Aircraft Vehicular Ad-Hoc Network (AVANET)

Krishan Kumar
Department of Computer Science, Invertis Institute of Management Studies, Bareilly, kumar_krishana@yahoo.com

ABSTRACT
In this paper I have presented a new concept AVANET (Aircraft Vehicular Ad Hoc Network) and propose some potential applications aimed at assisting pilots, this concept has been derived from the concepts of vehicular ad hoc network. In this chapter I have proposed a concept of vehicular ad hoc network to communicate among aircrafts. In vehicular ad hoc networks individual vehicles can help each other, locate resources and establish trustworthiness under highly dynamic conditions, lacking any centralized trust authority. To ascertain the accuracy and reliability of data aggregated in a distributed manner, I present a system (AVANET) for such networks that enables devices to quickly adapt to changing local conditions. Our objective in this paper is to explore the security-related challenges in this envisaged setting. While this chapter presents no solid technical results, I believe that it provides a valuable analysis of an environment that is very likely to become real in the near future. In particular, it describes one instantiation of an information infrastructure for en-route pilot assistance: PAHNI (Pilot Ad Hoc Networking Infrastructure).

KEYWORDS
Air traffic control, AVANET(Aircraft Vehicular Ad Hoc Network), vehicular network

1. INTRODUCTION
With the air traffic controllers, aeronautical-specific communication protocols (e.g., ACARS3) are used over a satellite link or a terrestrial link based on VHF/HF3 or 1090 MHz Extended Squitter (1090-ES) [1]. As more and more aircrafts are equipped with GPS and Wi-Fi transmitters, it becomes easier to design systems that will allow aircrafts to interact autonomously with each other (Figure1). Indeed, aircraft manufacturers are already equipping their aircrafts with such devices. Though, currently these systems are a proprietary, I envision a natural evolution where agent applications shall be developed for vehicular systems, e.g., to improve car routing in dense urban areas. Using a simulation environment, which models a real transportation network in a space, I demonstrate the benefits achieved by self-congestion of aircrafts in air by using vehicular ad hoc network, and named it as aircraft vehicular ad hoc network. In this problem, it is assumed that all aircrafts are moving in a horizontal plane (Figure1). Our investigation is a feasibility study of the use of symmetric primitives, resulting in some efficiency improvements of potential value. More specifically, I develop a realistic trust model, and an architecture that supports our concept.

2. MOTIVATION
Motivation for this paper has arisen from a paper [2] which focuses on security concerns with a future ad hoc network of data linked eEnabled airplanes [3], and proposes a framework to protect communications. The framework identifies emerging threats and vulnerabilities, specifies security requirements and mitigation solutions. Major security challenges anticipated in the ground infrastructure and eEnabled airplanes are presented along with some open problems. Also incidents like crashes [4] lost of aircrafts, vehicle breakdowns etc. lead to disruption of the normal flow of traffic. Such events when detected should be quickly propagated for timely adaptation by affected vehicles. Existing methods of propagating traffic information like broadcast media (radio, TV) and dynamic message boards lack detail and personalization. Also, current mechanisms are centralized, i.e., event reports have to gain back to some collection center and then rebroadcast over local agents in aircraft cockpit. Such information is usually periodically available and is often delayed. Moreover, notification of such traffic incidents often lack a detailed description of the event, which is likely to mislead the pilot, or belated – leaving no time to adapt or feIr choices to adapt. Effective adaptation to traffic conditions will depend on the ability of Traffic Information Systems (TIS) to provide detailed, reliable, timely, and localized information to vehicles likely to be affected.

I consider vehicular networks which are hybrid in nature i.e. networks with both an infrastructure based and an ad hoc network component [6]. Because of high mobility nature of vehicles, one might argue that the vehicular network should be implemented using a pure ad hoc architecture, allowing groups of nodes to exchange information without the need of an authority or infrastructure. HoIver, there are clear benefits associated with a hybrid solution, where a backbone service provider can provide various services. These will in turn act as incentives for collaboration among users, and for not disconnecting from the network. I do not consider partial disconnection of devices, in which users have some functionality disabled, but not all. Our motivation for this is the increased sophistication required for such an attack. I distinguish betten two main categories of communication in our hybrid network [5].
3. ASSUMPTIONS
It is assumed in AVANET that cryptographic and security
counties are properly managed and protected. Sufficient
protection is provided for robustness against Ill known denial
of service attacks. In case of a network system failure, asset
distribution via physical media is assumed adequate to meet
requirements for timely data delivery from an aircraft in some
applications, such as for delivery of software. Further, airlines
are assumed capable of managing configurations and health of
their fleet in a reliable and correct manner. Sufficient physical
security checks are in place to prevent unauthorized cabin
access to onboard systems. Additionally, the air traffic
controllers are assumed to properly conduct the traffic
management tasks. Third party service providers are not
considered responsible for airplane operation. The main
elements and assumptions of the envisaged AVANET
infrastructure are as follows:

3.1 LOCATION AWARENESS
I expect that, in the near future, most aircrafts will be equipped
with GPS receivers providing fairly accurate geographical
position coordinate.

