

MODERN JETS, RETRO CIPHERS: HOW MONOALPHABETIC SUBSTITUTION CIPHERS ARE STILL IN USE

Matthew Smith^{*}, Daniel Moser^{\$}, Martin Strohmeier^{*},
Vincent Lenders[¥], Ivan Martinovic^{*}

^{*}University of Oxford
first.last@cs.ox.ac.uk

^{\$}ETH Zurich
first.last@inf.ethz.ch

[¥]armasuisse
first.last@armasuisse.ch

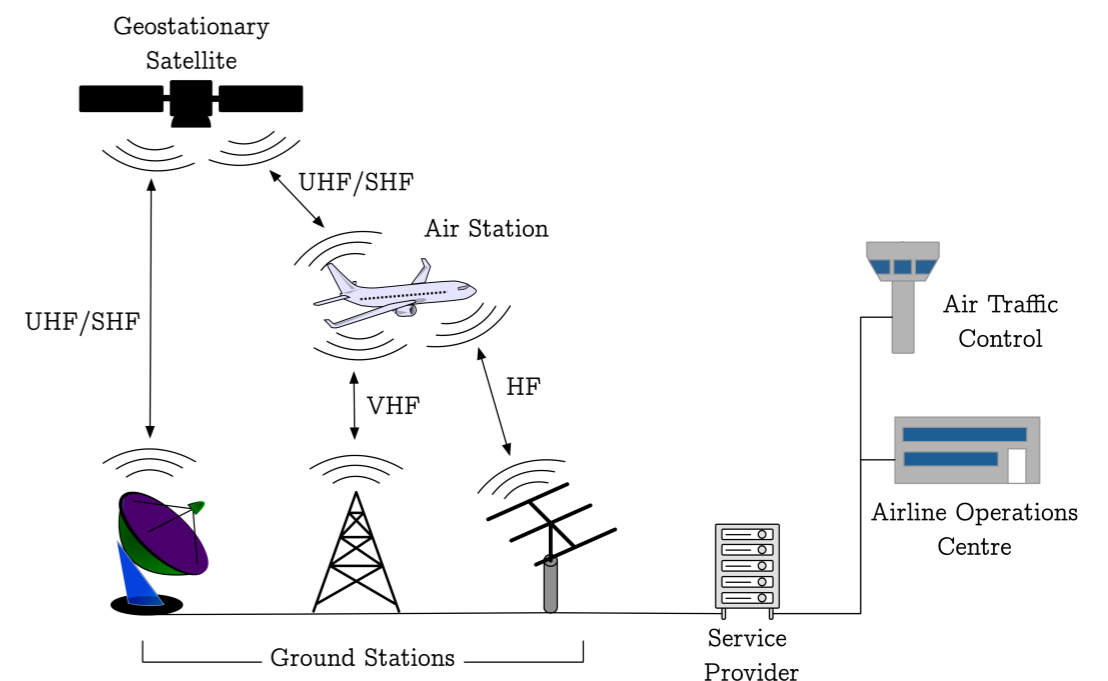
Real World Crypto 2018, January 10-12, Zurich



