5-2015

This thesis is submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology Management

Farhan Mohammed

United Arab Emirates University

College of Information Technology

E-Commerce Track

EFFICIENT DATA COMMUNICATION IN UNMANNED AERIAL VEHICLES

Farhan Mohammed

This thesis is submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology Management

Under the Supervision of Dr. Imad Jawhar

May 2015

Declaration of original work

I, Farhan Mohammed, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Efficient Data Communication in Unmanned Aerial Vehicles*", hereby, solemnly declare that this thesis is an original research work that has been done and prepared by me under the supervision of Dr. Imad Jawhar, in the College of Information Technology at UAEU. This work has not been previously formed as the basis for the award of any academic degree, diploma or a similar title at this or any other university. The materials borrowed from other sources and included in my thesis have been properly cited and acknowledged.

Student's Signature____________________________ Date _______________

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Dr. Imad Jawhar
   Title: Associate Professor
   Department of Networking
   College of Information Technology

   Signature ______________________________ Date _______________

2) Member: Dr. Nader Mohamed
   Title: Associate Professor
   Department of Networking
   College of Information Technology

   Signature ______________________________ Date _______________

3) Member (External Examiner): Dr. Amjad Gawanmeh
   Title: Assistant Professor
   Department of Electrical and Computer Engineering
   Institution: Khalifa University of Science, Technology and Research

   Signature ______________________________ Date _______________

This Master Thesis is accepted by:

Dean of the College of Information Technology: Dr. Shayma Al Kobaisi

Signature ______________________________ Date ____________________

Dean of the College of the Graduate Studies: Professor Nagi T. Wakim

Signature ______________________________ Date ____________________

Copy ____ of ____

Abstract

A large number of recent advancements in the technology of Unmanned Aerial Vehicles (UAVs) have enabled them to be very useful and effective in many applications in today's society. They demonstrate a high degree of stability and agility in the air. A few years ago military applications were the main driving force behind the development of UAVs and UAV systems. Many of their applications included monitoring, surveillance, data transmission and communication. Recently, several opportunities have emerged and participated in driving the development of UAV technology further ahead. Such opportunities include integration of UAVs with smart cities, disaster recovery, military and commercial surveillance, environmental monitoring, and emergency response. In order for UAVs to perform their various tasks and responsibilities effectively, UAV communication becomes an important component. Furthermore, such communication must be done using trusted strategies and protocols so that the related missions and services are not attacked or compromised in intentional or un-intentional manners. On the other hand, Mobile Ad hoc Networks (MANETs) are a collection of autonomous nodes with a dynamic topology. They provide the potential for autonomous group organizations with extended communication capabilities in several operations. UAVs and MANETs share many common characteristics. Consequently, a group of flying UAVs can be considered a MANET where the individual UAVs are modeled as nodes.

The main contributions provided in this thesis are the following: (1) characterization of different UAV-based networking architectures, (2) identification of the characteristics and issues in MANET protocols that lead to efficient UAV-based communication, (3) classification of different data traffic types and requirements for efficient UAV-based communication in various applications and environments, (4) classification of the different trust-based protocols and schemes that can be adopted by UAVs, (5) comparison of the communication requirements between military and commercial applications, (6) classification of trust protocols and schemes for various UAV applications, and (7) providing a case study on UAVs and their applications in Smart Cities.

Keywords: Unmanned Aerial Vehicles, Mobile Ad hoc Networks, communication, trust, trust management, smart cities.

Title and Abstract (in Arabic)

بيانات الاتصال الفعال في المركبات الجوية بدون طيار

الملخص

عددا كبيرا من التطورات الأخيرة في تكنولوجيا طائرات بدون طيار (UAV) لها أن تكون مفيدة جدا وفعالة في العديد من التطبيقات في مجتمع اليوم. وهي تعبر عن درجة عالية من الاستقرار وخفة الحركة في الهواء. وكانت قبل بضعة سنوات التطبيقات العسكرية القوة الدافعة الرئيسية وراء تطوير الطائرات بدون طيار وأنظمة الطائرات بدون طيار. شملت العديد من التطبيقات الخاصة بهم الرصد والمراقبة، ونقل البيانات والاتصالات. في الآونة الأخيرة، ظهرت العديد من الفرص في تطوير تكنولوجيا الطائرات بدون طيار. فرص مثل تكامل الطائرات بدون طيار مع المدن الذكية، والتعافي من الكوارث، المراقبة العسكرية والتجارية، والرصد البيئي، والاستجابة للطوارئ. من أجل الطائرات بدون طيار لأداء مختلف المهام والمسؤوليات على نحو فعال، يصبح التواصل الطائرات بدون طيار عنصرا هاما. وعلاوة على ذلك، ويجب أن يتم هذا الاتصال باستخدام استراتيجيات والبروتوكولات موثوق بحيث البعثات والخدمات ذات الصلة ليست هاجم أو الانتقاص المتعمد في الأدب غير العمدية. من ناحية أخرى، الشبكات المخصصة للموبايلات (MANET) هي عبارة عن مجموعة من العقد مستقلة مع طوبولوجيا الحيوية. أنها توفر إمكانية للمنظمات مجموعة مستقلة مع قدرات الاتصالات طويلة في العديد من العمليات. UAV وMANET تشترك في العديد من الخصائص المشابهة. ونتيجة لذلك، يمكن اعتبار مجموعة من الطائرات بدون طيار تحلق MANET حيث غرار الطائرات بدون طيار الفردية والعقد.

المساهمات الرئيسية المقدمة في هذه الدرسة هي التلاية (1) :توصيف مختلف أبنية الربط الشبكي القائم على الطائرات بدون طيار، (2) تحديد الخصائص والقضايا في MANET بروتوكولات لتوفير كفاءة الاتصالات القائمة على الطائرات بدون طيار، (3) تصنيف مختلف أنواع حركة مرور البيانات للاتصال القائم على الطائرات بدون طيار الفعالة في مختلف التطبيقات والبيئات، (4) تصنيف البروتوكولات الثقة المختلفة والمخططات التي يمكن اعتمادها من قبل الطائرات بدون طيار، (5) مقارنة بين متطلبات التواصل بين التطبيقات التجارية و الجيش، (6) تصنيف بروتوكولات الثقة والمخططات لمختلف تطبيقات الطائرات بدون طيار و (7) دراسة عن الطائرات بدون طيار وتطبيقاتها في المدن الذكية.

الكلمات المفتاحية: طائرات بدون طيار، الشبكات المخصصة للموبايلات، اتصالات، المدن الذكية، الثقة، وادارة الثقة.

Acknowledgements

I would like to thank the committee member for their guidance, support, and assistance throughout my preparation of this thesis, especially my advisor Dr. Imad Jawhar. I would also like to thank Dr. Nader Mohamed for introducing me to the research area of Unmanned Aerial Vehicles (UAVs).

I would like to thank Dr. Mohamed Serhani, coordinator for M.Sc. in IT Management, and the instructors of the College of IT, United Arab Emirates University, for assisting me with all my studies and research.

Special thanks go to my parents and sisters who helped me along the way. I am sure they suspected it was endless. Also I would like to thank my colleagues at the College of Information Technology for their indispensable support and guidance.

Dedication

To my beloved parents and family

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AODV	Ad hoc On-Demand Distance Vector
AOTDV	Ad hoc On-demand Trusted-path Distance Vector
CORE	Collaborative Reputation
CPR	Cardiopulmonary Resuscitation
DMTR	Dynamic Mutual Trust-based Routing
DSR	Dynamic Source Routing
FAA	Federal Aviation Administration
FACES	Friend-based Ad hoc routing using Challenges to Establish Security
FANET	Flying Ad hoc Networks
FSO	Free Space Optics
GIS	Geographic Information Systems
HMM	Hidden Markov Model
IDS	Intrusion Detection Systems
LTE	Long-Term Evolution
M2M	Machine-to-machine
MANET	Mobile Ad hoc Network
NGO	Non-Governmental Organization
PKI	Public Key Infrastructure
QoS	Quality of Service
RFID	Radio Frequency Identification
SOC	Service Oriented Computing
SOM	Service Oriented Middleware
SORI	Secure and Objective Reputation-based Incentive
TAODV	Trusted Ad hoc On-Demand Distance Vector
T-AODV	Trust-embedded Ad hoc On-Demand Distance Vector
TARP	Trust-Aware Routing Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

Chapter 1: Introduction

1.1 Overview

Unmanned aerial vehicles (UAVs) are proving to be an extremely flexible platform for a variety of applications. With advances in computation, sensor, communication, and networking technologies, the utilization of UAVs for military and civilian areas has become extremely popular in the last two decades. It is a relatively easy task to use UAVs in an unmanned aerial system (UAS) for increasing communications range and data aggregation capability. For example, if all communication infrastructures are destroyed in a disaster area, and there is an immediate need to build a network between rescue teams, then UAVs can easily be used as a communication relay between rescue teams to effectively coordinate rescue activities (Sahingoz, 2013).

UAVs have to exchange information with each other and with the control station in order to meet the needs of their applications. The Mobile Ad hoc Network (MANET) is a solution to deliver this information to its destination over long ranges via one or multiple relays. In fact, MANET is a multi-hop wireless network where each node in the network acts as a mobile wireless terminal as well as a router to forward information to its neighbours. Thus, all nodes in the network are connected without requiring a pre-existing infrastructure, which makes MANET a cost-effective technology.

A MANET is a self-configuring network of mobile hosts connected by wireless links that together form an arbitrary topology. Due to the lack of centralized control, dynamic network topology, and multi-hop communication, the provision of making routing secure in MANETs is much more challenging than in infrastructure-based networks (Kukreja, Singh, & Reddy, 2013).

In MANETs, the mobile nodes perform route discovery and route maintenance in a self-organized way, allowing communication among nodes beyond wireless transmission range instead of cooperating with any fixed infrastructure or centralized administration to form a network. The characteristics of the nodes, such as mobility and fundamentally limited capacity of the wireless medium, attenuation, multi-path propagation, interference, and disruption by attacks, lead to significant challenges for routing protocols in MANETs (Chuanhe, Yong, Wenming, & Hao, 2009).

Traditional MANET routing protocols assume that all nodes in the network work in a benevolent manner, and that no predefined trust exists between communication partners. This may render the network vulnerable to malicious attacks in case of the presence of selfish and malicious nodes. Selfish nodes are those that, in order to save their own batteries, do not propagate packets from other nodes as per the protocol, while malicious nodes may perform impersonation, fabrication, or modification attacks against the network traffic. Since the communication safety of a host depends solely on a proper choice of the path used to reach the destination, it is important for a host to know the reliability of the nodes forming the route (Safa, Artail, & Tabet, 2009).

1.2 Problem Statement

As all the existing work in the area of secure routing in MANETs is based on key management, heavy encryption techniques, or continuous monitoring of neighbours, these approaches are expensive and they do not fit MANETs well. Thus, trust-based routing, which has a relatively reduced overhead, is more appropriate for the UAV environment.

As relay nodes, UAVs can adopt trust protocols of MANETs to address communication issues. Multi-UAV operations significantly complicate communication scenarios in several applications. In fact, the high mobility of UAVs disrupts the flow of data in an already established path. By adopting the trust protocols of MANETs, the establishment of a trusted communication path becomes easier and allows the continuation of the flow of essential information.

Trust management is needed when participating nodes (UAVs) without any previous interactions desire to establish a network with an acceptable level of trust relationships among themselves. Trust management has diverse applicability in many decision-making situations, including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes.