3.2 AD HOC NETWORKING
Many high-end aircrafts are already being equipped with
sophisticated computing components interconnected via a
wireless Local Area Network (LAN). This trend will very
likely extend into wireless networking. In particular, I assume
that short-range wireless ad hoc networking for inter-vehicle
communication will become ubiquitous.

3.3 ACCESS TO FIXED INFRASTRUCTURE
A fixed infrastructure, comprised of (at least) a number of base
stations (e.g. ATC toI) strategically positioned in close
proximity to the highways, is necessary to facilitate the upload
of data from the aircrafts. This data can be used for monitoring
current traffic conditions, as Ill as managing traffic. Vehicles
elsewhere can also query the fixed infrastructure for trip
planning purposes.

4. SYSTEM OVERVIEW
Consider a space area with some aircrafts. Pilots and
passengers in these vehicles are interested in information
relevant to their trip. For example, a pilot would like
his/her vehicle to continuously display on a map, at any time, the
available spaces around the current location of the
aircraft. Or, the pilot may be interested in the traffic
conditions one mile ahead. Such information is
important for drivers to optimize their travel, to alleviate traffic congestion, or to avoid wasteful driving. The challenge is processing queries in this highly mobile environment, with an acceptable delay, overhead and accuracy. One approach to solving this problem is maintaining a distributed database stored at fixed sites that is updated and queried by the moving vehicles via the infrastructure wireless networks.

In Figure1 I depict a typical scenario for our system. Several aircrafts travel on a highway while communicating locally, via an ad hoc wireless network, and globally, via a fixed infrastructure wireless network. Each aircraft is outfitted with a laptop or PDA equipped with a wireless LAN card (e.g., 802.11) for local communication, and a wide-area wireless device (e.g., a cellular phone) for the connectivity to the infrastructure network. Each aircraft forms, around itself, a local area of communication. Aircrafts that are further away, although they may constitute part of a neighbor’s local area, are not part of that particular aircraft’s communication network. All aircraft broadcast information omni-directionally and receive data from all directions.

There is no point-to-point communication link. The purpose of the ad hoc network is to impart information, i.e., the aircraft’s vital signs, to vehicles in close proximity and to receive the same data from them. The information is processed locally to provide the driver with a map indicating the status of each aircraft in the immediate vicinity, e.g., speed signal, bearing angle, signal status, braking, etc. A sample Aircraft Immediate Vicinity Awareness (AIVA) screen is depicted in Figure2; it shows some potential vital signs that may be reported.

In addition to the local ad hoc network, each vehicle also communicates, at a much lower frequency rate, with the infrastructure network in order to upload its vital signs. This data is used by the infrastructure for maintaining up to date traffic conditions and for performing traffic management. It also constitutes the highly dynamic database that pilots can query to extract traffic and trip planning information. This refers to the Enroute Traffic Condition Helper (ENTRACH).

I envision that, in addition to communication and processing devices, each vehicle will also be outfitted with a GPS receiver and sensors that collect information regarding the vital signs of the aircraft. Furthermore, each aircraft will have, on each of its four sides, a simple detection device that will monitor the presence (or absence) of another vehicle in the immediate vicinity. This feature is necessary to ensure a safe system that is not prone to the vagaries of wireless communication. Figure3 illustrates a sample unit (i.e., laptop or PDA) that will be fitted into each vehicle with its corresponding communication, GPS links and sensor feeds.

5. APPLICATIONS

The AVANET infrastructure provides numerous possibilities to revolutionize the automotive and transportation industry of the future. For example, data captured by AVANET, when
properly aggregated, can be fed into the traffic monitoring and flow control system for real-time traffic [7] management. Alternatively, such information can be archived for off-line analysis to understand traffic bottlenecks and devises techniques to alleviate traffic congestion. There are numerous application possibilities and scenarios.