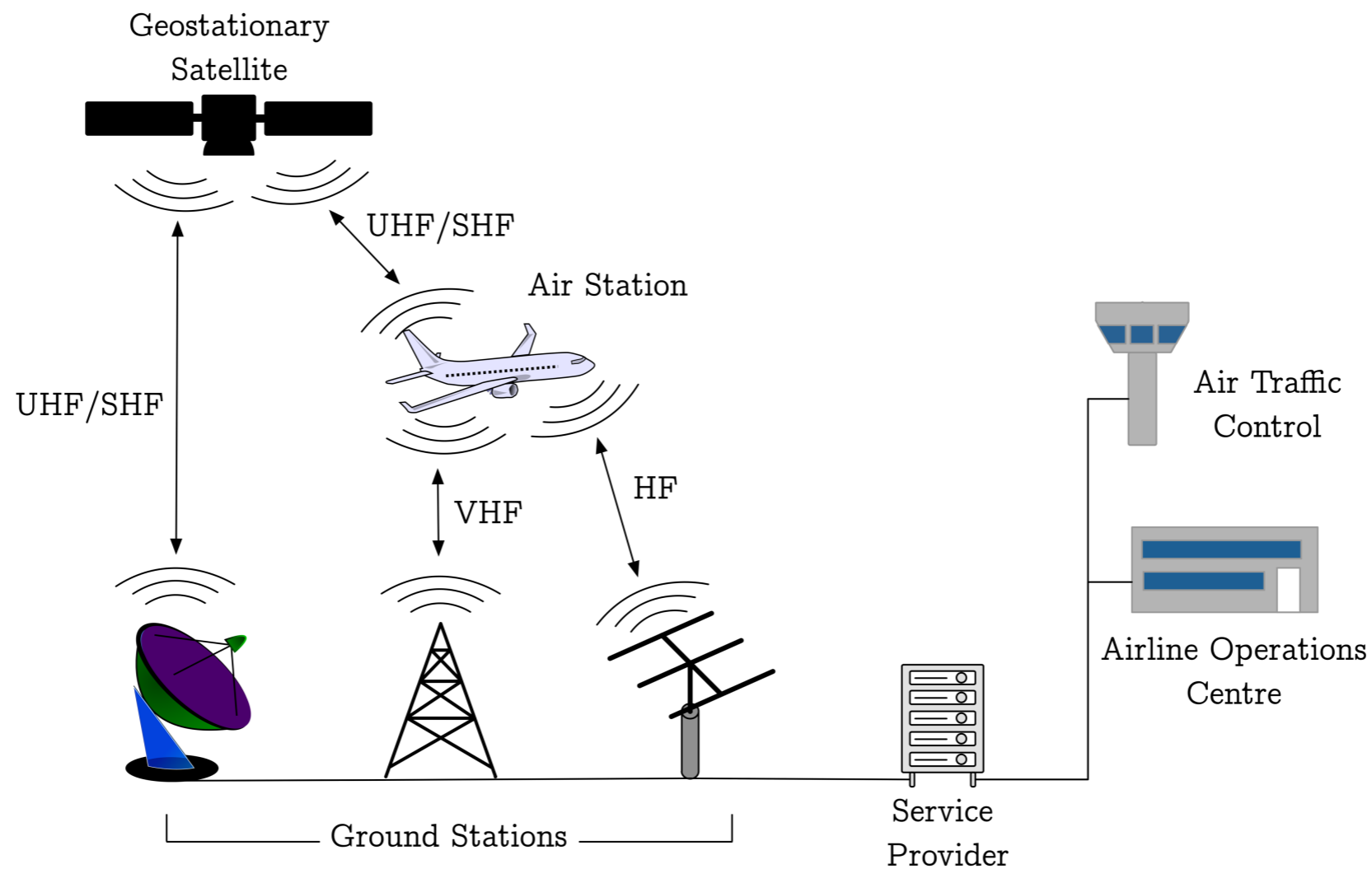
UNIVERSITY OF
OXFORD

WHAT IS ACARS?

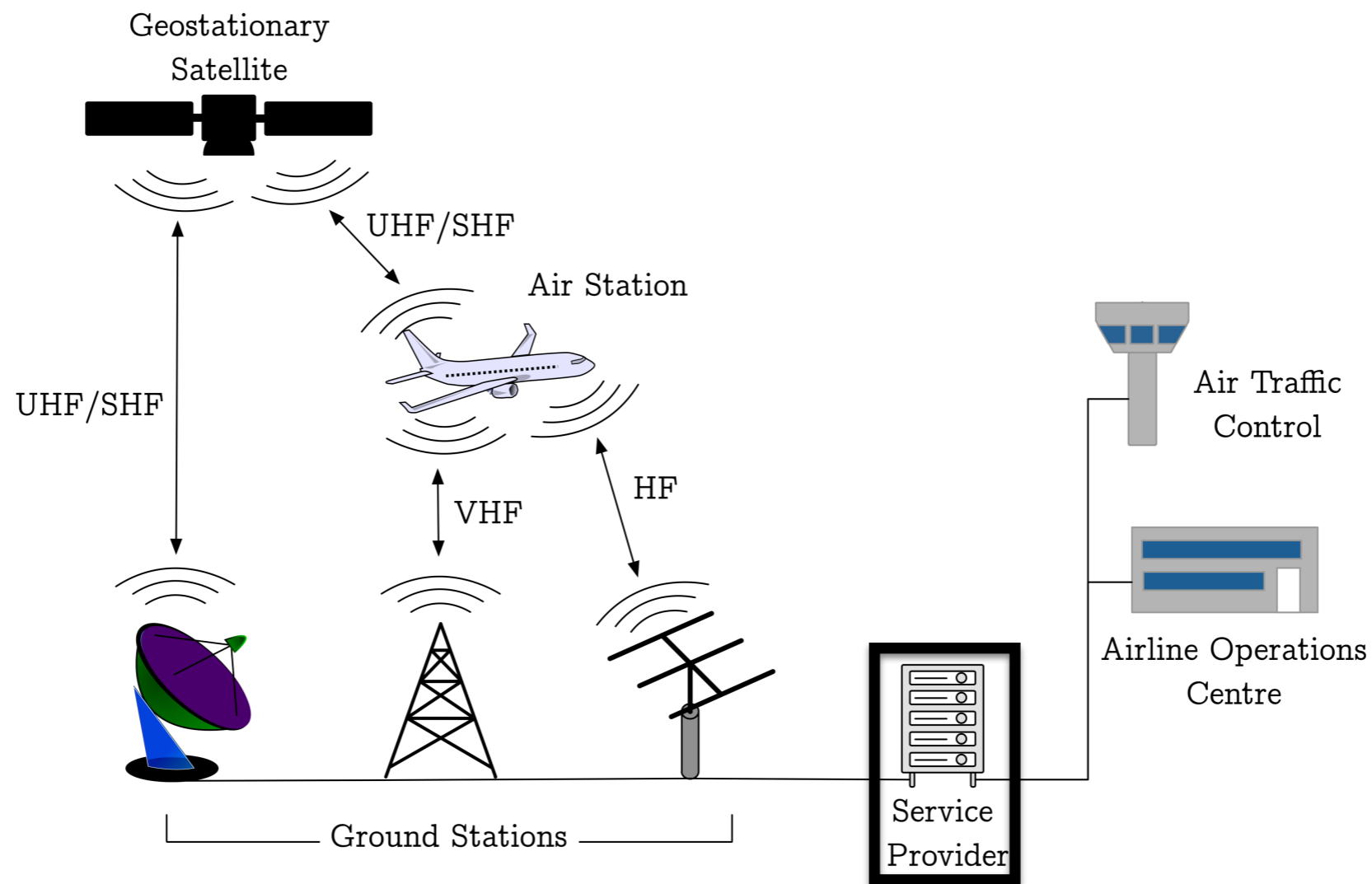
- **Aircraft Communications Addressing and Reporting System (ACARS)** is a widely-used avionic data link on both commercial and non-commercial aircraft
- Around since late 1970's, it is now used for **vastly different purposes** to its original intention
- Since then, it has become **multi-medium and multi-purpose**
- Easily collectible with **\$10 hardware**