1.3 Contributions

The main contributions of this thesis are the following:

- Characterization of different UAV-based networking architectures.
- Identification of the characteristics and issues in MANET protocols to provide efficient UAV-based communication.
- Classification of different data traffic types for efficient UAV-based communication in various applications and environments.
- Classification of trust-based protocols and management schemes that can be adopted by UAVs.
- Comparison of the communication requirements between military and civilian applications.
- Case study on UAVs and their applications in smart cities.
- Identification of different applications of UAVs for United Arab Emirates.
- Classification of the trust protocols and schemes appropriate for various UAV applications.

1.4 Scope

The scope of this thesis is to provide an elaborate discussion on UAVs and their types, classify their applications in different domains, classify different trust-based protocols and management schemes that can be adopted by UAVs, propose various UAV applications where such protocols and schemes can be adopted, identify their related issues, and elaborate on the applications of UAVs in smart cities and in UAE. This thesis does not cover the technicality associated with trust-based protocols and management schemes.

1.5 Research Methodology

The main purpose of this thesis is to analyze the different trust-based routing protocols and management schemes of MANETs and map the characteristics to UAVs, considering the modifications, to provide efficient UAV based communication in various applications and environments.

In this thesis, a literature survey is conducted on different trust-protocols and management schemes. After analyzing them, a table characterizing the features of each protocol and scheme was provided. This literature survey is covered in Chapter 4, titled "Trust-Based UAV Communication".

Based on the analysis, we provide our propositions on the applicability of different protocols and management schemes in various UAV applications. All the references that were gathered for this thesis were collected from the UAEU E-library and resources and databases like IEEE, Springer and ACM.

1.6 Thesis outline

The rest of the thesis is organized as follows. Chapter 2 provides related work on UAVs and MANETs. Chapter 3 discusses the applications of UAVs in the military and commercial domains. It also provides a case study on UAVs’ potential use in smart cities and identifies different related opportunities. Chapter 4 introduces communication in UAVs where several concepts are discussed. Such concepts include trust-based communication, properties of trust, trust protocols, and trust management schemes that can be adopted by UAV communication systems. Chapter 4 ends with a case study on trust management in UAV networks where several trust issues are discussed. Finally, Chapter 5 concludes the thesis.

Chapter 2: Background and Related Works

2.1 Unmanned Aerial Vehicles

Small and medium-sized inexpensive UAVs equipped with wireless communication capabilities are now commercially available. Some of these only carry basic control units, while others are programmable and equipped with sensors, actors, cameras, storage, and embedded processors. They demonstrate a high degree of stability and agility in the air. A few years ago, military applications were the main driving force behind the development of UAVs and UAV systems. However, very recently, a number of civil applications have emerged and participated in driving the development of UAV technologies further ahead. These civil applications are divided into three categories: safety control, scientific research, and commercial applications. An example of a UAV is shown in Figure 2-1.

Figure 2-1: An unmanned aerial vehicle (McCray, 2014).

UAVs at the beginning were known for their military use, which gave some people a limited view of this technology. When UAVs were allowed to serve in civil applications, the image of UAVs changed, and provided the media with a good representation and good impression about UAVs. In addition, UAVs were involved in some humanitarian activities, such as monitoring areas affected by hurricanes. For example, in Nepal, UAVs were involved in wildlife protection. The Non-Governmental Organization (NGO) that was involved in the project trained their guards on how to use UAVs in protecting wildlife, which helped stop some of the crisis. NGOs in Japan use UAVs to monitor illegal Japanese whaling in the southern hemisphere. That is what gave the research and technical communities a good impression about UAVs and encouraged their use (Franke, 2013).

UAVs can play important roles in the management of different applications, such as search and rescue, situation awareness in natural disasters, environmental monitoring, and perimeter surveillance. Some of these applications require high mobility and the need to reach locations that are difficult to access with ground vehicles (Oller et al., 2005). Although manned aerial vehicles can be used for these applications, such utilization could require long hours of repetitive, high levels of focus, as well as costly flights that place a heavy burden on pilots and a very high cost on the organization that operates the aerial vehicles. Using a UAV for repetitive tasks generally results in enhanced task efficiency. This is mainly due to the high accuracy, mobility, and repeatability levels of UAVs (Saggiani & Teodorani, 2004). Furthermore, using manned aerial vehicles in dangerous missions exposes pilots to high risks and life-threatening situations; in contrast, using UAVs will eliminate or minimize this risk.

The architecture of a typical UAV consists of components such as the control system, the monitoring system, the data processing system, and the landing system. The internal systems provide a wide range of functions, from navigation to providing data transfer to ground stations. The UAV market is still growing, and UAVs are being used in new activities and in solving new problems every day. Many organizations are interested in developing UAV systems to reduce the costs of related services (Kharchenko & Prusov, 2012). Table 2-1 provides an overview of different categories of UAVs.

Table 2-1: Categorization of UAVs (Dai, Li, & Zhai, 2010)

UAV Categories	**Acronym**	**Range (km)**	**Flight Altitude (m)**	**Endurance (hours)**	**MTOW (kg)**	**Currently Flying**
Tactical						
Nano	η	< 1	100	< 1	< 0.025	YES
Micro	μ	< 10	250	1	< 5	YES
Mini	Mini	< 10	150–300	< 2	< 30	YES
Close Range	CR	10–30	3000	2–4	150	YES
Short Range	SR	30–70	3000	3–6	200	YES
Medium Range	MR	70–200	5000	6–10	1250	YES
Medium Range Endurance	MRE	> 500	8000	10–18	1250	YES
Low Altitude Deep Penetration	LADP	> 250	50–9000	0.5–1	350	YES
Low Altitude Long Endurance	LALE	> 500	3000	> 24	< 30	YES
Medium Altitude Long Endurance	MALE	> 500	14000	24–48	1500	YES
Strategic						
High Altitude Long Endurance	HALE	> 2000	20000	24–48	12000	YES
Special Purpose						
Unmanned Combat Aerial Vehicle	UCAV	Approx 0.1500	10000	Approx. 2	10000	YES
Lethal	LETH	300	4000	3–4	250	YES
Decoy	DEC	0–500	5000	< 4	250	YES
Stratospheric	STRATO	> 2000	>20000 & < 30000	> 48	TBD	NO
Exo-Stratospheric	EXO	TBD	> 30000	TBD	TBD	NO
Space	SPACE	TBD	TBD	TBD	TBD	NO

To date, some of the inhibiting factors for using UAVs in civilian applications include the cost of acquiring UAVs, building the required applications, and operating the system. UAVs are easy to deploy and are flexible in performing difficult tasks, supporting high-resolution imagery and covering remote areas. On the other hand, a device with such abilities must have some ethical and legal impacts. Some countries have privacy and data protection acts and laws. However, most UAV applications were deployed in the military and security fields.

The Federal Aviation Administration (FAA) (Federal Aviation Administration, 2014), which authorized the civil use of UAVs, imposed some conditions. UAVs can be used for public applications provided that the UAVs are flown at a certain height level. Figure 2-2 shows airspace in accordance with FAA classifications. The FAA pays a lot of attention to Class A—all U.S. airspace from 18,000 to 60,000 feet, where commercial planes fly. This is followed by the airspaces around airports, called Class B (big airports), C, and D (smaller airports). Class G (700–1,200 feet), which is unregulated airspace, is allocated for UAV use for civilian applications.

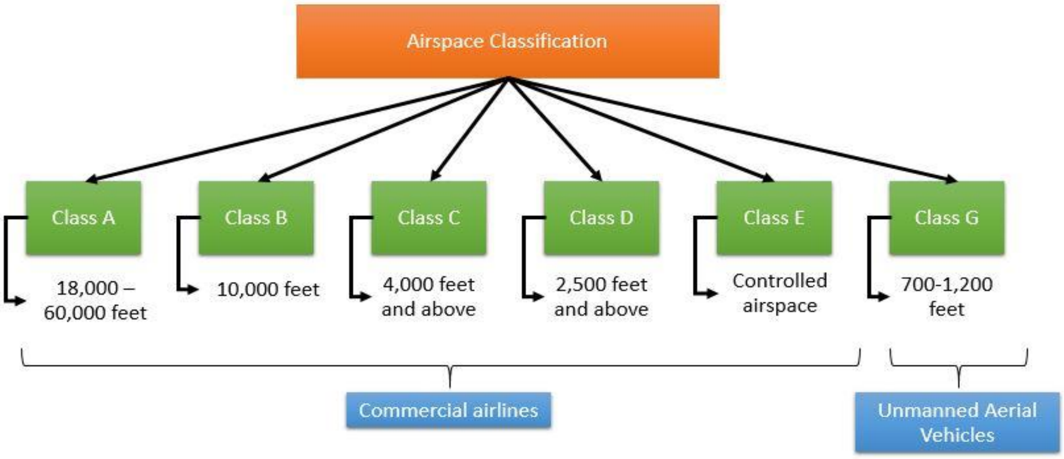

Figure 2-2: FAA airspace classifications

Since UAV can move quickly and flexibly, it is absolutely impossible to communicate using wires when they are flying. Even using wireless techniques, the flying attitude and speed of a UAV should be considered. However, there are also a number of advantages when UAVs use wireless networking. Some of them are (Dai, Li, & Zhai, 2010):

- UAVs can provide on-demand, high-quality communication due to line-of-sight signal propagation.
- UAVs can be sensing and data fusion nodes dynamically deployable in the region of interest.
- UAVs can tailor their flight paths to enhance the quality of wireless networking and communication.
- UAVs can themselves carry and forward huge amounts of data..

2.2 Mobile Ad-hoc Networks (MANETs)

MANETs form one of the most promising fields for the research and development of wireless networks. As the popularity of mobile devices and wireless networks significantly increased over the past years, wireless ad-hoc networks have now become one of the most vibrant and active fields of communication and networks (Goyal, Parmar, & Rishi, 2011).

A MANET is a collection of independent mobile nodes, which are connected with wireless links, such as IEEE 802.11 a/b/g/n, 802.16, etc. It dynamically configures an infrastructure-less network by using these mobile nodes, not only as hosts, but also as routers. These nodes are free to move, and the network topology changes rapidly over time.

The MANET nodes, such as notebooks, netbooks, tablets, sensor nodes, etc., are generally small and have limited processor/energy capacity. It is difficult to build and maintain such a network. Therefore, some main functionalities of network layers, such as routing, should be done dynamically by these mobile nodes. With the increase in utilization rates and application areas of MANETs, mobile nodes have begun to be embedded in vehicles such as cars, ambulances, fire engines, tanks, etc. This new networking concept is called Vehicular Ad-Hoc Network (VANET), which extends the range of MANETs and enables its usage in new application areas (Huo, Xu, Zhang, & Shan, 2011).

Flying UAV networks are a kind of extension of traditional MANETs. Flying Ad hoc Networks (FANETs) were introduced as a new form of MANET in which the nodes are UAVs (Bekmezci, Sahingoz, & Temel, 2013). According to this definition, only multi-UAV systems can form a FANET (Figure 2-3). On the other hand, not all multi-UAV systems form a FANET. MANETs can be used to provide communication between the UAVs.

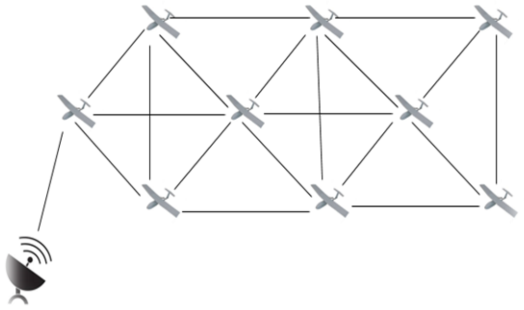

Figure 2-3: Flying Ad-hoc Networks

As UAVs and MANETs share similar characteristics, MANET protocols can be adapted by UAVs for communication with appropriate extensions and adaptations, which are outlined below (Jawhar, Mohamed, & Al-Jaroodi, 2014):

- UAV mobility: Some routing protocols perform better but suffer large message overhead when nodes are highly mobile. This is mostly due to dynamic network topology.
- Number of UAVs in the network: Scalability is a major concern. Some routing protocols perform better on small-sized networks. Others perform better in large-scale networks.
- Memory and storage capacity: As the size of the network increases, some protocols

may require more storage capacity to promote better performance.

