS is always encrypted. Then the surveillance operator's equipment receives it, but it cannot decrypt the video because it does not have the decryption key. It only relays the encrypted video to a privacy server.

The encrypted data is decrypted at a cloud-based privacy server, and analyzed based on the most up-to-date privacy policy. After the filtering operation, the sanitized video is sent to the surveillance operator. The privacy policy at the privacy server can be modified any time on demand. Any privacy requirements and violation can be monitored and enforced in real-time at the server.

4.2 Operating Procedure

Figure 4.2 shows the operating sequence and the various interaction between different participants of the system.

4.2.1 Camera certification and key assignment

The camera is equipped with a shared symmetric key with the privacy server. It is suggested that the key should be stored in a Trusted Platform Module (TPM) to avoid key theft. A TPM is a

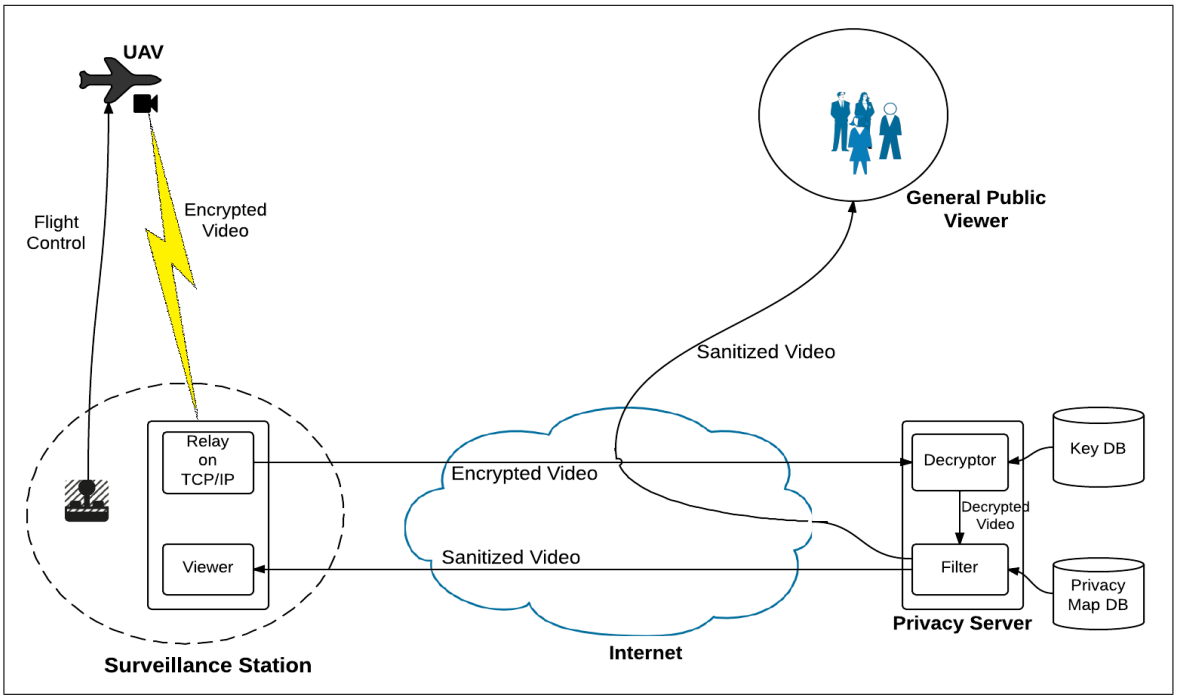

Figure 4.1: UAS Architecture

hardware device to store cryptographic information which provides higher security against external software attack and physical theft. The IP address of the privacy server(s) is pre-configured in the camera.

4.2.2 Camera owner registers the privacy service subscription with the Privacy Server (PS).

After purchasing the camera, the owner creates an account and registers the camera ID.

4.2.3 Key confirmation

Upon powering up, the camera looks for the privacy server and they confirm proper communication. The camera may operate in non-encryption mode before the connection with the server is made.

4.2.4 Privacy filtering

As the encrypted video image comes to the privacy server, the server decrypts it and looks up the privacy policy for the surveyed region. As well as static filtering based on the location, a dynamic filtering can be applied with image-processing algorithms or by human operator to filter out any inappropriate video scenes.