WHAT IS ACARS?

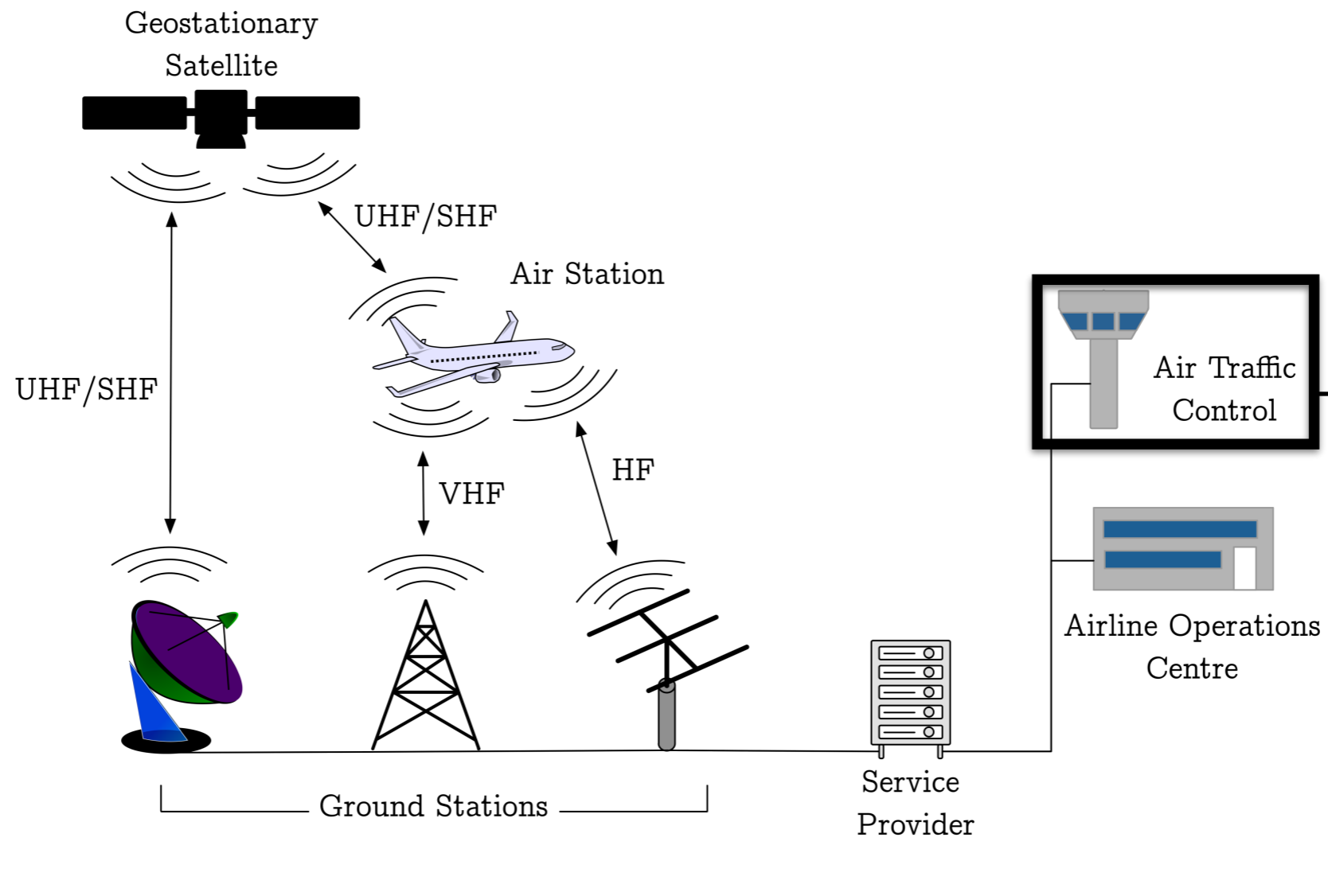


WHAT IS ACARS?