- Power consumption: Some protocols require more power and energy to perform well in UAV networks; hence, appropriate energy-aware protocols are necessary.
- Transmission robustness and security: The quick reaction of a UAV and its security during any given task is an important factor. However, more security requires more overhead, which reduces robustness.
- Connection to infrastructure: Some protocols require seamless connection to infrastructure, as it may be important to certain applications, like centralized storage and access to infrastructure/the Internet.
- Throughput: This is an important factor because, depending on the application, we need to consider the data traffic rates that can be supported by UAV networks.
- Handoff and roaming: As UAVs move in and out of range of various communication gateways, appropriate and timely handoff and roaming strategies must be used to ensure seamless switching between base stations/access points.
- Processing capability: Some protocols require large computations and processing in real time.
- Co-located networking protocols: In locations where other networked devices are used, it is crucial not to interfere with them, as this may reduce protocol efficiency.

Chapter 3: UAV Applications

The potential civilian, commercial, and scientific applications of UAVs are numerous. The most common use of UAVs across all domains (both within and outside of the military) is persistent surveillance and data collection. UAVs have already been fielded for missions such as law enforcement, wildfire management (Zajkowski, Dunagan, & Eilers, 2006), pollutant studies (Corrigan, Roberts, Ramana, Kim, & Ramanathan, 2008), polar weather monitoring (Curry, Maslanik, Holland, & Pinto, 2004), and hurricane observation (Frew & Brown, 2008). Table 3-1 provides examples of applications in several categories based on military and civilian domains.

Table 3-1: UAV Applications for the Civilian and Military Domains

Category	**Military Applications**	**Civil Applications**
Security	▪ Security and Control ▪ Aerial Reconnaissance ▪ Aerial Traffic and Security Watch ▪ Battlefield Management	▪ Border Patrol ▪ Port Inspection
Search and Rescue	▪ All-Terrain Search and Rescue ▪ Life Raft Deployment ▪ Rescue Point Marking	▪ Epidemic Emergency Medical Supply
Monitoring	▪ Waterways and Shipping ▪ Pollution Control and Air Sampling ▪ Chemical, Biological, Radiological, and Nuclear Deployments	▪ Forest Fire Surveillance ▪ Traffic Monitoring
Impact and Disaster Management	▪ Impact and Disaster Effects Management ▪ Rescue and Clear-Up Effort Supervision ▪ Disaster Damage Estimation	▪ Disaster Management ▪ Damage Assessment ▪ Hurricane Monitoring
Communications	▪ Secure Telecommunications ▪ Telecom Relay and Signal Coverage	▪ Unsecure Communications
Munitions	▪ Air-to-Ground Missiles ▪ Guided Shells ▪ Anti-Tank Missiles ▪ Air-to-Air Missiles ▪ Wide-Area Munition Deployments	

3.1 Military Applications of UAVs

The U.S. military began experimenting with UAVs as early as World War I. By World War II, UAVs could be controlled by radio signals, usually from another aircraft. Vehicles that could return from a mission and be recovered appeared in the late 1950s. Today, UAVs perform a wide range of missions and are used by all branches of the military. Some of them are described below (Glade, 2000).

3.1.1 Transportation

UAVs could be used to transport cargo, especially in relatively small quantities that would apply in tactical situations. The current state of technology may be sufficient to create remotely piloted or autonomous helicopters that are capable of delivering supplies and ammunition to troops in the field, as long as specific instructions and restrictions guide these UAVs.

3.1.2 Intelligence, Surveillance and Reconnaissance

UAVs are frequently used for intelligence, reconnaissance, and surveillance option missions, which take into account that UAVs have long endurance times, can be positioned flexibly near potential targets, and are small and relatively difficult to detect. The long endurance of UAVs is particularly important for surveillance when these operations could be conducted over days. In this sense, UAVs could relieve manned platforms of the need to maintain the high operational time for extended periods that are the norm in modern military contingencies.

The U.S. military uses several UAVs in surveillance missions. The U.S. Air Force has used the Global Hawk (Figure 3-1) for surveillance missions, and the U.S. Army and Navy developed the Outrider UAV for tactical reconnaissance. Meanwhile, the U.S. military is developing UAVs that can fly autonomously and broadcast real-time information, which the U.S. Army will use for reconnaissance, jamming, chemical or biological detection, and placing remote sensors on the battlefield.

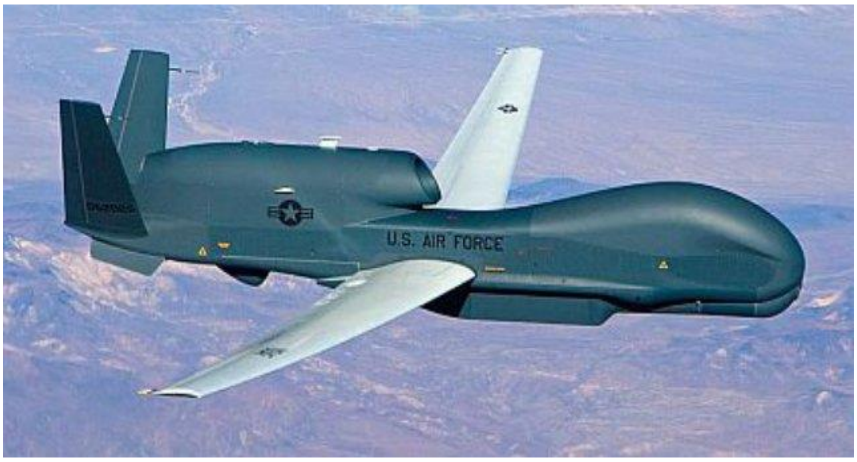

Figure 3-1: The Global Hawk UAV (Curry R. , 2014)

3.1.3 Attacking Fixed Targets

The U.S. military has developed UAVs that demonstrated the ability to launch weapons against air defence sites. As early as 1972, a Ryan Lightning Bug drone successfully launched an AGM-65 Maverick electro-optical missile against a radar control van. It is possible that UAVs could detect whether states are involved in manufacturing or storing weapons of mass destruction, and attack those facilities.

The U.S. Air Force Scientific Advisory Board suggested that, to attack these facilities, the United States should develop “dual-equipped” UAVs with multi-spectral sensors and weapons. This surveillance UAV would fly along with UAVs that are armed with precision guided penetrating weapons, which employ kill mechanisms that prevent the spread of these materials. UAVs can be used to attack high-value, fixed ground targets in military operations. Once military commanders give the location, type of target, and desired weapons effects to the UAV, it would determine the proper way to attack the targets with a remote operator or some form of automation.

3.1.4 Attacking Mobile Targets

The concept of attacking mobile targets with UAVs is quite popular, and involves using sensors on high-altitude, long-endurance UAVs in conjunction with aircraft. The fundamental problem with using UAVs is the difficulties of detecting and identifying targets in modem combat operations. For now, the problems of finding and destroying the right targets in combat operations mitigate against using UAVs for attacking mobile targets. If equipped with surveillance and reconnaissance sensors as well as munitions, low-observable UAVs that operate at high altitudes for long periods could be used to detect cruise missiles. The relatively long endurance of the UAVs, when coupled with the ability to detect and identify targets, could make remotely operated UAVs a viable option for this mission.

3.1.5 Combat Support Missions

A related idea is to use UAVs for the electronic support operations that are performed by strike aircraft and bombers, which involves using UAVs in conjunction with aircraft to target and jam fire-control radars. This category of UAV could function as a decoy that duplicates the radar, infrared, and radio signatures of fighter aircraft to increase their survivability. Once UAVs detect the location of enemy air defences and transmit that data to manned attack aircraft, these or other UAVs could deliver weapons to destroy enemy air defences.

3.1.6 Air-to-Air Combat

In the foreseeable future, technology will permit UAVs to conduct offensive and defensive combat operations against aircraft, cruise missiles, and ballistic missiles. If military commanders could use advanced UAVs to intercept aircraft, they would be able to shift manned aircraft to other combat missions. If we look to the longer term, it may be technologically feasible to develop UAVs that can replace the current generation of combat aircraft with vehicles whose performance and survivability exceeds that of piloted vehicles. Furthermore, UAVs could be used to attack facilities that produce or store weapons of mass destruction, as well as attacking critical fixed and moving targets. While some form of remotely piloted vehicle may be valuable in air combat, many concepts that rely on degrees of automation exceed current technological capabilities.

3.2 Commercial Applications of UAVs

Applications of UAVs are not only increasing in the domain of the military, but also in the public and commercial domains. Several companies are trying to adopt UAVs for their business purposes. A great example is Amazon.com, which introduced the Amazon Prime Air (Figure 3-2), a delivery UAV that delivers products to their owners within a few minutes after the purchase of the product. This began a competition with the delivery giant UPS, who is now working on developing UAVs for their business (Mohammed, Idries, Mohamed, Al-Jaroodi, & Jawhar, 2014).

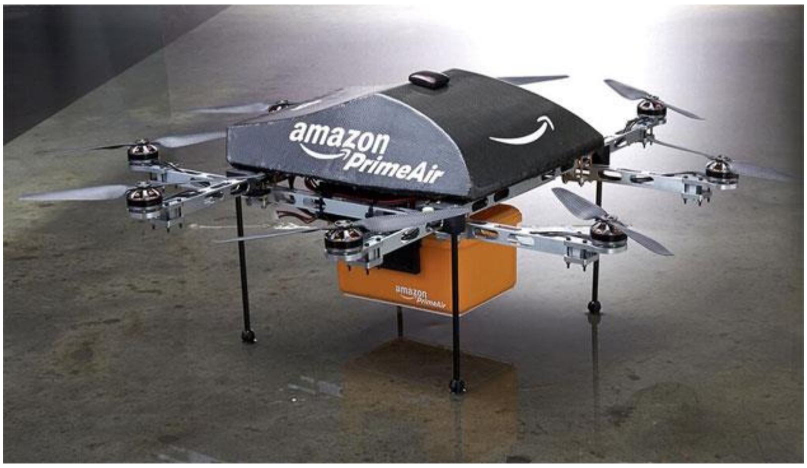

Figure 3-2: Amazon PrimeAir (Smith, 2013)

Facebook announced plans to use UAVs to provide Internet services worldwide. These UAVs are solar-powered and will rely on free space optical (FSO) communication to transmit data using light. The project, called Internet.org, aims to provide internet access to 5 billion users who currently lack it (Constine, 2014).