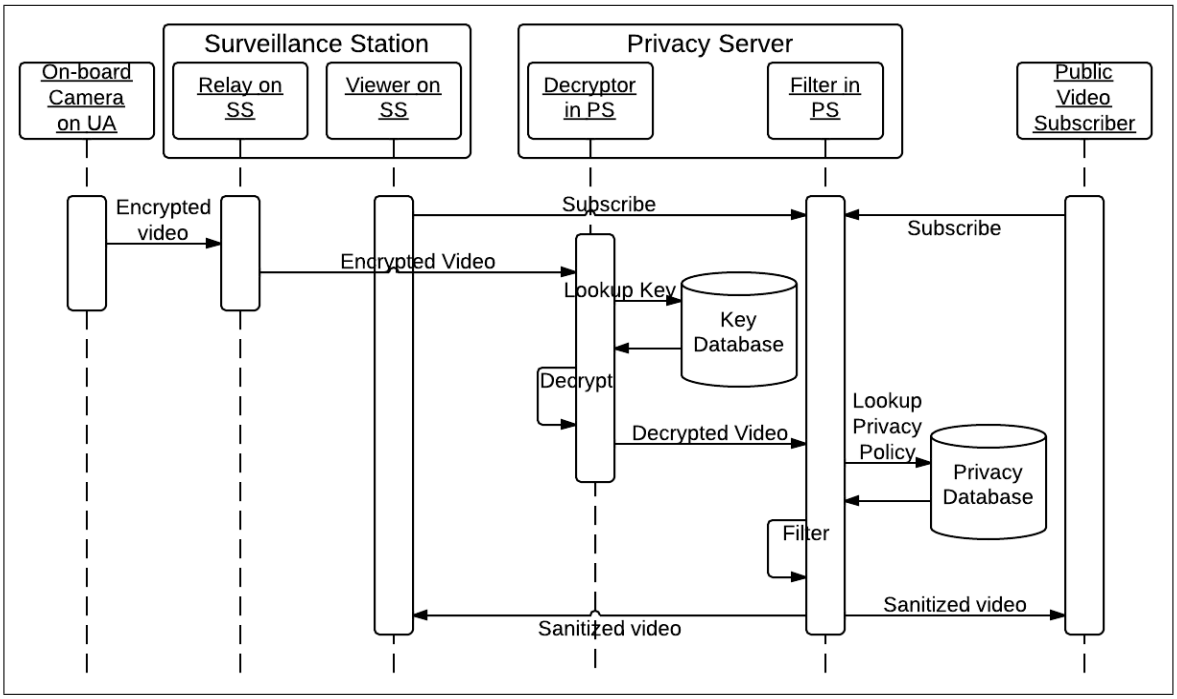

Figure 4.2: Interaction Among Participants

4.2.5 Sanitized video delivery

The resulting sanitized video is delivered to the surveillance operator or anybody with an authorization.

4.3 Cryptographic Scheme

The 3-tier model (camera, surveillance station, privacy server) may look similar to 802.11i protocol [29] where the Authenticator (access point) passes the message from the Supplicant (wireless client) to the Authentication server (RADIUS). However, there is a fundamental difference. The video stream from the UAS to the privacy server is a broadcast in essence. The privacy server doesn't need to authenticate any camera with hand-shaking sequence. The encrypted channel is already pre-established with the shared key. The camera doesn't need to authenticate the privacy server, either. If the camera contacts a wrong privacy server, the data cannot be decrypted as the keys do not match and thus privacy is not compromised. To explain the encryption process, different entities are denoted as following.

- Surveillance Station = SS
- Privacy Server = PS

There is no encryption between any entities at the data link layer.

- UAS → SS : Proprietary wireless channel (No encryption)
- SS → PS : Public Internet (No encryption)

The video stream is packetized and encrypted in the following format.

- V = [video data, sequence number, hash]

The sequence number identifies the video data from the UAS and the hash authenticates that the video is coming from the right source.

The encrypted video data is delivered from UAS to the PS via SS. The SS packages is within an IP packet, and sends it to the PS. SS is not part of the cryptographic process. It simply relays the encrypted video stream to PS.

K is the shared key between UAS and PS. The encrypted video is decrypted at PS with the help of the shared key and it is then filtered based on the privacy policy of the surveyed region. The resulting sanitized video (SV) is sent back to the SS.

- UAS → SS : {Camera ID | E (V, K)}
- SS → PS : {Camera ID | E (V, K)}
- PS : D (E(V, K)) = V,
  SV = Filter (V)
- PS → SS : {SV}

4.3.1 Data Encryption and Decryption

For the encryption, a simple block cipher mode with Advanced Encryption System (AES) is used. Currently AES is considered the strongest encryption algorithm. To use AES for stream cipher,