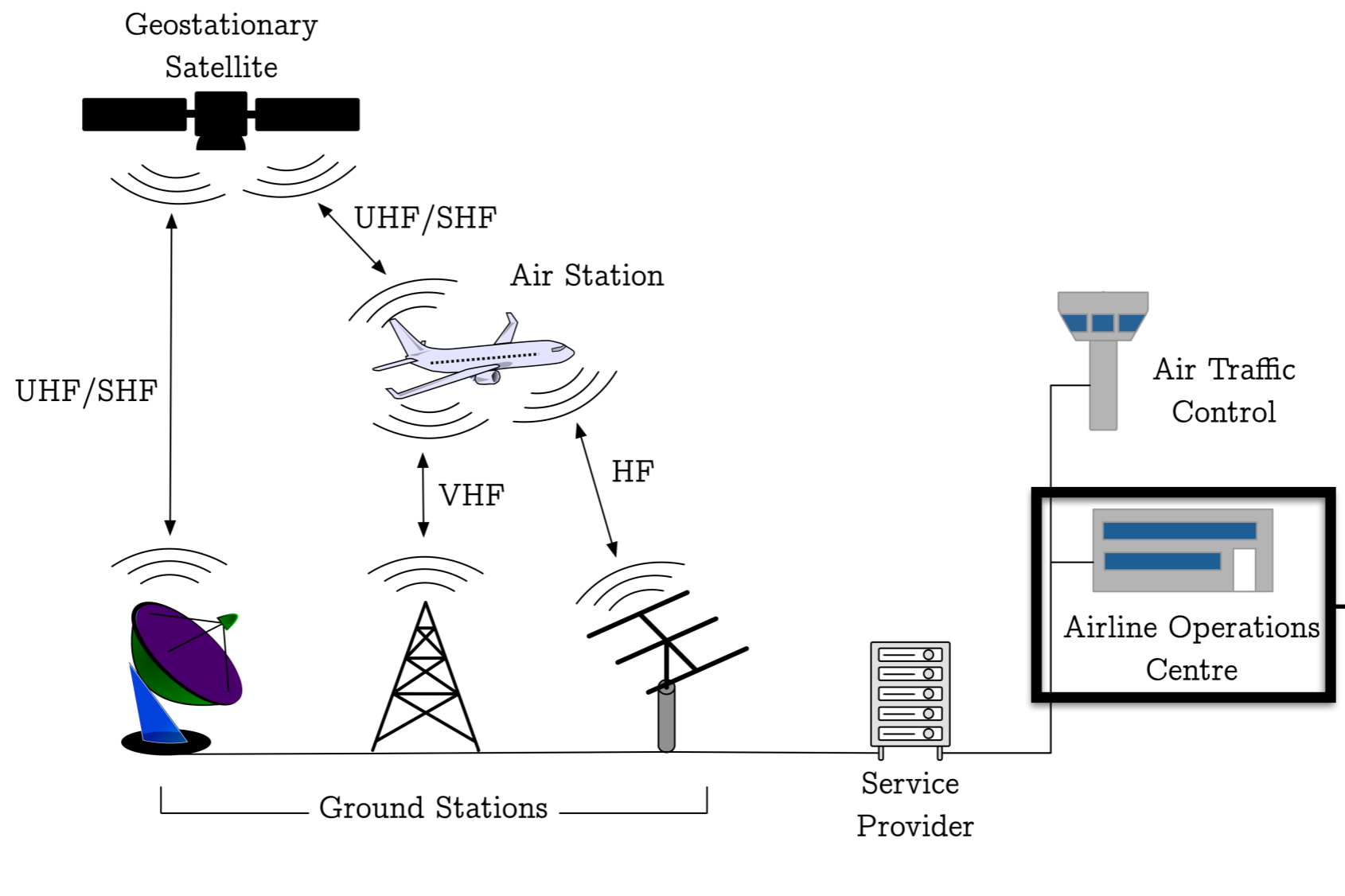
Service provider handles messages - like cell networks

WHAT IS ACARS?