EasyJet, an airline company, also announced the use of UAVs (Figure 3-3) for performance evaluation and maintenance assessment of their fleet of aircrafts. The UAVs will be programmed to assess the carrier's fleet of Airbus A319 and A320 planes, reporting back to engineers on any damage that may require further inspection or maintenance work. According to EasyJet's engineering head, UAV technology could be used effectively to help perform aircraft checks that would usually take more than a day. Through UAVs, such maintenance could be performed in a couple of hours and potentially with greater accuracy. Bristol Robotics Laboratories, who is in collaboration with EasyJet to develop a safe, effective, and efficient UAV for EasyJet, agrees to the concept of aircraft inspection as a great application for UAVs. Embedded with smart navigation and computer vision, these UAVs can acquire accurate data from difficult angles (EasyJet to use unmanned drones to inspect its aircraft, 2014)

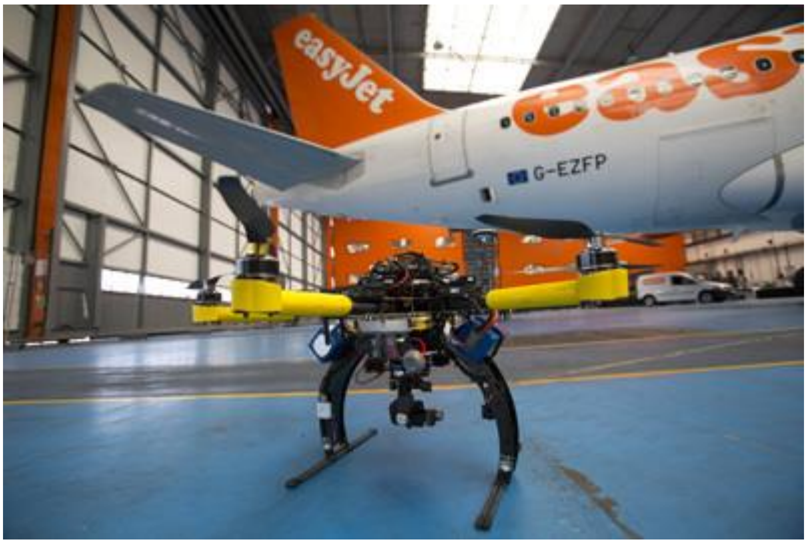

Figure 3-3: A UAV by EasyJet (Dronologista, 2014)

In Canada, UAVs are being used by the film industry to shoot commercials and films. For the past three years, Kaspi Films has been using UAV technology to shoot everything from car commercials to aerial videos for several companies. The film industry has been an early adopter of the commercial potential of UAVs, as studios are drawn to their versatility and low cost compared to filming with traditional jib arm cranes or helicopters. These UAVs can be fitted with cameras and can be used by individuals for filming family events, such as weddings, or doing extreme sports like mountain climbing and surfing (Canadian businesses harness drone technology, 2014).

3.3 UAVs for Smart Cities: A Case Study

One of the emerging areas of UAVs and their applications is their involvement in smart cities. The smart city approach not only aims to maintain the quality of life of residents and visitors, but also to improve living by leveraging IT infrastructure and novel communication technologies. A smart city is a model of efficiency, innovation, and ubiquitous access to a wide range of automated services. UAV applications can provide several services that can be beneficial to smart cities.

3.3.1 Opportunities for UAVs in Smart City

3.3.1.1 Traffic and Crowd Management

Efficiency of security and safety systems in a city have become a serious concern, not only for smart cities, but also for any type of city. The involvement of UAVs in smart policing activities has lately been supported by the U.S. Congress and top-level federal agencies such as the Bureau of Justice Assistance and the U.S. Department of Justice. In addition, the integration of mobile applications, secure and reliable wireless networks, forensic mapping software, and UAVs can help smart cities become safe places for living. Figure 3-4 shows a law enforcement UAV.

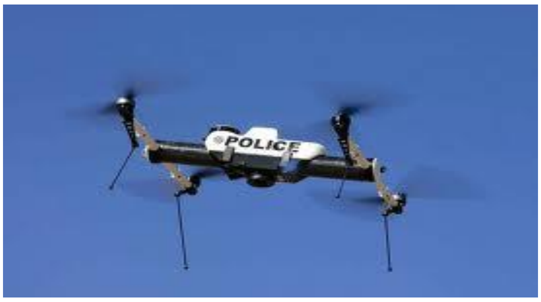

Figure 3-4: A Law enforcement UAV (Design, 2014)

3.3.1.2 Healthcare Applications

UAVs could be deployed in basic life support applications; recently, some development has taken place for using a UAV to provide support for cardiovascular patients. A UAV could carry a defibrillator and other equipment directly to a patient to provide cardiopulmonary resuscitation (CPR) (Radio Television Russia, 2014). Furthermore, the availability of basic life support and health services is one of a city's core issues. Such an application will provide many opportunities for basic life support systems to be deployed quickly via UAV systems. In addition, the UAV could work as ambulances and safety & rescue providers for remote areas. This transforms the role of UAV applications to become more supportive than informative. Therefore, this approach will give an opportunity to develop wearable devices to integrate with UAV systems.

For example, in a remote area occupied by many people, UAVs could provide different services, such as basic life support, basic ambulatory services, and the providence of medical supplies. Such applications will reduce the costs of providing these services to remote areas. Furthermore, it could provide the same services to those who are in public areas and accident-prone areas within the smart city. Researchers are developing UAVs that can carry supportive tools for those who are drowning in the sea. The UAV can carry and drop tools like buoys and CPR devices with life and real-time communication with the command centre. In addition, UAVs could be deeply involved in the previously mentioned applications, since most of the current researchers are working on enhancing the payload, power consumption, and ability to handle different weather conditions. Due to such advancements, many capabilities will be added to UAV applications to play advanced roles and tasks.

3.3.1.3 Civil Security Control

The integration of UAV solutions with machine-to-machine (M2M), radio frequency identification (RFID), long term evolution (LTE), and live video streaming increased the role of UAVs in public safety areas. In addition, the trends towards intelligence and data mining give UAVs an opportunity to be involved in civil security activities, like providing security services for smart cities. This new trend will move the cities' management personnel from being reactive to being proactive and leveraging data.

Furthermore, the involvement of UAVs in surveillance activities will reduce costs and increase the efficiency of operations. The usage of UAVs will allow the city to deploy a quick operations room, updated with efficient data flow, and will allow the city to smoothly manage big public events with huge numbers of attendees, and also to provide full technical coverage.

3.3.1.4 Agriculture and Environmental Management

UAVs can be used to fertilize the crops by dropping fertilizer/water from above. They can also be used to monitor the growth of crops, and they can monitor the environment by using wireless sensors that can measure environmental substances such as CO_2 emissions and other harmful substances, which will allow them to monitor oil and gas facilities.

3.3.1.5 Guidance

UAVs could work as guides for tourist attractions and public facilities, like university campuses. They could guide visitors around the area and communicate with them through smart phone apps (SkyCall, 2014) or on-board audio systems. The UAV can also integrate an on-board camera as both an information gathering system, such as relaying images to a base location upon encountering a user, as well as a manually controlled camera accessible to visitors. In addition, the same approach could be integrated with other applications in rescue contexts. Furthermore, such applications will affect UAVs ability due to their requirements and limitations, such as payload and power efficiency. In addition, UAVs act as guides in museums, some being equipped with multi-language translation capabilities.

3.3.1.6 Geo-spatial and Surveying activities

One of the new trends in UAV civil applications in smart cities is using UAVs in geospatial surveying. The main design of a smart city requires the optimization of data flows provided by wireless sensor networks, as sensors are the main component of any autonomous system such as those involving UAVs. The system also requires real-time processes integrated with the available information repository, since handheld devices and wireless sensors are known for their low power consumption and high performance. This can provide a tool for the smart city technological base. This combination of technologies creates a wide range of applications and opportunities, such as fire management in open areas, where the use of UAVs and micro-UAVs is very beneficial.

The potentials vary from a wide range of available solutions and innovations that are evolving quickly. Yet, the obstacles and difficulties to UAV system deployments are linked to political and cultural issues to a greater extent than the cost and benefit issues. Due to the reliability of most UAV designs, the integration of such technologies make it possible to install wireless sensors on-board to make the UAVs usable in geospatial land surveying and geographic information system (GIS) applications in smart cities, in addition to being helpful for environmental analysis. These opportunities may lead to cost reductions and cutting down the number of manpower hours involved in such activities.

3.3.1.7 Natural Disaster Control and Monitoring

Using UAVs in disaster situations like fires, floods, and earthquakes will help the authorities control such emergency situations efficiently and effectively. UAVs will analyse the situation properly and also help in acting properly in certain disastrous situations because the UAVs can reach areas that humans cannot reach.

One example is the use of UAV in Estes' (2014) work. Another example is using UAVs to locate people in natural disasters and to deliver needed emergency resources used to save people's lives. Two natural disasters hit Fukushima, Japan, in 2011. The first one was the strongest earthquake in Japanese history, followed by a tsunami that claimed the lives of more than 15,000 people, while a whole region was destroyed. One of the main challenges was that there was a severe lack of information about the situations from within the disaster areas. UAVs are ideal monitoring machines in these circumstances (Madrigal, 2011). UAVs can also be used to establish an emergency communications system to replace a damaged communications infrastructure after natural disasters such as earthquakes, floods, hurricanes, and fires, to help in managing the emergency (Tuna, Nefzi, & Conte, 2013). Multiple UAVs can be efficiently allocated at different locations to re-establish the communication infrastructures.

3.3.1.8 UAV as Wearable Device

The most recent UAV technologies are for developing UAVs as wearable devices, like a tiny wearable camera on a wrist band (Figure 3-5). The wrist straps unfold to create a quad copter that flies, takes photos or video, and comes back to you. The product is still under development. Wearable UAVs could play roles in protecting children in play areas and provide live broadcasting to their parents. During the initial stages of providing services in the context of smart cities, UAVs should be deeply involved in the applications of public security, safety, and life support operations.

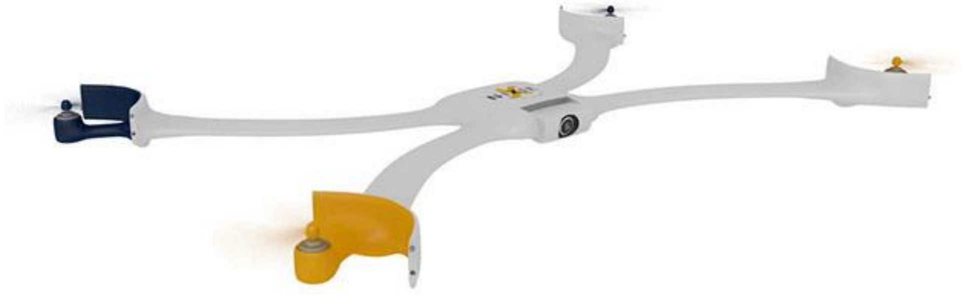

Figure 3-5: Nixie, a wearable UAV (Dent, 2015)

3.3.1.9 UAVs for Merchandise Delivery

As UAVs are flexible to fly and reach different destinations, they can be used efficiently to deliver small customer orders. It can be used to deliver different orders within short times even in crowded cities. DHL is investigating utilizing UAVs for their delivery operations (Heutger & Kückelhaus, 2014). In addition, Google is also developing a program called Project Wing to build autonomous delivery systems capable of carrying parcels to nearly every person within a few minutes (Nieva & Rosenblatt, 2014). Google has been working on Project Wing for more than two years. Initial testing is being conducted for rural deliveries in Queensland, Australia.

3.3.2 Seamless Integration between UAVs and Smart Cities

The infrastructure of smart cities consists of a large number of heterogeneous software and hardware components. In addition, they have some systems, such as sensor networks, servers, databases, control devices, intelligent transportation vehicles, and others. Therefore, the seamless integration of UAVs into a smart city is not an easy task. There is a need for advanced middleware platforms to support such integration.

Middleware is considered a valuable solution for integrating UAVs with other systems in smart cities. However, it is not easy to develop a middleware that will meet the many requirements in terms of considering the UAV characteristics and different application architectures such as smart cities, as well as the required specifications for the middleware (Shah, Roy, Jain, & Brunette, 2003). Middleware can provide the following features and advantages for the integration of UAVs into smart cities.