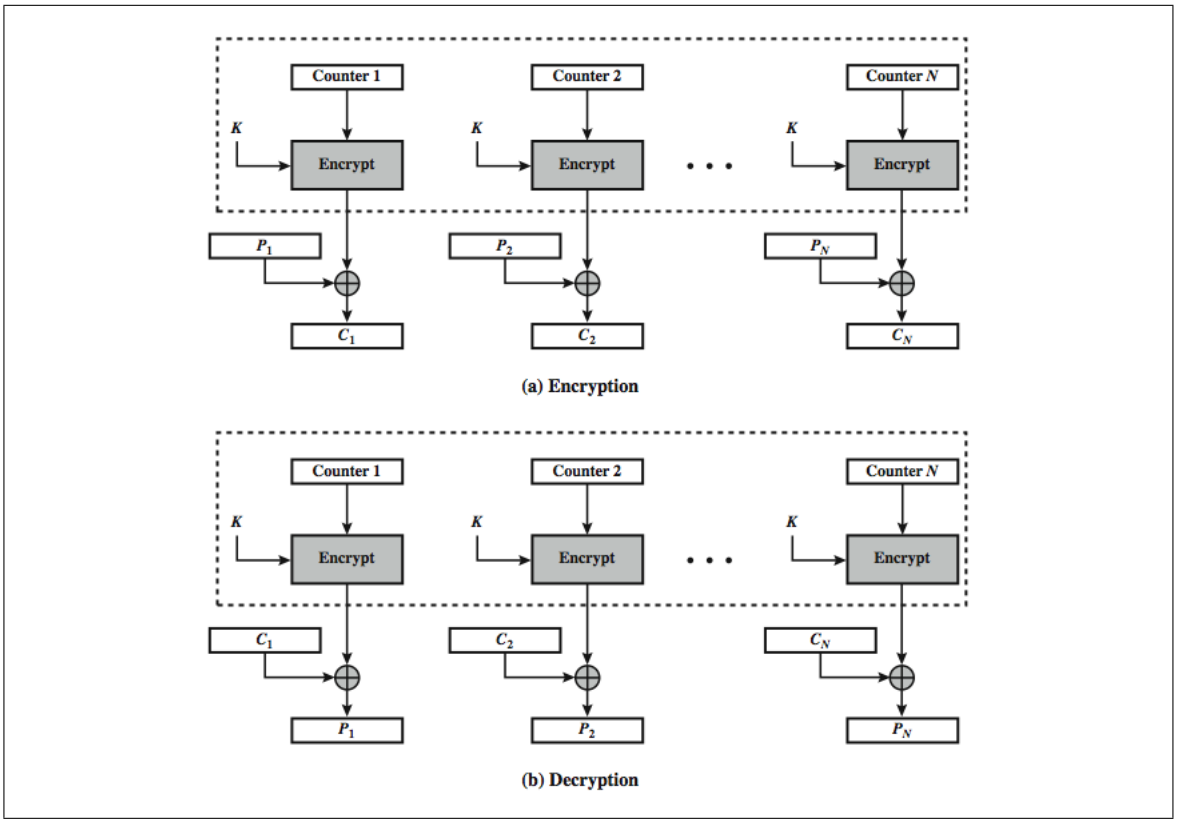

Figure 4.3: Block Cipher with CTR mode

Counter mode (CTR) is employed for its simplicity and efficiency. Counter mode works as illustrated in Figure 4.3 [29].

Counter mode turns a block cipher into a stream cipher. The counter is initialized to some value and the successive values are typically generated by incrementing the previous counter value by 1 (modulo 2^b, where b is the size of counter). Unlike other block cipher modes, the goal of the counter mode is to generate a random key stream to be used for stream cipher. This is achieved by encrypting successive values of the counter with the symmetric key. All plaintext inputs are Exclusive-ORed with this key stream to produce ciphertext. During decryption process, the same key stream is created and then Exclusive-ORed with the ciphertext to produce the plaintext.

The size of the counter value must be sufficiently large to avoid recycling because a reused counter value could be used for a cryptanalysis attack. A 48-bit value can be used for this purpose. Given the encryption block size of 128-bits (2^7 bits) and the bandwidth of a high definition video stream of, for example, 4 Mbps (2^{22} bits/sec), the video will generate 2^{15} ($= 2^{22}$ /2^7) blocks per second. In

other words, the counter value will repeat after 2^{33} seconds ($= 2^{48}\ /2^{15}$), which will take more than 100 years even if the video is continuously transmitted without stopping.

Chapter 5

TYPES OF DATA AND MULTI-LEVEL PRIVACY

UAS collects different types of data from various locations. For each type of data, there may be different requirements for privacy protection. For simplicity, the type of data is limited to video data. The video data input can be categorized into different levels and relevant privacy schemes may be applied. With this scheme, the public can fine-tune their privacy preference.

5.1 Navigation-Critical Data

The data is categorized into navigation-critical data and navigation-neutral data. It should be noted that navigation does not rely only on camera. In many cases, camera input is not used at all for navigation [30]. The Sense-and-Avoid (SAA) functions do not use camera. The See-and-Avoid function may use a camera, but it does not rely on a high-resolution camera like the surveillance camera. For collision avoidance and navigation, only the general shape of the object, color, or brightness levels are sufficient, thus low-resolution cameras may be sufficient.

5.2 Meta Data

Complete erasure of the video may be too limiting for the surveillance operation. Some level of summary data may be released to the surveillance operator or the general public. For example, the privacy-protected region may display a text output such as, "pool", "bedroom", "person sleeping on the grass", "person smoking", or "man urinating". High-quality meta data or summary data after filtering may improve the utility of the surveillance operation. Navigation-critical video data can also be transformed into a non-privacy invading forms, such as size, location, mobility, or meta data forms.

5.3 Levels of Privacy

The privacy requirements for video surveillance can be categorized as following. The default mode can be set as 5).

1. No video or meta data allowed
2. No video allowed
3. Mosaic image allowed
4. Low-resolution video allowed
5. High-definition video allowed

Figure 5.1 illustrates the varying levels of video quality.

Figure 5.1: Varying Levels of Privacy

In some cases, people feel annoyed when a UAS flies nearby in low altitude. They should be able to set the minimum distance from the location. For example,

1. More than 1000 feet
2. More than 500 feet
3. More than 100 feet
4. More than 50 feet
5. Landing allowed

The above rules can be applied only during a certain time period. Outside of this period, it could fall back to the default privacy level.

1. Applied at all times

2. Applied only at day time

3. Applied only at night time

4. Applied only in specific time or day

Table 5.1 shows a sample privacy policy database incorporating the multi-level privacy requirements.

Table 5.1: Sample Privacy Policy Database

Latitude	**Longitude**	**Address**	**Privacy Level**	**Distance**	**Time Period**	**Target Type**
X1 to X2	Y1 to Y2	234 Main St, Town, State	Low res video	>1000 feet	only at night time	Residence
X3 to X4	Y3 to Y4	987 Pool Ave, Town, State	Meta data	>500 feet	only at day time	Community pool
X5 to X6	Y5 to Y6	543 Some Rd, Town, State	No video	>100 feet	at all times	School play ground
X7 to X8	Y7 to Y8	775 What Ct, Town, State	Low res video	Landing allowed	only at day time	Park

Chapter 6

PRIVACY PROTECTION FILTERING

Within the privacy server, the filtering module performs a filtering operation according to the privacy database. The result of filtering may be blanking out the whole scene, blurring the scene, with mosaic images, or scaling down the resolution. This video transformation could be applied to the entire video image, or a small section in the video. There are three ways to apply the privacy policy as follows.