ATC use ACARS to control aircraft without requiring voice

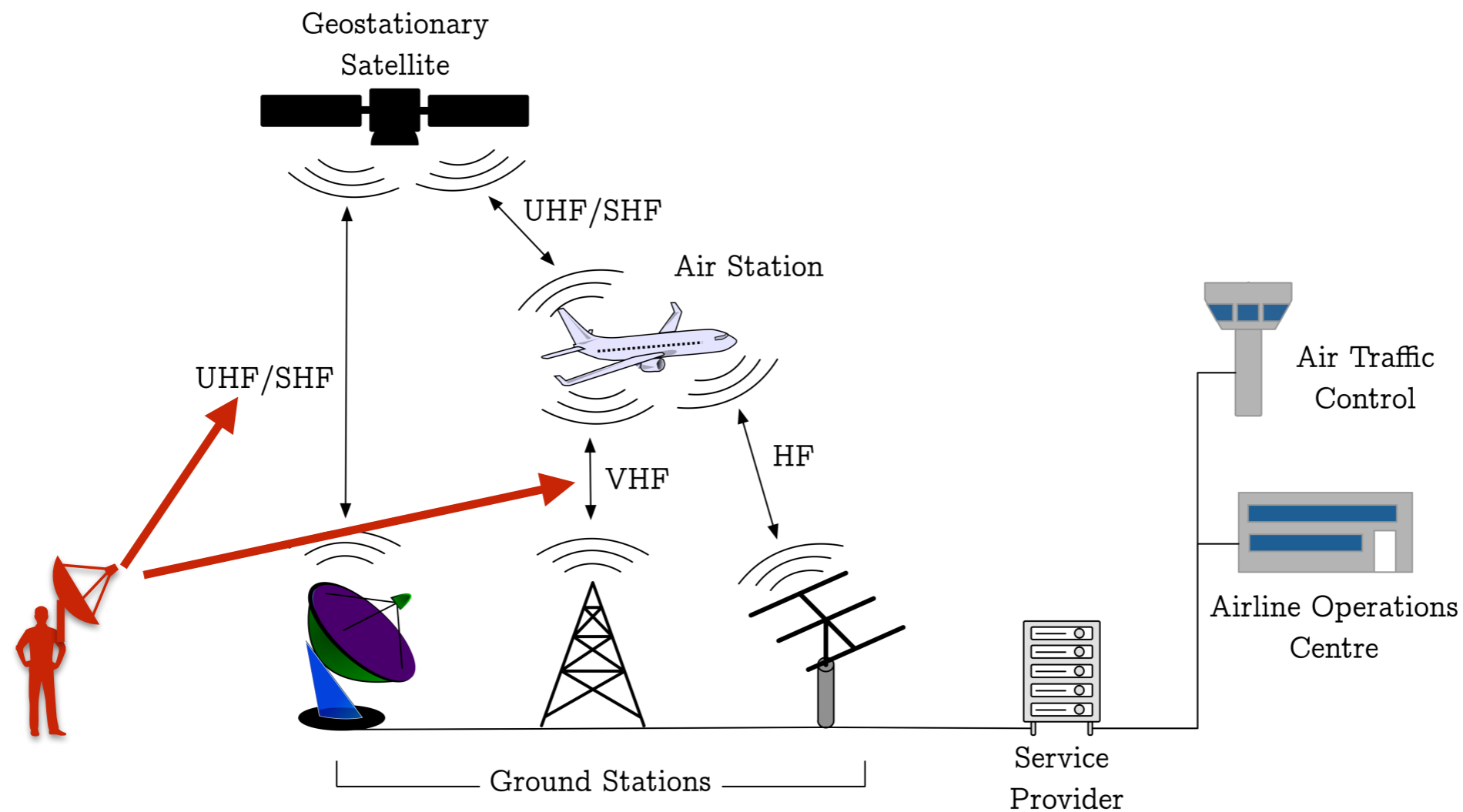
WHAT IS ACARS?



AOC communications allow administration in-flight, e.g. passenger updates, gate information



WHAT IS ACARS?



Software defined radios collected from one location over 9 months - ~1 million messages

SECURITY IN ACARS

- A number of ACARS applications clearly require some authentication or confidentiality - but **ACARS has no security as standard**
 - 'Post-hoc' solutions exist (e.g. Secure ACARS)
- However, it costs extra on top of existing ACARS - this deters users - no use thus far



SECURITY IN ACARS

- A number of ACARS applications clearly require some authentication or confidentiality - but **ACARS has no security as standard**
 - 'Post-hoc' solutions exist (e.g. Secure ACARS)
- However, it costs extra on top of existing ACARS - this deters users - no use thus far

Many users require privacy but don't want to pay



ANALYSING MESSAGES

- We collected over a million VHF and SATCOM ACARS messages, and noticed that some business aircraft were sending scrambled messages

07*?X.0)Emk.;M].;4;Dm)m..)Y(*)]s(\$).M4U).U;;).MmD)..D+0
07*?X.0)EmUmkm]..D00M)4k.)]rr6)Y-\).k.<);4<k);000)..;;+U
07*?X.0)EmUmUU]..D0Mk)m;.)]E{-)6-r).k.;);;;;);4;;)..U+.



ANALYSING MESSAGES

- We collected over a million VHF and SATCOM ACARS messages, and noticed that some business aircraft were sending scrambled messages

Key identifier

07 : ?X.0)Emk.;M].;4;Dm)m..)Y(*)]s(\$).M4U).U;;).MmD)..D+0
07 : ?X.0)EmUmkm]..D00M)4k.)]rr6)Y-\).k.<);4<k);000)..;;+U
07 : ?X.0)EmUmUU]..D0Mk)m;.)]E{-)6-r).k.;);;;;);4;;)..U+.