- Offers tools and functions to simplify the development of UAV-based smart city applications.
- Offers high-level abstractions and interfaces to facilitate UAV-based smart city application integration, reuse, and development.
- Hides the heterogeneity of the UAV and smart city devices, platforms, and operating environments.
- Hides the distribution and communication details in the environment.
- Facilitates communications among the different components of the UAV-based smart city systems.
- Provides common services for general-purpose functions needed by different UAV-based smart city applications to reduce development efforts and avoid the duplication of services.

- Provides a common architecture to add new services and features without having to change the UAV-based smart city applications.
- Offers value-added features and non-functional properties such as security, reliability, and quality of services.
- Supplies the necessary tools to enhance the performance and increase the stability, safety, and scalability of the UAV-based smart city applications.

To design a middleware framework, many challenges and issues need to be considered, such as quality of service (QoS), hardware resources, changes in network topology and size, heterogeneity, application knowledge, security, and integration with other systems. Furthermore, the middleware design may include advanced services, such as collaborative sensing, collaborative acting, collaborative communication, collaborative control, and collaborative data processing and collaborative control between UAVs and other smart city systems (Idries, Mohamed, Jawhar, Mohammed, & Al-Jaroodi, 2015) (Mohammed, Idries, Mohamed, Al-Jaroodi, & Jawhar, 2014) (Mohamed, Al-Jaroodi, Jawhar, & Lazarova-Molnar, 2013). Generally, the usage and deployment of an advanced middleware for UAV-based smart city applications can reduce the cost of development, deployment, and operations.

A new and advanced approach in middleware technologies is the use of service-oriented middleware (SOM) (Al-Jaroodi & Mohamed, 2012). This approach has already been proven to simplify the implementation as well as help in relaxing the project management issues of a number of industrial domains. It was used for wireless sensor networks (Mohamed & Al-Jaroodi, 2011), manufacturing (Bo et al., 2010), telecommunications (Groba, Braun, Springer, & Wollschlaeger, 2008), and distributed monitoring and control systems (Bo et al., 2010). The approach was used in these domains to reduce the effort and cost of development, testing, and operations.

Similarly, SOM can play an import role for developing and operating UAV-based smart city applications. Accordingly, we anticipate a successful migration of the model to support UAV smart city application development and provide a generic middleware platform that will increase productivity and widen the range of smart city applications that can be designed and built using UAV systems.

Moving forward, SOM extends the capabilities of middleware and provides high flexibility for adding new and advanced functions to UAV applications. SOM logically views UAVs as a provider for a set of services for user applications. With SOM, all hardware devices, such as sensors, actuators, data storage devices, communication devices, and processors, can be viewed and utilized as services (Taylor et al., 2006).

In addition, other advanced services, such data aggregation, adaptation, security, safety, system autonomy, reliability, and management, can be designed, implemented, and integrated in an SOM framework to provide a flexible and easy environment to develop effective UAV applications. SOM for UAVs is necessary to support several otherwise hard-to-incorporate functionalities in the service-oriented computing (SOC) model. These functionalities include the functional and non-functional requirements that different services might need. For any service-oriented application, there several common functionalities, such as service registry, discovery, communications, reliability, and security, that are irrelevant to the application. These can be easily generalized and made available via an SOM platform to be used by different smart city applications developers (Mohamed & Al-Jaroodi, 2013; Mohamed, Al-Jaroodi, Jawhar, & Lazarova-Molnar, 2014).

3.4 UAV Applications for UAE

The UAE is one of the recent countries that has invested in the applications of UAVs for improving people’s lives. With the 2020 Expo in the near future, several applications of UAVs can be useful for improving the economy and lifestyle of UAE. Some of these applications are outlined below.

3.4.1 Wildlife Monitoring

The UAVs can document vast diversity of wildlife by gathering images from different locations. The UAVs can hover over the locations and send pictures/videos back to the authorities who can analyze them. This eliminates the need for humans to manually gather data as it could be dangerous considering the weather conditions in UAE during summer.

3.4.2 Oil Field Detection

UAVs can be used to detect the availability of oil fields in UAE. As UAE is one of the major players in this industry, scanning for more oil fields with the help of UAVs can be more efficient. UAVs can be equipped with sensors and can be deployed at certain locations where they can analyze the land for possible oil sites.

3.4.3 Pipeline Monitoring

Effective monitoring of oil pipeline systems is an important task due to the high environmental cost of an undetected oil spill. As such locations are quite far from the mainland, UAVs can help in monitoring the pipelines more efficiently and quickly. UAVs can be attached with sensors and can periodically monitor the plant for potential damage. They can gather high resolution images that can determine the source of damage. Also the UAVs can gather images at locations that are quite difficult to do manually.

3.4.4 Port Inspection

UAVs can be used for the surveillance of suspicious activities and to support inspection at ports in UAE. The UAVs can be deployed to cover areas that are unreachable manually. They can provide live feed of the port from various angles to the ground staff where they can observe for any suspicious activities.

Chapter 4: Trust-Based UAV Communication

One of the most important design problems for multi-UAV systems is communication, which is crucial for cooperation and collaboration between the UAVs. If all UAVs are directly connected to an infrastructure, such as a ground base or a satellite, the communication between UAVs can be realized through the infrastructure. However, this infrastructure-based communication architecture restricts the capabilities of the multi-UAV systems. Ad-hoc networking between UAVs can solve the problems arising from fully infrastructure-based UAV networks. For efficient communication, UAV systems must also consider the communication requirements for military and commercial applications, different data traffic and Quality of Service (QoS) requirements. Table 4-1 provides the classification of UAV applications with their data traffic and QoS requirements and Table 4-2 identifies the communication requirements for military and commercial purposes.

Table 4-1: UAV Application and their Data Traffic and QoS Requirements

Data Traffic	**Delay Tolerance**	**Bandwidth Requirements**	**Applications**
Store and forward sensing	High	Low	Agricultural and environmental management, habitat monitoring.
Store and forward pictures	High	High	Geo-spatial surveying, military surveillance.
Command and control	Low	Low - Medium	Military flights, guidance, emergency response (medical, environmental, etc.), combat support, transportation
Real-time sensing	Low	Low	Traffic and crowd control
Store and forward videos	High	Medium - High	Natural disaster management, wearable devices (bandwidth depends on quality)
Real-time video	Low	High - Very high	Border patrol, military surveillance, air-to-air combat, attack fixed/mobile targets.

In general, Frew and Brown (2008) described four communication architectures that can be used in UAVs. These four architectures are direct link, satellite, cellular, or mesh networking. A direct link between the ground control station and the UAVs is the simplest architecture. However, obstructions can block the signal, and at longer ranges, the UAV requires a high-power transmitter, a steerable antenna, or significant bandwidth in order to support high-data-rate downlinks. The amount of bandwidth scales with the number of UAVs, so that many UAVs may not operate simultaneously in the same area.

Table 4-2: Classification of communication requirements for military and commercial UAV applications

Requirements	**Military**	**Civilian**
Platform safety	High	High
Payload management	High	Medium – High
Air traffic control connectivity	Necessary	Unnecessary
Detect, sense and avoid mechanisms	High	Medium – High
Data transmission speed	High – Very high	Medium – High
Interference with other networked devices	No interference (remote locations)	Can interfere (connection through wireless medium)

Finally, plane-to-plane communication will be inefficiently routed through the ground control station in a star topology and not exploit direct communication between cooperative UAVs operating in the same area. Direct plane-to-plane communication will be limited by the characteristics of the link technology and may prove difficult between two highly mobile platforms.

Satellite provides better coverage than a direct link to the ground control station. A lack of satellite bandwidth already limits existing UAVs operations. For high-data-rate applications, a bulky steerable dish antenna mechanism unsuitable in size, weight, and cost for small UAVs is necessary. Further, the ground control station requires a connection to the satellite downlink network. The ground control station may have obstructed satellite views because of terrain or clutter. Finally, multiple UAVs operating in an area will suffer significant delays if their communication is mediated by satellites.

Cellular refers to an infrastructure of downlink towers similar to the ubiquitous mobile telephone infrastructure. The mobile telephone infrastructure is not designed for air-to-ground communication. A single UAV transmitter can blanket a large area with its signal-degrading system performance. Therefore, small UAV operations may require a dedicated cellular infrastructure. The cellular architecture provides several advantages.

Firstly, coverage can be extended over large areas via multiple base stations. UAVs would hand off between different base stations as needed during flight. Secondly, the multiple base stations provide a natural redundancy so that if one link is poor, another link may perform better. Thirdly, a limited bandwidth can be reused many times over a region and capacity can be increased as needed to meet demand. The reuse can grow by adding more base stations as the number of users grows. Fourthly, the infrastructure can be shared by different UAVs. Once installed, many UAVs can each pay for the fraction of the infrastructure that they use. These advantages must be weighed against the cost. Such a solution applies where the infrastructure investment can be amortized across frequent and regular UAVs flights.

Meshing refers to a networking architecture where each node (i.e., a radio on a UAV or ground node) can act as a relay to forward data. Communication between a UAV and a ground control station can take place over several hops through intermediate nodes. The shorter range simplifies the link requirements, and bandwidth can be reused more frequently and thus more efficiently. Plane-to-plane communication can be direct and also benefit from the mesh routing protocols that employ additional relays as needed to maintain communication.

However, such meshing requires intermediate nodes to be present for such relaying to take place. Furthermore, nodes may be required to move specifically in order to support communication. Mesh architecture is thus a promising architecture for resolving many communication issues. Mesh architecture describes UAVs as relay nodes in MANETs. In such architecture, trust is an important factor for robust communication.

Trust is defined as the reliability, timeliness, and integrity of message delivery to their intended next hop. Initially, each node in the system is authenticated by an authentication mechanism if possible and is assigned a trust value according to its identity. If no information is available about the trustworthiness of a node, an unknown value will be assigned to that node until observed behaviour can adjust its trust level. The routing protocol can then choose the best route according to the current trust levels of the nodes in the MANET. When a node is compromised, it exhibits altered behaviour, which can be detected by intrusion detection systems (IDSs) by neighbouring nodes and reported to interested nodes (Liu, Joy, & Thompson, 2004).

Trust report distribution mechanisms are necessary for nodes to receive indications of potential threats or trustable behaviours in the network. One simple approach to distributing trust reports is for a node to only broadcast trust reports to its immediate neighbours. This means that each node would maintain a trust level table that includes only the next hop for each route. The nodes would then select routes based solely on the trust levels of its neighbours. Once a data message transmission is initiated, each node along the route would evaluate the route against its own trust level table. If during this evaluation any node determines that the trust requirement of the message cannot be met by the next hop in the selected route, an error message would be returned to the originating node. The originator would then select a new route.

Each node stores these routes in a table in which a record is maintained for each source node of which the node is aware. When a node observes an interval of good behaviour, or detects a threat on one of its neighbours, it examines its table and identifies all source nodes that have recently routed messages through the node under observation. The observing node then sends a directed trust report to these source nodes, using the simple dynamic trust level route selection scheme just described to ensure appropriate security for trust report routing.

When a data message transmission is requested, the source node can then pick a proper route based on the trust levels it maintains. The nodes along the route do not need to perform the hop-by-hop trust evaluation. This approach is also useful for the intentional frequent moving of malicious nodes. A malicious node can keep moving a long distance after performing malicious actions for a short time. The nodes that are aware of that node's behaviour would be too far away to be influential in reporting the node's behaviour without using the directed trust report scheme (Liu, Joy, & Thompson, 2004).

4.1 Properties of Trust in UAVs

As UAVs are the relay nodes, we can assume that the properties of trust in UAVs are similar to the properties of trust in MANETs. The properties of trust (Figure 4-1) in MANETs are as follows:

- Trust is dynamic: Trust establishment in MANETs should be based on temporally and spatially local information; due to node mobility or failure, information is typically incomplete and can change rapidly. It is pointed out that, in order to capture the dynamicity of trust, trust should be expressed as a continuous variable, rather than as a binary- or even discrete-valued entity. A continuous valued variable can represent uncertainty better than a binary variable (Adams, Hadjichristofi, & Davis IV, 2005).