6.1 Static Filtering

The privacy server keeps the privacy protection levels based on the location and the municipal regulations. The UAS sends the information on camera's view such as,

- Current location of UAS
- Camera direction
- Distance to the object

The UAS may also report the flight direction, so that the privacy server can predict the privacy level change, and warn the UAS. Privacy server determines the camera's field of view and the resolution at the object. The resolution of the image at the target object should be determined in consideration of the distance. Figure 6.1 shows two cases where the video resolution can be equivalent. It looks up the privacy table, and applies necessary policy.

6.2 On-Demand Filtering

When a UAS is spotted taking video, a person concerned with his or her privacy may request not to take the picture, or change the privacy level. Figure 6.2 shows a mock up mobile web page to

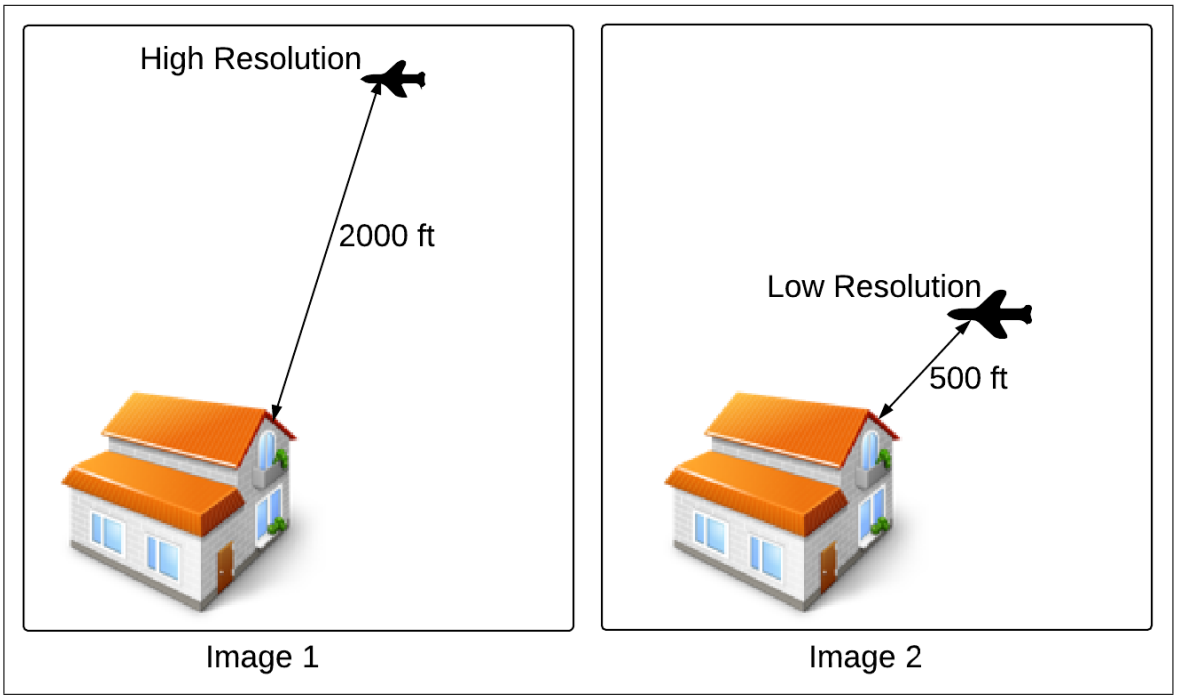

Figure 6.1: Equivalent Video Quality

request privacy protection.

6.3 Processed Filtering

The privacy server employs advanced image processing algorithm, and actively processes the image to search a scene that violates privacy even if it is not specified in the static privacy policy table. When it detects one, such as someone urinating against wall, it takes a relevant action such as, blurring the face of the person or replacing it with meta data.

Figure 6.2: Privacy Protection Request in Real Time

Chapter 7

GENERALIZED ARCHITECTURE

A single privacy server can not be used to communicate to all the UAS. Multiple privacy servers are needed to achieve this task. The simple camera-to-privacy server model needs to be extended to cover a large number of UAS and multiple privacy servers. A UAS should be able to connect to any available privacy server and communicate efficiently. Figure 7.1 describes the generalized architecture.