08 ,suL}Zq`cLLK=LLa`aLZ`YLZP\,0ZPf0,ZLaLYZLKeeZLc}KZLLc[`
08 ,suL}Zq`tee}=LLaL}KZ}vvZ=yy~ZPuAfZLaYYZYevLZY}eLZLLc[t
08 ,suL}Zq`KYev=LLK}aKZ}tLZbZbZLaYYZYevvZY`YvZbbbbbb

09 |\L46c+N s6,,G4418,hcN84cGeodc-r!Lc4Bh1c8B4hc8BBBc44Z5Z
09 |\L46c+N,BZ,G44BBZNc614c-r|Gc-W|Pc4BhZc48hNc48BZcbbbbbb
09 |\L46c+N s8NhG44s6,,c6B4c-W|Pc-r.-c4B68c888Bc88NZc44B5,

CIPHER & USAGE PROPERTIES

- 9 static keys were used by all aircraft using the cipher
- Using frequency analysis (and some deduction), we could recover ~76% of the substitutions for the 9 keys using 2690 messages
- All aircraft used the Honeywell Primus avionics suite



Bombardier Learjet 45



Gulfstream G650

AIRCRAFT TYPE

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1

AIRCRAFT TYPE

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1



AIRCRAFT TYPE

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1



AIRCRAFT TYPE

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1



HIDDEN AIRCRAFT

- A significant proportion of aircraft using this cipher **also used a block, so do not appear on flight trackers.**



HIDDEN AIRCRAFT

KL1749 /KLM1749
KLM
Operated by KLM cityhopper

AMS		LUX	
AMSTERDAM		LUXEMBOURG	
CET (UTC +01:00)		CET (UTC +01:00)	
DEPARTURE		ARRIVAL	
SCHEDULED	21:20	SCHEDULED	22:20
ACTUAL	22:00	ESTIMATED	22:39

GREAT CIRCLE DISTANCE: 315 KM
302 KM 00:27 AGO → 23 KM IN 00:11
KL1749 - AVERAGE FLIGHT TIME: 00:36

More KL1749 flights

TYPE (E75L)
Embraer ERJ-175STD

REGISTRATION	MODE-S CODE
PH-EXP	4855D2
SERIAL NUMBER (MSN)	AGE (JUL 2017)

Flightradar24

ed a

HIDDEN AIRCRAFT



The screenshot displays a flight tracking interface. On the left, a panel shows details for a C25A aircraft. The aircraft image is a white Cessna 525A CitationJet CJ2+ with red and blue stripes. The text below the image reads "© Flightradar24", "C25A", and "3D VIEW". Below this, the aircraft type is listed as "TYPE (C25A) Cessna 525A CitationJet CJ2+". A table of technical specifications follows:

	REGISTRATION N/A	MODE-S CODE N/A
	SERIAL NUMBER (MSN) N/A	AGE N/A
	CALIBRATED ALTITUDE 41,000 ft	VERTICAL SPEED 0 fpm
	GPS ALTITUDE 40,325 ft	TRACK 138°

The right side of the screenshot shows a map of the region around Kaiserslautern, Germany. A purple line indicates the flight path of the C25A, starting from the southwest and heading northeast. Several other aircraft are visible on the map, represented by yellow airplane icons with identification numbers. The map includes labels for various towns and cities, such as Trier, Idar-Oberstein, Kaiserslautern, and Saarbrücken. The Flightradar24 logo is visible in the bottom right corner of the map area.

HIDDEN AIRCRAFT

- A significant proportion of aircraft using this cipher **also used a block, so do not appear on flight trackers.**
- This implies that they are privacy sensitive - and so are being undermined by the weak cipher