- Trust is subjective: In MANET environments, a trustor node may determine a different level of trust against the same trustee node due to different experiences with the node derived from a dynamically changing network topology.
- Trust is not necessarily transitive: For example, if A trusts B, and B trusts C, it does not guarantee that A trusts C. In order to use the transitivity of trust between two entities to a third party, a trustor should maintain two types of trust: trust in a trustee and trust in the trustee's recommendation of the third party.
- Trust is asymmetric: In heterogeneous MANETs, nodes with higher capability (e.g., more energy or computational power) may not trust nodes with lower capability at the same level that nodes with lower capability trust nodes with higher capability.
- Trust is context-dependent: In MANETs, depending on the given task, different types of trust (e.g., trust in computational power or trust in unselfishness, trust in forwarding versus trust in reporting) are required (Cho, Swami, & Chen, 2011).

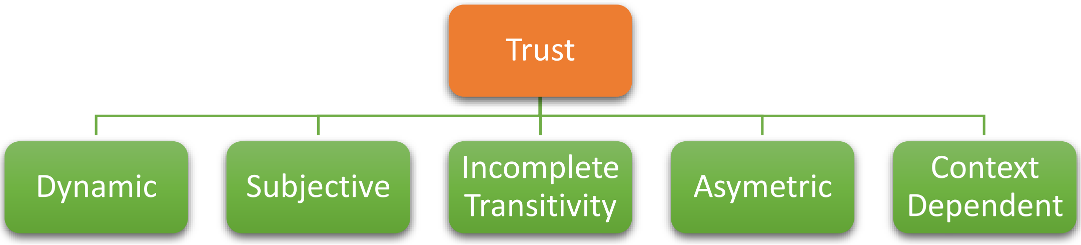

Figure 4-1: Properties of trust in MANETs

4.2 Different Trust Protocols

There are several trust-based protocols developed for MANETs to ensure secure communication among them. As UAVs can be considered nodes of MANETs, these protocols can be applied to UAVs.

In their work, Ghosh, Pissinou, and Makki proposed a trust-based ad-hoc on-demand distance vector (AODV) routing protocol that isolates malicious nodes acting independently or in collusion. The protocol requires the existence of a public key infrastructure (PKI). As intermediate nodes are not allowed to send RREP, it increases the delay in route discovery. In the protocol, a method for computing trust can be incorporated (Ghosh, Pissinou, & Makki, 2004).

Trust-embedded AODV (T-AODV) was proposed by Ghosh, Pissinou, and Makki (2005), which extends their work from 2004. The model computes, distributes, and updates trust. The working of the protocol is same as in 2004, with the difference that this solution works only when a malicious node sends false accusations. Each node maintains and periodically scans the tables, requiring the nodes to have more memory. The protocol requires the existence of a PKI.

Trusted AODV (TAODV) routing protocol was proposed by Li, Lyu, and Liu (2004). Trust is represented by an opinion as used in subjective logic. If a node behaves in a normal manner, other nodes increase their opinions of the node, and vice-versa. The nodes authenticate each other by verifying the certificate, which is an added overhead. The protocol is unable to detect an internal attack, in which a malicious node may refuse to forward packets or authenticates itself to the source but later on acts as a black hole.

A trusted routing protocol, called dynamic mutual trust-based routing (DMTR) (Chuanhe, Yong, Wenming, & Hao, 2004), based on the dynamic source routing (DSR) protocol, was proposed that secures the network using the trust network connect (TNC), and improves the path security, which is selected by barrel theory. Exchanges of trust tables between nodes requires lots of bandwidth, and increases the overhead.

A scheme for establishing trustworthy routes has been proposed by Pirzada, Datta, and McDonald (2006). Each node executes the trust model, having three main components: the trust agent, the reputation agent, and the combiner. The trust agent derives the direct trust, the reputation agent derives the indirect trust, and the combiner computes the final trust by combining the information received from both agents. If malicious nodes collude, the model may fail. If nodes have varying transmission power ranges, the mechanism of passive trust assignment might not work properly.

A trust-based DSR routing protocol for discovering routes in the presence of malicious nodes was presented by Pirzada and McDonald (2007). Each node monitors its neighbours and updates their trust levels depending on their behaviour. Trust values are propagated in the network with data traffic. Each node, before forwarding a packet, uses this trust information to find the most trustworthy path. Direct trust is computed based on Pirzada, Datta, and McDonald’s (2006) work.

A routing algorithm, tr-DSR, which is extended DSR, was proposed by Wang, Yang, and Gao (2005). The algorithm returns the routes having higher trust rather than the shortest path. In the proposed algorithm, some route replies are redundant, and the number of route request re-broadcasts can be reduced by allowing only legitimate nodes to rebroadcast the route requests.

In friend-based ad-hoc routing using challenges to establish security (FACES) (Dhurandher, Obaidat, Verma, Gupta, & Dhurandher, 2011), the trust of the nodes is determined by sending challenges and sharing friends lists. The proposed algorithm is divided into four stages: challenge your neighbour, rate friends, share friends, and route through friends. Challenges are sent to authenticate the nodes. Nodes that complete the challenge are put into the friends list; otherwise, they are put into the question mark list. In the rate friends' stage, friend rating is done on the basis of the amount of data they transmit and ratings obtained by other friends. This protocol requires that each node stores different lists.

An ad-hoc on-demand trusted-path distance vector (AOTDV) routing protocol was presented by Li, Jia, Zhang, Zhang, and Wang (2009). Here, the trust of a node is represented as a weighted sum of forwarding ratios, and path trust is computed as a continued product of node trusts. Here, the node is considered malicious based on its forwarding behaviour. Misbehaving nodes may participate in route discovery but may refuse to forward data packets. So, for calculating the trust of such a node, the control packet forwarding ratio (CFR (t)) value can be given less weight than the data packet forwarding ratio (DFR (t)) value. Table 4-3 highlights the features, requirements, and limitations of the above-mentioned trust protocols.

Table 4-3: Summary of Trust-Based Routing Protocols in MANETs

Protocol	Features	Requirements	Weakness/Overheads
Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes	Isolates malicious nodes acting independently or in collision	Requires the existence of a PKI	Increases delays in route discovery
Trust-Embedded AODV (T-AODV)	Model also works for colluding malicious nodes	All nodes have identical radio range, requires a PKI	Malicious node sends false accusation message, increases delays in route discovery
Incorporating Trust and Reputation in the DSR Protocol	Divided into three components: trust agent, reputation agent and the combiner	Assumes that nodes do not have varying transmission power	Uses a promiscuous mode for trust assignment, trust is based solely on the forwarding behaviour
Dependable Dynamic Source Routing Protocol	Each node monitors its neighbours and updates trust	Assumes that nodes do not collude	Nodes work in promiscuous mode, trust is based on the forwarding behaviour
TR-DSR: A routing protocol based on trust	Reduces routing traffic by forwarding requests to selected nodes	Solution uses pre-computed trust values	Some route replies are redundant
Opinion-Based Trusted Routing Protocol (TAODV)	Trust is represented by opinion as used in subjective logic	Requires the nodes to authenticate each other by verifying the certificate	Unable to detect in case a malicious node authenticates itself but later on acts as a black hole
Dynamic Mutual Trust-Based Routing protocol (DMTR)	Contains three components: the requestor, the decision maker, and the executant	Uses Trust Network Connect (TNC) and barrel theory	Exchange of trust table between nodes requires lots of bandwidth
FACES: Friend-Based Routing Protocol	Can handle many attacks	Incorporates friend-based mechanisms	
Trust-Based on-Demand Multipath Routing Protocol	Meets the trust requirement of the data packets	Neighbours are evaluated using packet forwarding ratio	Misbehaving nodes may not give true path trust in case of colluding attack

4.3 Trust Management Schemes

In Marti, Giuli, Lai, and Baker’s (2000) work, a reputation-based trust management scheme was proposed that consists of a watchdog that monitors node behaviours and a pathrater that collects reputation and takes response actions (e.g., isolating misbehaving nodes as a result of misbehaviour detection). This work is an initiative to dynamically incorporate direct observations into trust values for secure routing. It extends DSR, but trust evaluation is based only on direct observations.

In Paul and Westhoff's (2002) work, a context-aware mechanism for detecting selfish nodes was proposed by extending DSR with a context-aware inference scheme to punish the accused and the malicious accuser. However, the use of digital signatures to disseminate information about the accused and the malicious accuser may not be viable in a resource-constrained MANET environment.

In Michiardi and Molva's (2002) work, CORE (COllaborative REputation) was proposed that has a monitoring mechanism complemented by a reputation functionality that differentiates between direct reputation, indirect reputation, and functional reputation (task-specific behaviour). The proposed protocol is developed to make decisions about cooperation or the gradual isolation of a node. A unique characteristic of this mechanism is that it exchanges only positive reputation information. However, this may limit its reliance on positive reports without the facility to submit negative feedback.

In He, Wu, and Khosla's (2004) work, a reputation-based trust management scheme using an incentive mechanism was introduced (secure and objective reputation-based incentive; SORI). This scheme encourages packet forwarding and discourages selfish behaviours based on quantified objective measures and reputation propagation by a one-way hash chain based authentication. The performance of this scheme in the presence of malicious nodes, as may be expected in a hostile environment, has not been investigated.

Nekkanti and Lee (2004) extended AODV using trust factors and security levels at each node. Their approach deals differently with each route request based on the node's trust factor and security level. In a typical scheme, routing information for every request would be encrypted, leading to large overheads; they propose using different levels of encryption based on the trust factor of a node, thus reducing overhead. This approach adjusts the security level based on the recognized hostility level and hence can conserve resources; however, the approach does not treat evaluations of trust itself.

Li, Lyu, and Liu (2004) also extended AODV and adopted a trust model to guard against malicious behaviours of nodes at the network layer. They represented trust as opinion stemming from subjective logic. The opinion reflects the characteristics of trust in MANETs, particularly dynamicity. The key feature is to consider system performance aspects by dealing with each query based on its level of trust. Depending on the level of trust of nodes involved in the query, there is no need for a node to request and verify certificates all the time, thereby leading to significant reduction of computation and communication overhead.

Wang, Soltani, Shapiro and Tan (2005) proposed a mechanism to distinguish selfish peers from cooperative ones based solely on local observations of AODV routing protocol behaviours. They use a finite state machine model of locally observed AODV actions to construct a statistical description of each peer’s behaviour. In order to distinguish between selfish and cooperative peers, a series of well-known statistical tests are applied to features obtained from the observed AODV actions. An interesting extension of this work would be to consider various patterns of node mobility, which can give additional insights.

In Zoudraki, Mark, Hejmo, and Thomas’ (2005) work, a trust establishment mechanism for MANETs, called Herms, was introduced to improve the reliability of packet forwarding over multi-hop routes in the presence of potentially malicious nodes. Essentially, direct observations are used to evaluate opinions about others. Also, confidence levels are used as a weight to evaluate the trust of other nodes based on a Bayesian approach. They also introduced a windowing scheme to systematically expire old data to maintain accuracy of the opinion metric in the face of dynamics. However, this scheme is vulnerable to attacks that can exploit the windowing scheme to disseminate false information to accuse good nodes and keep bad nodes in the system (such as badmouthing attacks).

In Sun, Yu, Han, and Liu's (2006) work, trust modelling and evaluation methods were proposed for secure ad-hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using entropy. In their definition, trust is a continuous variable and does not need to be transitive, thus capturing some of the characteristics of trust in MANETs. However, this work considers packet dropping as the only component of direct observations to evaluate trust.