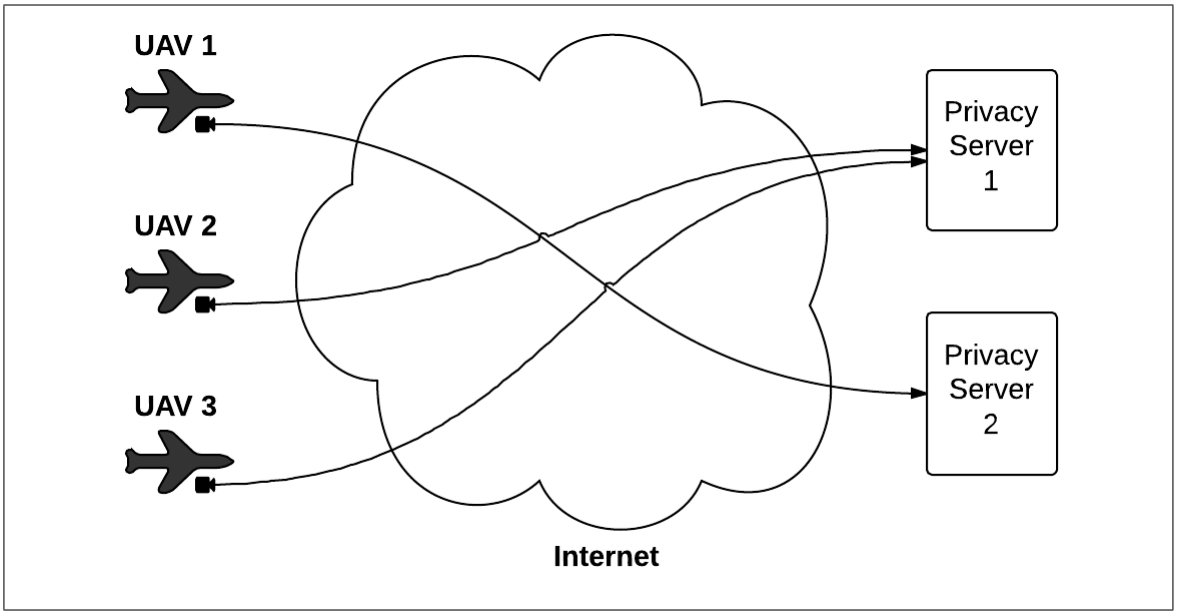

Figure 7.1: Generalized Architecture with Multiple Cameras and Privacy Servers

7.1 Encryption Key Distribution

Before starting the video surveillance operation, the camera and the privacy server need to share a key. Key management can be an issue because there are multiple servers and clients. It is

impractical for all the servers to keep the key information individually for thousands of cameras. Therefore Kerberos model can be used for this process which is a key distribution protocol that has been commonly used in network-based key distribution such as Microsoft Active Directory [29].

7.2 Kerberos

Kerberos is a service that is used for key distribution and user authentication between several clients and servers. Kerberos provides a centralized key distribution server whose function is to distribute session keys between the server and the client. It also authenticates the client to the server and vice-versa. Kerberos is based on symmetric key encryption and does not make use of public-key encryption.

The Kerberos Key Distribution Server is composed of two servers, an Authentication Server (AS) and a Ticket Granting Server (TGS). Initially all cameras register their key at AS, and the Privacy Servers register their key at the TGS as shown in Figure 7.2. The AS and the TGS also share a symmetric key among themselves. After the initialization, the registered keys are never used for data encryption, but used only for distributing the session keys.

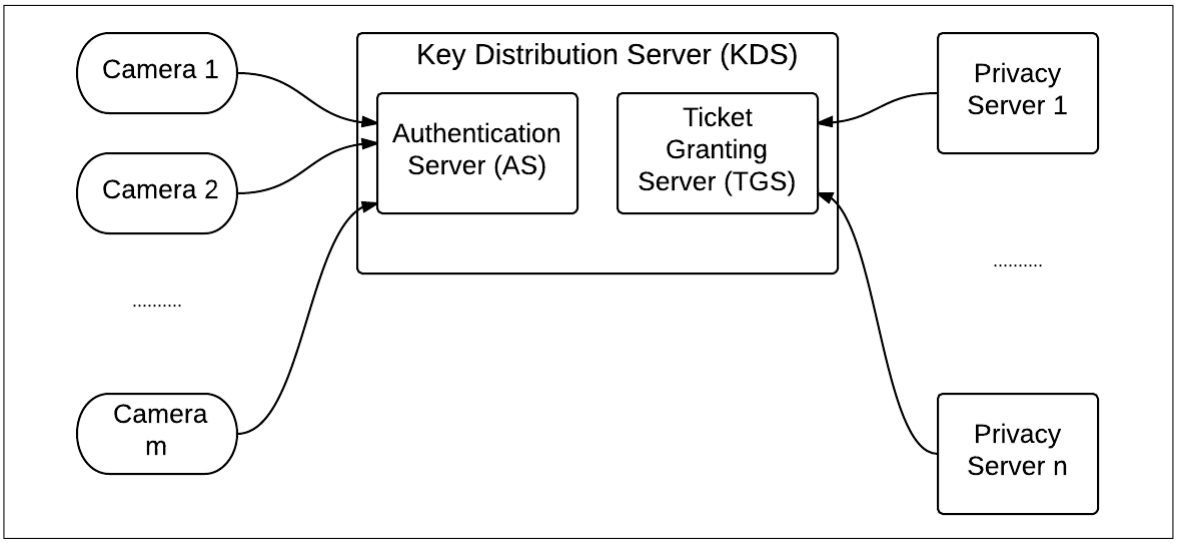

Figure 7.2: Key Registration at Kerberos

Before the camera can establish a secure connection with the privacy server, it needs to communicate with the AS and the TGS to generate session keys. Figure 7.3 illustrates the process of key distribution.