One of the most compelling AVANET application examples is what I call “Aircraft Immediate Vicinity Awareness” or AIVA for short. AIVA aims to communicate to each vehicle vital signs (Figure 2) of other vehicles travelling in close proximity. Proximity in this context means the area that falls within direct range of transmission of the wireless networking device found in each vehicle. Such vital signs may include the status of bearing angle, signal indicator, relative/absolute speed, headlights etc. It is important to note that all of these signs are, in any case, intended for external display, e.g., the status of the turn signal is always in plain view. In other words, no new information that might be construed as private is intended for communication outside a vehicle. I anticipate that the information collected by AIVA will assist the pilots by offering them better awareness of their immediate surroundings as III as of the current and intended behavior of the nearby vehicles. Pilots shall be able to better concentrate on the trajectory ahead if they no longer have to look sideways to observe flanking and tailgating vehicles. Also, notorious blind spots can be effectively eliminated if pilots are continuously made aware of the surrounding space. Furthermore, traffic conditions ahead can be observed faster if pilots are warned of activity, one or two vehicles ahead. Consequently, I expect AIVA to increase trajectory safety by preventing some accidents.

Another, very different, application has to do with trip planning. I refer to it as “Enroute Traffic Condition Helper” or ENTRACH for short. In it, vehicles communicate directly to the fixed infrastructure (base stations) and report their vital signs (as above) as III as the speeds of surrounding vehicles. This information is then efficiently gathered and coalesced into regional traffic snapshot databases. Vehicles, both on and off the highway, can query these databases and obtain immediate information on traffic conditions towards intended destinations.

6. RELATED WORK

Due to their enormous potential, vehicular ad hoc [8] networks have gained an increasing attention in both industry and academia. Methods and apparatus are provided for a traffic warning system (TWS) for light aircraft by using ad hoc networks [9]. The need for security and privacy in vehicular networks was recognized early on [10]; it was not until very recently that the numerous challenges have started to spur some increased research interest. Zarki et al. [11] describe an infrastructure for driver assistance. In particular, they focus on immediate vehicle vicinity awareness and highway traffic conditions. In this context they discuss security requirements for the system which are met by introducing digital signatures and a public key infrastructure. Duri et al. [12] focus on assuring privacy and integrity of data in telematics applications. They present a comprehensive data protection framework which integrates security components based on standard protocols like SSL or IPSec. The work by Golle et al. [13] focuses on detecting and correcting malicious data. In [14], [15], Hubaux et al. provide a comprehensive discussion of security and privacy issues in vehicular networks. They propose solutions based on the use of digital signatures and anonymous public keys.

A basic architecture of an airborne ad hoc network is established in [1]. The relationship between network connectivity and information reachability, which accounts for information latency and depends on transmission protocols, is discussed. Two general performance criteria are introduced that measure the connectivity performance of an airborne network subject to a specified maximum number of hops in the network. The data exchanged in vehicular networks can range from information pertaining to the vehicle itself to timing information and information observed in close proximity or surroundings. The richness of data is meaningful to transmit in cases of emergency, as it may allow for faster dispatch of appropriate emergency services, or get precisely personalized service such as auditing. I only require loose time synchronization (by the authorities) for the interpretation of
collected data; these will infer the local times of nodes originating and forwarding data. For practical purposes, authorities may also push clock corrections to nodes it communicates with.

7. SOME CONSTRAINTS
Any new mechanism or requirement from the AVANET must be integrable with the existing ill-defined regulations. Average lifetime of a typical commercial plane, and hence of its assets, is in the order of several decades. Time-dependent requirements for the airplane assets must take this constraint into account. The constraint also imposes the need for long-term solutions. Further, the different phases of flight can be categorized into three operational stages: on-the-ground, takeoff or landing, and in-flight. The time period of each operational stage of the airplane is fixed. Applications and mechanisms are therefore expected to function within these time constraints. Furthermore, some real-time operations of the airplane must be performed in a timely manner requiring computation and communication efficient solutions.

In its end-to-end flight, an airplane may traverse multiple airports with possible lack of network connectivity at one or more traversed airports. Additionally, the airplane may find varying network environment such as in terms of protocol standards, security technologies, and export restrictions [16]. The airplane may also interact with multiple on-board systems, e.g., airport wireless access point and airline systems. Solutions for the AVANET therefore must be adaptable and scalable to ensure seamless air travel for the airplane. Furthermore, airplanes follow predictable routes, except during free flight [17] and travel from one airport to another in an estimated trip time. Therefore, airplanes within communication range and moving in a similar direction can be expected to navigate as a group of nodes forming a fully connected network graph within the group. For example, ADS-B based on 1090-ES can provide a communication range betwen 40 to 90 nautical miles [1].