HIDDEN AIRCRAFT

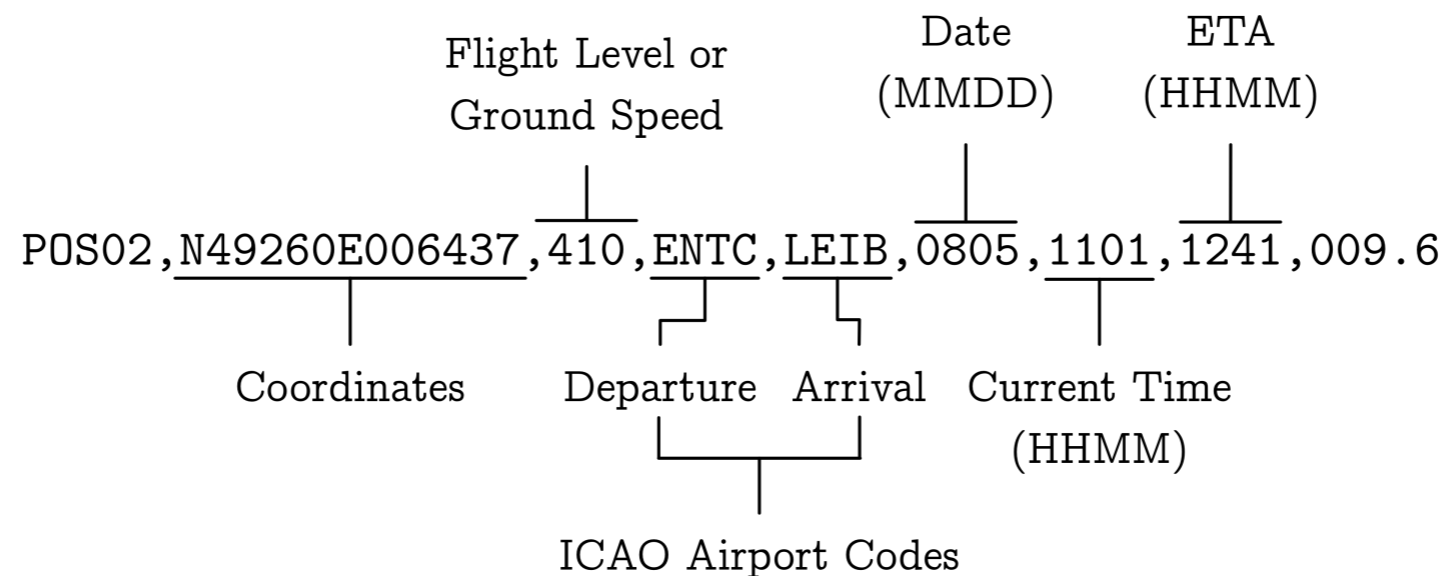
- A significant proportion of aircraft using this cipher **also used a block, so do not appear on flight trackers.**
- This implies that they are privacy sensitive - and so are being undermined by the weak cipher

Data Set	Not Blocked	Blocked	Total
VHF	5 (10%)	44 (90%)	49
SATCOM	10 (6%)	146 (94%)	156



MESSAGE CONTENT

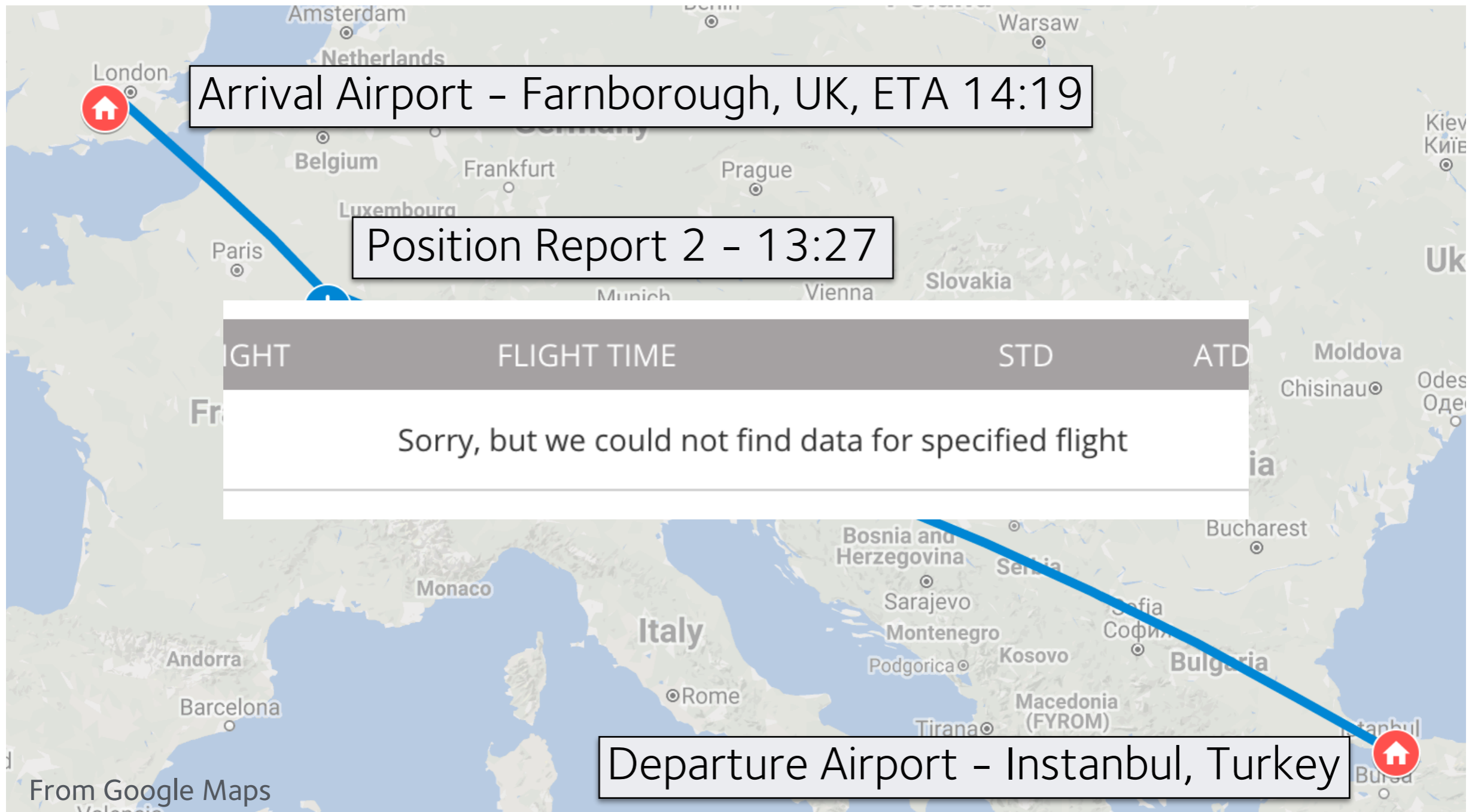
- 29% of messages were status reports, revealing **position**, **departure** and **arrival airports**