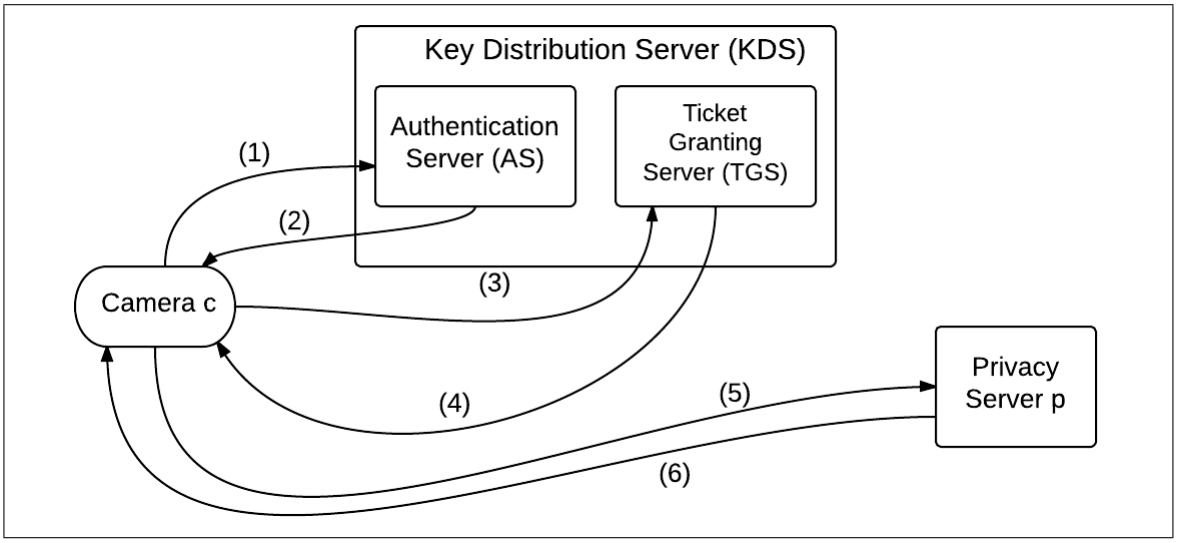

Figure 7.3: Key distribution in the field

- At the beginning of the surveillance operation, the camera contacts the AS as shown in step (1).
- In step (2), the AS sends a Ticket Granting Ticket (TGT) to the camera which is encrypted with the shared key between the AS and the TGS. The TGT contains a long-term session key to access the TGS. The camera cannot decrypt the TGT.
- In step (3), the camera sends this TGT to the TGS.
- After validating the TGT, the TGS sends a short-term key to the camera to access the desired privacy server in step (4). This key is also encrypted with the key shared between TGS and the privacy server, thus preventing the camera to decrypt it.
- The camera now contacts the privacy server with this key in step (5).
- The privacy server authenticates a proper connection in step (6).

If the particular privacy server is busy, the camera can ask for a new ticket for a different privacy server.

7.2.1 Exchange of Messages

Several messages are exchanged among the client (camera), AS, TGS and the server (PS) at different phases of the process before the client and the server can authenticate themselves to each other and

share a secret symmetric key. Table 7.1 shows the various messages exchanged during the process [29].

Table 7.1: Summary of Kerberos Message Exchanges

(1) C → AS	$ID_c \| ID_{tgs} \| TS_1$
(2) AS → C	$E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$
	$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain TGT

(3) C → TGS	$ID_v \| Ticket_{tgs} \| Authenticator_c$
(4) TGS → C	$E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$
	$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$
	$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$
	$Authenticator_c = E(K_{c,tgs}, [ID_c \| AD_c \| TS_3])$

(b) Ticket Granting Service Exchange to obtain Service Granting Ticket

(5) C → V	$Ticket_v \| Authenticator_c$
(6) V → C	$E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)
	$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$
	$Authenticator_c = E(K_{c,v}, [ID_c \| AD_c \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Following notations have been used in the table to describe the process.

C = Client (Camera)

AS = Authentication Server

TGS = Ticket Granting Server

V = Server (Privacy Server)

Table 7.1 is divided into 3 parts to differentiate the exchange of messages between {C and AS}, {C and TGS} and {C and V}. Following messages are exchanged during the process.

Message (1)

C sends a message to AS requesting access to the TGS. The message contains the client ID (ID_c), ticket granting server ID (ID_{tgs}) and a timestamp (TS_1). The timestamp allows AS to verify that the client's clock is synchronized with that of the AS.

Message (2)

AS responds back with a ticket-granting ticket that is encrypted with the key derived from the client's password (K_c). The encrypted message contains a copy of the session key for C and TGS ($K_{c,tgs}$), ticket granting server ID (ID_{tgs}), timestamp (TS_2), ticket lifetime ($Lifetime_2$) and the ticket to access the TGS ($Ticket_{tgs}$). The ticket ($Ticket_{tgs}$) is also encrypted with the key known to AS and the TGS (K_{tgs}) and contains the session key ($K_{c,tgs}$). This allows a secure delivery of the session key to both C and the TGS. The client ID (ID_c) and the network address (AD_c) are used to authenticate the ticket.

Message (3)

C, now has the session key and the ticket. With these information, C sends a message to the TGS that includes the ticket, requested server ID (ID_v) and the authenticator ($Authenticator_c$). The authenticator includes the client ID, client network address and a timestamp (TS_3) and is encrypted with the session key. The authenticator is intended to be used only once and has a very short lifetime.

Message (4)

The TGS can decrypt the ticket as it already knows the key (K_{tgs}). It also decrypts the authenticator with the help of the session key gained from the ticket. The TGS, then validates the client ID and the network address in the authenticator and the ticket to authenticate the client. Once the authentication is done, the TGS sends a service-granting ticket back to the client. The service-granting ticket is encrypted with the session key shared by C and the TGS. It includes a new session key to be shared between C and V ($K_{c,v}$), server ID (ID_v), timestamp (TS_4) and the ticket to access the server ($Ticket_v$). The ticket ($Ticket_v$) also contains the session key ($K_{c,v}$), client ID, client network ID, server ID, timestamp of the ticket and the lifetime of the ticket ($Lifetime_4$). This ticket is encrypted with the shared key between the TGS and the server (K_v).

Message (5)

C can decrypt the service-granting ticket with the session key ($K_{c,tgs}$) to get the ticket to access the server ($Ticket_v$). C sends the ticket ($Ticket_v$) and a new authenticator ($Authenticator_c$) to V. The authenticator is similar to the previous one except that it is encrypted with the new session key ($K_{c,v}$) and has a new timestamp (TS_5).