The airline fleet operation and maintenance costs must be reduced. Therefore, any proposed solution for the AVANET must minimize overhead at the airlines. Further, in order to obtain return-of-investment from existing systems and processes, any new technology must be compatible with legacy systems and processes in commercial aviation.

8. SECURITY REQUIREMENTS
We are actually dealing with an environment that is very dynamic and composed of high-motion vehicles. This results in rapidly changing networking topologies. In addition, data exchanged between the vehicles is extremely time sensitive. On the other hand, since the communication devices are mounted in vehicles, the power supply is unlimited. This makes it possible to use fairly large antennas and on-board GPS devices. Also, data is only of interest to a small set of neighboring vehicles.

8.1 CONFIDENTIALITY
Unauthorized access to sensitive assets that can be leveraged for future attacks or personal gain must be prevented.

8.2 INTEGRITY AND AUTHENTICITY
For preventing any corruption of assets by the adversary, the identity and content of the asset received at the destination must be verified to be the same as at the source. Further, the source identity must also be verified.

8.3 AUTHORIZATION
The verifiable identity of each entity accessing or distributing any asset in the AVANET must be checked to possess the appropriate permission and privilege.

8.4 CORRECT DETECTION
Any manipulation of an asset must be detected as soon as possible so as not to disrupt the predicted time for flight, while also eliminating or reducing false alarms.

8.5 NON-REPUDIATION
All actions performed on each asset must be logged in a format and for a time period that can satisfy both regulatory and airline needs. Further, for the purpose of forensics, the traceability of actions on each asset must be undeniably associated with at least one authorized entity.

9. CHALLENGES
It can be anticipated that the rapid advances currently witnessed in the networking, security and privacy of the emerging vehicular ad hoc networks (VANETs) can significantly benefit the airborne ad hoc networks [18], [19]. For instance, cooperative navigation and collision avoidance applications in VANET have the same objective as their counterparts in the airborne ad hoc networks. Interesting research may lie in leveraging design of secure solutions being developed in VANET, for mitigating threats to AVANET. For example, the position information broadcasts from airplanes approaching or navigating in an urban environment, such as terminal areas, can potentially present side channel information for unauthorized parties. In such scenarios, it may be useful to employ anonymous identifiers and mitigation of unauthorized location tracking in airborne ad hoc networks. Although existing literature argue for commonality among the safety and security disciplines [20], [21] it remains an open problem as to how the two fields can be combined. While security affects safety, it is not clear how to express the relevant security considerations and how to accommodate security risks and mitigations in the context of a safety analysis.

10. CONCLUSION AND FUTURE WORK
Traffic congestion is already a major problem worldwide and it is becoming more and more serious because the numbers of aircrafts in space are increasing at a higher rate than space capacity. This paper has introduced AVANET a novel traffic management system, which aims to optimize the usage of existing space capacity and effective communication among all the aircrafts in space. This is the hybrid approach of two
different technologies i.e. mobile ad hoc networks and vehicular network. This approach suggests a model which provides a high degree of efficiency coupled with security and privacy.

The development of security primitives for AVANET is an area that has not received a lot of attention to date. I believe there is a great need for a careful modeling of likely threats, and the development of matching security mechanisms. It may be worthwhile to consider the potential threat associated with an increased reliance on wireless communication for the smooth flow of traffic; for example, it may be important to study the potential impacts of DoS attacks on any VANET system; this aspect emphasizes the importance of using light-light cryptographic constructions. The AVANET promises applications that can significantly benefit next-generation air transportation systems. Our security analysis focused on information assets that could impact airplane operation, airplane maintenance and air traffic control, and provided a classification for major threats to the AVANET. I presented some of the challenges that can be expected with their use in the AVANET.

REFERENCES
[5]. Jong Youl Choi , Markus Jakobsson, Susanne Itzel, Balancing Auditable Privacy and Privacy in Vehicular Networks, Q2SWinet'05, October 13, 2005, Montreal, Quebec, Canada., ACM 1-59593-241-0/05/0010.
[8]. Chip (Brig) Elliott, Self Organizing and Self-Healing Ad-hoc Networks, WLAN 57- BBN Technologies Cambridge, MA, 02138, Presented at WLAN 2001 by Jerry Burchfield