MESSAGE CONTENT

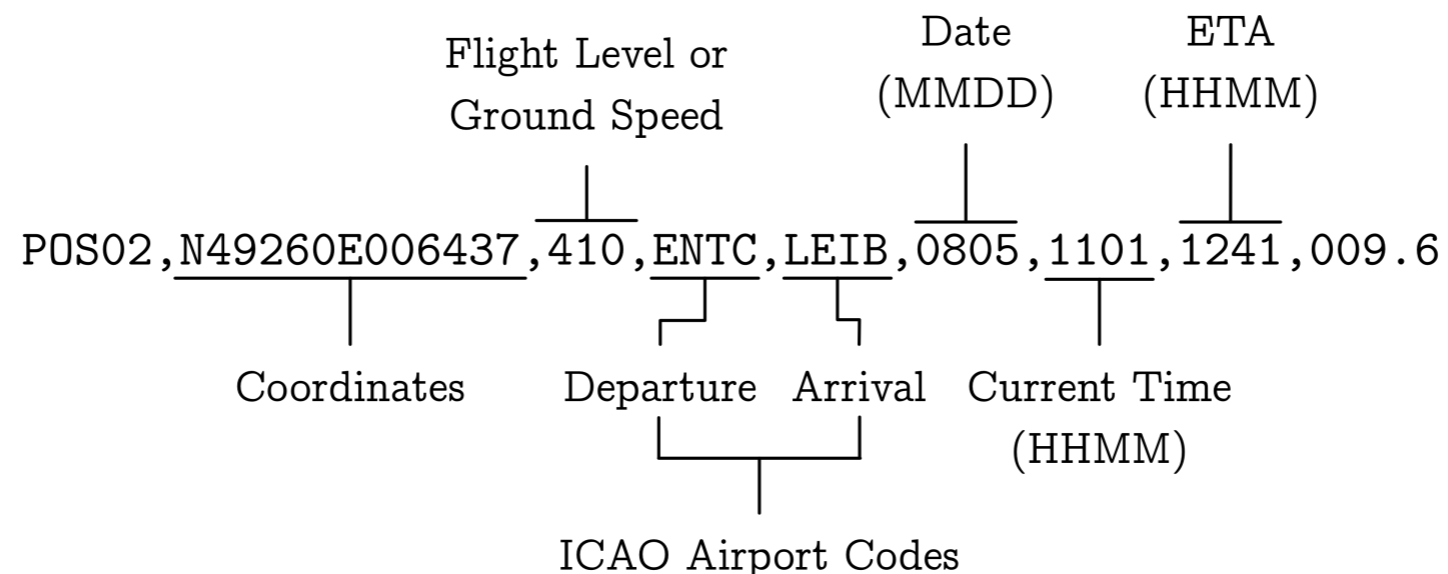


MESSAGE CONTENT



MESSAGE CONTENT

- 29% of messages were status reports, revealing **position**, **departure** and **arrival airports**
 - Blocked aircraft sent 90% of all status reports



RESPONSIBLE DISCLOSURE

- Reported to Honeywell prior to publication and met with a resounding ‘it’s not a problem’
- Cipher isn’t encryption but obfuscation thus not a security risk

“OBFUSCATION BECOMES ENCRYPTION WHEN A HIGH LEVEL OF CONFIDENTIALITY IS ASSURED. THE CONFIDENTIALITY ASSURANCE OF THE SUBSTITUTION CIPHER IS LOW.”



FULL PAPER: ECONOMY CLASS CRYPTO: EXPLORING WEAK CIPHER
USAGE IN AVIONIC COMMUNICATIONS VIA ACARS - FC2017

QUESTIONS

Matthew Smith^{*}, Daniel Moser^{\$}, Martin Strohmeier^{*},
Vincent Lenders[¥], Ivan Martinovic^{*}

^{*}University of Oxford
first.last@cs.ox.ac.uk

^{\$}ETH Zurich
first.last@inf.ethz.ch

[¥]armasuisse
first.last@armasuisse.ch

Real World Crypto 2018, January 10-12, Zurich



UNIVERSITY OF
OXFORD