Message (6)

V can decrypt the ticket ($Ticket_v$) with its key (K_v) and gain access to the session key ($K_{c,v}$). It can also decrypt the authenticator with the help of this session key and validate the information in the ticket and the authenticator. If mutual authentication is required, V can send a message back to C with the timestamp (TS_5) incremented by 1. This message is encrypted with the session key ($K_{c,v}$). Since, this message is encrypted with the session key ($K_{c,v}$), C can be assured that it was created by V. The contents of the message confirm that it is not a replay of the authenticator.

Thus, by the end of this process, the client (camera) and the server (PS) share a secret key $K_{c,v}$. This key, itself, can be used to encrypt the video stream from the camera to the PS or it can be used to share a new key between the two.

7.3 Video Subscription Management

Independently from the encryption/decryption operation, it is necessary to decide who gets the sanitized video stream. The owner of the camera can manage the access rights. At the time of purchasing, he or she establishes the ownership and creates a management account. From this account, he or she can allow the IP address or particular users to get the video image. The owner's surveillance station shall be obviously the first allowed machine, but he or she can also allow other people to access the video.

Chapter 8

ADVANTAGES

This proposed scheme has a number of advantages over conventional blanking technique.

8.1 Flexible Privacy Policy

The privacy policy for the proposed scheme is applied on the ground, unlike the blanking technique. This feature gives an advantage in that the privacy policy can be modified in real-time when needed. Based on the privacy policy, multiple levels of privacy can be designed depending on the sensitivity of the region under surveillance.

8.2 Separation of Camera from Image Processing

The video image processing is done at a cloud-based server. So the owner of the camera does not need to worry about upgrading the camera software. Advanced image processing algorithms can be immediately employed without a camera software upgrade. Therefore, a relatively low cost camera can be used for a longer period. Also, by sharing the common privacy server among multiple camera owners, the cost for using the privacy server can become lower. This lowers the price of the system, which may increase the adoption rate.

8.3 Legal Protection

If a surveillance operator uses an approved camera, he or she is better protected from a legal problem because the compliance to the privacy policy is automatically ensured. Operators may prefer using a compliant camera to their own non-compliant camera. For government entities, this could be a great relief because they don't become liable for privacy invasion. It is similar to the car-mounted video camera in police cars where policemen can prove that they didn't do anything illegal while investigating an incident.

8.4 Supporting Forensic Investigation for Privacy Violation

Since the video stream is monitored and archived at the privacy server while it is taken, real-time compliance checking or auditing can be performed naturally. Upon any violation, the law enforcement can investigate the incidents with the logged data. The logging data types, logging process, and cryptographic verification process will have to be developed.

8.5 Availability of the Video Streaming to a Larger Audience

With the cloud-based privacy server model, video sharing becomes a natural built-in feature. It allows real-time video sharing over the Internet with whoever is authorized to watch. For example, in a kids' soccer game, one person may fly a UAS taking video, and the video is fed to the privacy server. The operator gives the account information to the parents who are watching the game, and they all can watch the aerial footage without a hassle. Any unsuitable scene for young children or private scene can be filtered out in real-time, so the whole family can enjoy the video. This video can also be saved at the privacy server so that people can watch it later.

Chapter 9

DISCUSSIONS

9.1 Need for Internet Connectivity

The greatest shortcoming with the proposed scheme is the need for constant Internet connection. With the prevalence of the wireless Internet coverage, this shouldn't be an issue normally. However, in remote places where no wireless Internet is available, a backup method is needed. A mobile privacy server can take a snapshot of the current privacy policy in the surveyed region, and sanitize the video on the spot. This may work because there is probably less privacy concern in remote places and the privacy policy is less frequently updated.

9.2 Denial of Service attack

A hostile entity may flood the privacy server with a large amount of traffic to create a Denial-of-Service condition [29]. Any server on the Internet is vulnerable to this attack, and the privacy server is no exception. Many techniques have been developed to thwart them and can be used to prevent this attack.

Chapter 10

CONCLUSION AND FUTURE WORK

UAS are the future of aviation. They can be used in a variety of civilian applications that are beneficial to the government and the public. The number of UAS flying in the air is going to rise enormously in the coming years. However, like any other technology, it can be misused to cause potential harm to the public. The biggest threat from using these UAS into civilian applications is regarding the potential impact they can have on privacy. These threats need to be neutralized if we want to successfully integrate UAS into the civilian airspace.

In this thesis, various privacy policies, protection strategies, and technical solution for UAS-based video surveillance were reviewed. Blanking technique with an on-board processing unit is currently the most viable solution, but the high cost and the need for upgrading the privacy map and software could slow its adoption. An alternative privacy-protection method with lower cost of implementation was proposed as a solution. In this scheme, all video surveillance images are initially encrypted, then delivered to a cloud-based privacy server through a surveillance station. The surveillance camera and the privacy server share a common key that is used for encryption and decryption. The privacy server decrypts the video using the shared key with the camera, and filters the video according to the privacy policy for the target region. The sanitized video is sent back to the surveillance station for further processing. This scheme can be extended to accommodate a larger system composed of multiple cameras and multiple privacy servers. The key distribution problem can be solved using Kerberos protocol.

Multiple privacy levels and different filtering strategies can also be handled through this method. It has several advantages including lower system cost, applicability of advanced image processing algorithms, legal protection for the UAS operators, and real-time streaming video availability to general public on the Internet, all of which may promote a wide adoption.

As future work, advanced filtering algorithms that are better suited for the privacy policies can be

developed to filter out unnecessary data from the decrypted video without the help of a human operator. An implementation plan can be developed to test this scheme in a real life environment. All the privacy protection and monitoring algorithms need to be implemented and tested in different environments like in the lab and on the ground with mobile units.