The trust-aware routing protocol (TARP) (Abusalah, Khokhar, & Guizani, 2008) was proposed, and a trust metric based on six trust components—software configuration, hardware configuration, battery power, credit history, exposure, and organizational hierarchy—was developed.

A distributed mechanism was proposed by Soltanali, Pirahesh, Niksefat, and Sabaei (2007) to deal with selfish nodes, as well as to encourage cooperation in MANETs based on the combination of reputation-based and currency-based incentive mechanisms, mitigating their defects and improving their advantages. Compared to existing works, this work considers more aspects of trust, such as dynamicity, weighted transitivity, and subjectivity. However, it used only packet forwarding behaviours to evaluate a node's trust and standard performance metrics to evaluate the proposed trust scheme.

A trust model was developed by Balakrishnan, Varadharajan, Tupakula, and Lucs (2007) to strengthen the security of MANETs and deal with the issues associated with recommendations. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR.

In Moe, Helvik, and Knapskog's (2008) work, a trust-based routing protocol was proposed that was an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In this work, selfish nodes are benign and selectively drop packets. Performance characteristics of the protocol when malicious nodes perform active attacks, such as packet modifications or identity attacks, need to be investigated further.

In Ayachi, Bidan, Abbes, and Bouhoula's (2009) work, implicit trust relations in AODV were formalized and demonstrated that a node can utilize these trust relations to isolate malicious nodes for secure routing. Nodes overhear neighbours' transmissions, from which they can build a neighbour routing table and check for deviation from normal behaviours for AODV. This scheme can detect malicious behaviours, such as message replication, message forgery, and some instances of message modification. However, it is not agreeable to the incorporation of other trust metric components, such as intimacy and competence, but monitored behaviours could feed into a trust evaluation scheme. Table 4-4 provides a summary of the trust management schemes.

Table 4-4: Summary of trust management schemes

Trust Management Scheme	Methodology	Scheme Features	Protocol
Reputation-based trust management scheme	Trust evaluation by direct observation	Watchdog and parthrater	DSR
Context-aware inference scheme	Direct Observation Reputation	Context-aware mechanism to detect malicious nodes	DSR
COllaborative REputation (CORE)	Direct Observation Reputation	Differentiates direct, indirect, and functional reputation	DSR
Secure and Objective Reputation-based Incentive (SORI)	Direct Observation Reputation	Encourages package forwarding, discourages selfish behaviour	DSR
Trust-based adaptive AODV	N/A	Adjusts security level at each node	AODV
Extension of AODV based on subjective logic	Direct Observation Recommendation	Considers system performance aspects by dealing with each query based on its level of trust	AODV
Specification-based approach as an extension to AODV	Direct Observation Reputation	Observe AODV actions and apply statistical methods to distinguish selfish and cooperative peers	AODV
Herms – trust establishment mechanism	Direct Observation Reputation	Herms – direct observations used for evaluation; Bayesian approach to evaluate confidence level; window scheme to remove old data	Ad-Hoc Networks
Trust modelling and evaluation	Direct Observation Recommendation	Trust is a continuous variable calculated using entropy; packet dropping to evaluate trust	Ad-Hoc Networks
Trust Aware Routing Protocol (TARP)	Direct Observation Recommendation	Trust based on six components	Ad-Hoc Networks
Distributed mechanism to deal with selfish nodes	Reputation and incentive based mechanism	Packet forwarding to evaluate trust	DSR
Security of MANETs	Direct Observation Recommendation	Utilizes only trusted routes, isolates malicious nodes based on observation	DSR
DSR extension based on incentive mechanism	Direct Observation Recommendation	Enforces cooperation among nodes, reduces benefits for selfish nodes	DSR
Trust mechanism based on relationships	Direct Information	Utilize trust relation to isolate malicious nodes based on previous records	AODV

4.4 Trust Protocols and Management Schemes for UAV Applications

Based on the above classifications of trust-based routing protocols and management schemes, the following table (Table 4-5) proposes several UAV applications where such protocols and schemes can be adopted.

Table 4-5: Trust Protocols and Schemes for UAV Applications

Protocol	**Features**	**UAV Applications**	**Management Schemes**
Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes	Isolates malicious nodes acting independently or in collision	Agriculture and environmental management, oil field detection, geospatial and surveying activities, wildlife monitoring	Context aware inference scheme
Trust-Embedded AODV (T-AODV)	Model also works for colluding malicious nodes	Wildlife monitoring, disaster damage assessment	Trust-based adaptive AODV
Incorporating Trust and Reputation in the DSR Protocol	Divided into three components: trust agent, reputation agent and the combiner	Geo-spatial and surveying activities, agriculture and environmental management	COllaborative Reputation (CORE), Secure and Objective Reputation-based Incentive (SORI)
Dependable Dynamic Source Routing Protocol	Each node monitors its neighbours and updates trust	Guidance, border patrol, port inspection	Reputation-based trust management scheme
TR-DSR: A routing protocol based on trust	Reduces routing traffic by forwarding requests to selected nodes	Natural disaster control and monitoring, natural disaster damage assessment	Security of MANETs
Opinion-Based Trusted Routing Protocol (TAODV)	Trust is represented by opinion as used in subjective logic	Civil security control, oil field detection	Extension of AODV based on subjective logic
Dynamic Mutual Trust-Based Routing protocol (DMTR)	Contains three components: the requestor, the decision maker, and the executant	Wildlife monitoring, agriculture and environmental management	Distributed mechanism to deal selfish nodes
FACES: Friend-Based Routing Protocol	Can handle many attacks	Traffic and crowd management, merchandise delivery, guidance, emergency response, civil security, pipeline monitoring, natural disaster control and monitoring	Trust mechanism based on relationships.
Trust-Based on-Demand Multipath Routing Protocol	Meets the trust requirement of the data packets	Wearable devices, traffic control and crowd management	Distributed mechanism to deal selfish nodes

4.5 Trust Management Issues in UAV Networks: A Case Study

Trust is defined as a belief level that one node can put on another node for a specific action according to previous direct or indirect information from its observation of behaviours. The belief level is the extent to which one node believes that another node is willing and able to obey the protocol and act normally. It is built on collected information from observations for a specific action (Li, Li, & Kato, 2008).

There are several trust-based protocols developed for MANETs to ensure secure communications among them. As the characteristics of UAVs and MANETs are similar, UAVs can be considered as nodes in MANETs, and these protocols can be applied to UAV networks.

The use of trust-based routing protocols will improve the integrity of the received data at the receiver node. The design of secure and stable routing protocols for MANETs is an active research area. Cooperation among nodes is necessary to sustain the integrity of network operations.

Managing trust in a UAV network is challenging when collaboration or cooperation is critical to achieving mission and system goals, such as reliability, availability, scalability, and re-configurability. Due to the unique characteristics of their environments and the inherent unreliability of wireless channels, several trust issues need to be addressed. Their dynamic nature and characteristics result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time. Several trust management issues are presented below.

4.5.1 Lack of Centralized Management

MANETs do not have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor traffic in a highly dynamic and large-scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

4.5.2 Cooperativeness

Routing algorithms usually assume that nodes are cooperative and non-malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

4.5.3 Dynamic Topology

Dynamic topology and changeable node membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behaviour could be better protected with distributed and adaptive security mechanisms.

4.5.4 Adversary inside the Network

Mobile nodes can freely join and leave the network. The nodes within the network may also behave maliciously. This malicious behaviour of the nodes is hard to detect. Thus, this attack is more dangerous than external attacks. These nodes are called compromised nodes.

4.5.5 Resource Availability

Resource availability is a major issue in MANETs. Providing secure communications in such a changing environment, as well as protection against specific threats and attacks, leads to the development of various security schemes and architectures. Collaborative ad-hoc environments also allow the implementation of self-organized security mechanisms.

4.5.6 Integrity

Integrity means that the nodes can be modified only by authorized parties or only in an authorized way. Modification includes writing, changing statuses, deleting, and creating. Integrity assures that a message being transferred is never corrupted.

Chapter 5: Conclusion and Future Works

5.1 Conclusions and Contributions

Using UAVs in many applications offers several advantages. Unlike manned aircraft, UAVs can be operated more economically. They are less limited by weather conditions for some advanced models, and they are easier to deploy. They can be operated in geographically challenging locations without putting any personnel at risk. In order to perform their tasks efficiently, trust-based communication among UAVs is a very important factor. As UAVs and MANETs share common characteristics, trust-based MANET models can be used as a basis for trust-based UAV communication. Consequently, UAVs can take advantage of existing research on trust-based MANET systems to ensure secure communication.

This thesis presented the various UAV models, their types, and their applications in different domains. It then elaborated on trust-based UAV communication, which introduced related trust-based communication protocols, trust management schemes, and various other issues. The main contributions of this thesis are the following:

- Characterization of different UAV-based networking architectures.
- Identification of the characteristics and issues in MANET protocols to provide efficient UAV-based communication.
- Classification of different data traffic types for efficient UAV-based communication in various applications and environments.
- Classification of trust-based protocols and management schemes that can be adopted by UAVs.
- Comparison of the communication requirements between military and civilian applications.

- Providing a case study on UAVs and their applications in smart cities.
- Identification of different applications of UAVs for United Arab Emirates.
- Classification of the trust protocols and schemes that are appropriate for various UAV applications.

5.2 Future Work

UAV-based communication is a very important field of research. Although some research has been done in this area, much more work is still needed in order to provide reliable, trusted and secure communication in UAV-based systems and their applications. For example, further investigations can be conducted in order to identify, enhance, and extend existing MANET protocols to be better adapted for the UAV communication environment and its special characteristics, which were identified earlier in this thesis. Furthermore, additional research can be done in order to provide better support of the various data traffic types that are used in different UAV system applications. Finally, UAV deployment and use in smart cities is very promising. However, it is in its early stages, and further analysis and research is needed to provide for efficient integration of the UAV systems into the various smart city environments.

Bibliography

Abusalah, L., Khokhar, A., & Guizani, M. (2008). A Survey of Secure Mobile Ad Hoc Routing Protocols. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*.

Adams, W. J., Hadjichristofi, G. C., & Davis IV, N. J. (2005). Calculating a Node's Reputation in a Mobile Ad Hoc Network. IEEE.

Al-Jaroodi, J., & Mohamed, N. (2012). Service-Oriented Middleware: A Survey. *The Journal of Network and Computer Applications*.

Ayachi, M. A., Bidan, C., Abbes, T., & Bouhoula, A. (2009). Misbehavior Detection using Implicit Trust Relations in the AODV Routing Protocol. *International Conference on Computational Science and Engineering.* IEEE.

Balakrishnan, V., Varadharajan, V., Tupakula, U. K., & Lucs, P. (2007). Trust and Recommendations in Mobile Ad hoc Networks. *Third International Conference on Networking and Services.* IEEE.

Bekmezci, I., Sahingoz, O. K., & Temel, S. (2013). Flying Ad-Hoc Networks (FANETs): A survey. Elsevier.

Bo, C., Yang, Z., Peng, Z., Hua, D., Xiaoxiao, H., Zheng, W., & Junliang, C. (2010). Development of Web-Telecom based Hybrid Services Orchestration and Execution Middleware over Convergence Networks. *Journal of Network and Computer Applications*.

Bouachir, O., Abrassart, A., Garcia, F., & Larrieu, N. (2014). A Mobility Model For UAV Ad hoc Network. *International Conference on Unmanned Aircraft Systems.* IEEE.

Canadian businesses harness drone technology. (2014).[online]. Retrieved June 04, 2014, from http://www.cbc.ca/news/canada/canadian-businesses-harness-drone-technology-1.2631329

Cho, J.-H., Swami, A., & Chen, I.-R. (2011). A Survey on Trust Management for Mobile Ad Hoc Networks. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*.