Bibliography

[1] F. A. A. U.S. Department of Transportation, "Integration of civil unmanned aircraft systems (uas) in the national airspace system (nas) roadmap," 2013.

[2] R. K. Barnhart, S. B. Hottman, D. M. Marshall, E. Shappee, *et al.*, *Introduction to unmanned aircraft systems*. CRC Press, 2012.

[3] J. Villasenor, "Privacy, security, and human dignity in the digital age: observations from above: unmanned aircraft systems and privacy," *Harv. JL & Pub. Pol'y*, vol. 36, pp. 457–915, 2013.

[4] J. D. Blom, *Unmanned Aerial Systems: A Historical Perspective*, vol. 45. Combat Studies Institute Press, 2010.

[5] J. M. Sullivan, "Revolution or evolution? the rise of the uavs," in *Technology and Society, 2005. Weapons and Wires: Prevention and Safety in a Time of Fear. ISTAS 2005. Proceedings. 2005 International Symposium on*, pp. 94–101, IEEE, 2005.

[6] E. B. Carr, "Unmanned aerial vehicles: Examining the safety, security, privacy and regulatory issues of integration into u.s. airspace," pp. 1–30.

[7] A. Roberts, "By the numbers: Drones." `http://www.cnn.com/2013/04/05/politics/drones-btn`, May 2013.

[8] R. Austin, *Unmanned aircraft systems: UAVS design, development and deployment*, vol. 54. John Wiley & Sons, 2011.

[9] K. Dalamagkidis, K. P. Valavanis, and L. A. Piegl, *On integrating unmanned aircraft systems into the national airspace system*. Springer, 2009.

[10] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European data protection: coming of age*, pp. 3–32, Springer, 2013.

[11] R. Gellert and S. Gutwirth, "The legal construction of privacy and data protection," *Computer Law & Security Review*, vol. 29, no. 5, pp. 522–530, 2013.

[12] A. Cavoukian, "Surveillance, then and now: Securing privacy in public spaces," tech. rep., Technical Report. 64 pages, 2013.

[13] K. Dalamagkidis, K. P. Valavanis, and L. A. Piegl, "Current status and future perspectives for unmanned aircraft system operations in the us," *Journal of Intelligent and Robotic Systems*, vol. 52, no. 2, pp. 313–329, 2008.

[14] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," pp. 1–39, Aug. 2012.

[15] D. A. Divis, "Uav operations in national air space advance as privacy fight heats up." `http://www.insidegnss.com/node/3687`.

[16] H. A. International, "Concerns over uav privacy issues continue." http://www.rotor.com/Publications/RotorNews/tabid/843/articleType/ArticleView/articleId/2281/Concerns-over-UAV-Privacy-Issues-Continue.aspx, April 2013.

[17] E. P. I. Center, "Domestic unmanned aerial vehicles (uavs) and drones." http://epic.org/privacy/drones.

[18] S. Gutwirth and M. Friedewald, "Emergent technologies and the transformations of privacy and data protection," *Computer Law & Security Review*, vol. 29, no. 5, pp. 477–479, 2013.

[19] A. Communication. http://www.axis.com.

[20] B. Security, "Cctv security systems explained." http://www.brickhousesecurity.com/category/video+surveillance+security+cameras/about+cctv+cameras.do.

[21] "Cctv: suspects in boston marathon bombings." http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10004981/CCTV-suspects-in-Boston-Marathon-bombings.html, April 2013.

[22] J. Stanley and C. Crump, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft: Report*. American Civil Liberties Union, 2011.

[23] J. Villasenior, "Will drones outflank the fourth amendment?." http://www.forbes.com/sites/johnvillasenor/2012/09/20/will-drones-outflank-the-fourth-amendment, September 2012.

[24] C. Somodevilla, "Lawmakers voice concerns on drone privacy questions." http://nbcpolitics.nbcnews.com/_news/2013/03/20/17389193-lawmakers-voice-concerns-on-drone-privacy-questions?lite, March 2013.

[25] H. Rahimi, A. Nur Zincir-Heywood, and B. Gadher, "Indoor geo-fencing and access control for wireless networks," in *Computational Intelligence in Cyber Security (CICS), 2013 IEEE Symposium on*, pp. 1–8, IEEE, 2013.

[26] F. Reclus and K. Drouard, "Geofencing for fleet & freight management," in *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, pp. 353–356, IEEE, 2009.

[27] A. Plane, "Geofencing." http://plane.ardupilot.com/wiki/geofencing-3/.

[28] A. Antonopoulos, "Geo-fencing for arducopter - keep your copter "fenced in"." http://diydrones.com/profiles/blogs/geo-fencing-for-arducopter-keep-your-copter-fenced-in, April 2012.

[29] W. Stallings, *Network Security Essentials: Applications and Standards*. Prentice Hall, 2011.

[30] P. Angelov, *Sense and Avoid in UAS: Research and Applications*. John Wiley & Sons, 2012.

Vita

Graduate College
University of Nevada, Las Vegas

Surendra Shrestha

Degree:

Bachelor of Technology in Computer Science 2008
IEC College of Engineering and Technology
Uttar Pradesh Technical University

Thesis Title:

A Light-Weight Real-Time Privacy Protection Scheme for Video Surveillance by Unmanned Aircraft Systems

Thesis Examination Committee:

Chairperson, Dr. Yoohwan Kim, Ph.D.
Committee Member, Dr. Laxmi P. Gewali, Ph.D.
Committee Member, Dr. Ajoy K. Datta, Ph.D.
Graduate Faculty Representative, Dr. Pramen Shrestha, Ph.D.