Chuanhe, H., Yong, C., Wenming, S., & Hao, Z. (2004). A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks. *Aerospace Conference.* IEEE.

Chuanhe, H., Yong, C., Wenming, S., & Hao, Z. (2009). A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks. IEEE.

Constine, J. (2014). *Facebook Will Deliver Internet Via Drones With "Connectivity Lab" Project Powered By Acqhires From Ascenta*. [online]. Retrieved June 04, 2014, from http://techcrunch.com/2014/03/27/facebook-drones/

Corrigan, C., Roberts, G., Ramana, M., Kim, D., & Ramanathan, V. (2008). Capturing vertical profiles of aerosols and black carbon over the Indan Ocean using autonomous unmanned aerial vehicles. Copernicus Publication.

Curry, J., Maslanik, J., Holland, G., & Pinto, J. (2004). Applications of Aerosondes in the Arctic. *American Meteorological Society*.

Curry, R. (2014). *First Flights in UK Airspace For Global Hawk*. [online]. Retrieved from UAS Vision: http://www.uasvision.com/2014/06/02/first-flights-in-uk-airspace-for-global-hawk/

Dai, C., Li, Y., & Zhai, W. (2010). *Communication among UAVs.*

Dent, S. (2015, April 15). *Nixie is a wearable drone that captures your activities on the fly*. [online]. Retrieved from http://www.engadget.com/2014/09/29/nixie-wearable-drone/

Design, A. (2014). *SUAS*. [online]. Retrieved from PhotoShip one: http://photoshipone.com/suas-2/

Dhurandher, S. K., Obaidat, M. S., Verma, K., Gupta, P., & Dhurandher, P. (2011). FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems. *IEEE Systems Journal*.

Drone Ambulance Saves Lives, Radio Television Russia. (2014). [online]. Retrieved from http://rt.com/news/200675-drone-ambulance-saves-lives/.

Dronologista. (2014). *Human Side of UAVs – easyJet To Introduce Drones*. [online]. Retrieved from https://dronologista.wordpress.com/2014/08/01/human-sides-of-uavs-easyjet-to-introduce-drones/

EasyJet to use unmanned drones to inspect its aircraft. (2014). [online]. Retrieved June 04, 2014, from theguardian: http://www.theguardian.com/business/2014/may/07/easyjet-unmanned-drones-inspect-airbus-aircraft

Estes, A. C. (2014). *Dubais turning drones into firefighters*. [online]. Retrieved from http://gizmodo.com/dubais-turning-drones-into-firefighters-1505685714

Federal Aviation Administration. (2014). [online]. Retrieved from http://www.faa.gov/

Franke, U. E. (2013). *The Five Most Common Media Misrepresentations of UAVs.* London: The Royal United Services Institute for Defence and Security Studies.

Frew, E. W., & Brown, T. X. (2008). Airborne Communication Networks for Small Unmanned Aricraft Systems. *IEEE.*

Ghosh, T., Pissinou, N., & Makki, K. S. (2004). Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks. *International Conference on Local Computer Networks.* IEEE.

Ghosh, T., Pissinou, N., & Makki, K. S. (2005). Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks. *Mobile Networks and Applications.* Springer.

Glade, D. (2000). *Unmanned Aerial Vehicles: Implications for Military Operations.* Center For Strategy and Technology Air War College.

Goyal, P., Parmar, V., & Rishi, R. (2011). MANET: Vulnerabilities, Challenges, Attacks, Application. *International Journal of Computational Engineering and Management*.

Groba, C., Braun, I., Springer, T., & Wollschlaeger, M. (2008). A Service-Oriented Approach for Increasing Flexibility in Manufacturing. *International Workshop on Factory Communication Systems.* IEEE.

He, Q., Wu, D., & Khosla, P. (2004). SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks. *Wireless Communications and Networking Conference.* IEEE.

Heutger, M., & Kückelhaus, M. (2014). *Unmanned Aerial Vehicles in Logistics: A DHL Perspective on Implications and Use for the Logistics Industry*. Retrieved from http://www.dhl.com/content/dam/downloads/g0/about_us/logistics_insights/dhl_trend_report_uav.pdf.

Huo, J., Xu, Z., Zhang, Y., & Shan, X. (2011). A UAV mobile strategy in mobile ad hoc networks. IEEE.

Idries, A., Mohamed, N., Jawhar, I., Mohammed, F., & Al-Jaroodi, J. (2015). Challenges of Developing UAV Applications: A Project Management View. *5th International Conference on Industrial Engineering and Operations Management* . IEEE.

Jawhar, I., Mohamed, N., & Al-Jaroodi, J. (2014). Data Communication in Linear Wireless Sensor Networks Using Unmanned Aerial Vehicles. *International Conference on Unmanned Aircraft Systems (ICUAS).* Orlando: IEEE.

Kharchenko, V., & Prusov, D. (2012). Analysis of unmanned aircraft systems application in the civil field. Taylor and Francis Group.

Kukreja, D., Singh, U., & Reddy, B. (2013). A Survey of Trust Based Routing Protocols in MANETs. *Journal of Advances in Computer Networks, 1*(4).

Li, J., Li, R., & Kato, J. (2008, April). Future Trust Management Framework for Mobile Ad Hoc Networks. *SECURITY IN MOBILE AD HOC AND SENSOR NETWORKS*.

Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2009). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security*.

Li, X., Lyu, M. R., & Liu, J. (2004). A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. *Aerospace Conference Proceedings.* IEEE.

Liu, Z., Joy, A. W., & Thompson, R. A. (2004). A Dynamic Trust Model for Mobile Ad Hoc Networks. *International Workshop on Future Trends of Distributed Computing Systems.* IEEE.

Madrigal, A. (2011). *Inside the Drone Missions to Fukushima*. [online]. Retrieved from http://www.theatlantic.com/technology/archive/2011/04/inside-the-drone-missions-to-fukushima/237981/

Marti, S., Giuli, T., Lai, K., & Baker, M. (2000). Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *MobiCom 2000 Proceedings of the 6th annual international conference on Mobile computing and networking* . ACM.

McCray, G. (2014). *A Drone of your own*. [online]. Retrieved from Quadcopters are fun: http://quadcoptersarefun.com/ADroneOfYourOwn.html

Michiardi, P., & Molva, R. (2002). CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. Springer.

Moe, M. E., Helvik, B. E., & Knapskog, S. J. (2008). TSR: trust-based secure MANET routing using HMMs. *Symposium on QoS and Security for Wireless and Mobile Networks* . ACM.

Mohamed, N., & Al-Jaroodi, J. (2011). A Survey on Service-Oriented Middleware for Wireless Sensor Networks. *Service Oriented Computing and Applications*.

Mohamed, N., & Al-Jaroodi, J. (2013). Service-Oriented Middleware for Collaborative UAVs. *The 14th IEEE International Conference on Information Reuse and Integration.* IEEE.

Mohamed, N., Al-Jaroodi, J., Jawhar, I., & Lazarova-Molnar, S. (2013). Middleware Requirements for Collaborative Unmanned Aerial Vehicles . *International Conference on Unmanned Aircraft Systems (ICUAS).* IEEE.

Mohamed, N., Al-Jaroodi, J., Jawhar, I., & Lazarova-Molnar, S. (2014). A Service-Oriented Middleware for Building Collaborative UAVs. *Journal of Intelligent & Robotic Systems*.

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). Opportunities and Challenges of Using UAVs for Dubai Smart City. *NTMS.* Dubai: IEEE.

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). UAVs for Smart Cities: Opportunities and Challenges. *The 2014 International Conference on Unmanned Aircraft Systems (ICUAS'14).* IEEE.

Nekkanti, R. K., & Lee, C.-w. (2004). Trust Based Adaptive On Demand Ad Hoc Routing Protocol. *Proceedings of the 42nd Annual Southeast Regional Conference* . ACM.

Nieva , R., & Rosenblatt, S. (2014). *Google spreads its wings, moving into drone deliveries*. [online].Retrieved from http://www.cnet.com/news/google-announces-project-wing-for-drone-deliveries/.

Oller, A., Lacroix, S., Merino, L., (. . .), Caballero, F. (2005). Multiple eyes in the skies: architecture and perception issues in the COMETS unmanned air vehicles project . *IEEE Robotics & Automation Magazine*.

Paul, K., & Westhoff, D. (2002). Context aware detection of selfish nodes in dsr based ad-hoc networks. IEEE.

Pirzada, A. A., & McDonald, C. (2007). Dependable dynamic source Routing without a trusted third party. *Journal of Research and Practice in Information Technology*.

Pirzada, A. A., Datta, A., & McDonald, C. (2006). Incorporating trust and reputation in the DSR protocol for dependable routing. *Computer Communications*.

Safa, H., Artail, H., & Tabet, D. (2009). A cluster-based trust-aware routing protocol for mobile ad hoc networks. Springer.

Saggiani, G., & Teodorani, B. (2004). Rotary wing UAV potential applications: an analytical study through a matrix method. Emerald.

Sahingoz, O. K. (2013). Mobile Networking with UAVs: Opportunities and Challenges. *International Conference on Unmanned Aircraft Systems.* IEEE.

Shah, R. C., Roy, S., Jain, S., & Brunette, W. (2003). Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks. IEEE.

SkyCall. (2014). [online]. Retrieved from http://senseable.mit.edu/skycall/

Smith, M. (2013). *Amazon Prime Air drones revealed on 60 Minutes, aim to deliver in half an hour*. [online]. Retrieved from engadget: http://www.engadget.com/2013/12/01/amazon-prime-air-drones/

Soltanali, S., Pirahesh, S., Niksefat, S., & Sabaei, M. (2007). An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks. *Third International Conference on Networking and Services.* IEEE.

Sun, Y. L., Yu, W., Han, Z., & Liu, K. R. (2006). Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*.

Taylor, G., Irving, M., Hobson, P., Huang, C., Kyberd, P., & Taylor, R. (2006). Distributed Monitoring and Control of Future Power Systems via Grid Computing. *Power Engineering Society General Meeting.* IEEE.

Tuna, G., Nefzi, B., & Conte, G. (2013). Unmanned aerial vehicle-aided communications system for disaster recovery. *Journal of Network and Computer Applications*.

Wang, B., Soltani, S., Shapiro, J., & Tan, P.-N. (2005). Local Detection of Selfish Routing Behavior in Ad Hoc Networks. *Journal of Interconnection Networks*.

Wang, C., Yang, X., & Gao, Y. (2005). *A Routing Protocol Based on Trust for MANETs.* Springer.

Zajkowski, T., Dunagan, S., & Eilers, J. (2006). Small UAS Communications Mission. *11th Biennial USDA Forest Service Remote Sensing Application Conference.*

Zoudraki, C., Mark, B., Hejmo, M., & Thomas, R. (2005). A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs. *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks.* ACM.

List of Publications

Idries, A., Mohamed, N., Al-Jaroodi, J., Jawhar, I. & Mohammed, F. (2015). *Challenges of Developing UAV Applications: A Project Management View*. Fifth International Conference on Industrial Engineering and Operations Management 2015. *IEOM.* Dubai: IEEE.

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J. & Jawhar, I. (2015). *Integrating Unmanned Aerial Vehicles with Smart Cities*. Journal of Intelligent and Robotic Systems, Springer (pending).

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). Opportunities and Challenges of Using UAVs for Dubai Smart City. *NTMS.* Dubai: IEEE.

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). UAVs for Smart Cities: Opportunities and Challenges. *The 2014 International Conference on Unmanned Aircraft Systems (ICUAS'14).* Orlando: IEEE.