# The aftermath of mystery flight MH370: what can engineers do?

# The aftermath of mystery flight MH370: what can engineers do?

Yijun Yu, *Member, IEEE*

***Abstract*—The mystery of missing MH370 flight a year ago is still unanswered: no one knows exactly where the crash was and what caused the problem. In order to answer these questions, a worldwide search has been carried out ever since to locate first-hand evidence which can be found in on-board flight data recorders (also known as blackboxes). To enhance aviation security, a proposal was made to use cloud computing to analyse live streamed flight data. This point of view article elaborates this proposal from an engineering perspective.**

***Keywords*—MH370, aviation safety and security, cloud computing, engineering**

## I. Brief history of disappearing planes

**Year 2014** will be remembered as a *dark* one in aviation history: in six fatal accidents with 19 or more passengers, almost 900 people lost their lives. It reversed the 10-year trend of improving safety in statistical records [1]. Amongst these major crashes, 239 died from the MH370 flight incident [2], 298 died from the MH17 flight incident [3], 162 died from Air Asia's QZ8501 flight incident [4], and 150 died from the Germanwings 4U9525 incident [5].

The root causes for all the crashes except MH370 are already known: the Germanwings plane crashed when a pilot was locked out from the cockpit by his malicious co-pilot; the QZ8501 lost its control due to rarely occurred weather conditions; and MH17 was shot down by military missiles while flying over a war zone. These causes have been found since the Flight Data Recorders, also known as the *blackboxes*, were eventually found at the crash sites. Such boxes contain well-protected information about the cockpit communication amongst pilots and between the ground controllers, and a number of engine operating parameters essential for the diagnosis. Once the reasons are confirmed by diagnosing the data extracted from the blackboxes, the aviation industry can issue guidelines necessary to improve the safety of our future flights.

Uniquely, however, it is not yet known what has really happened to the missing MH370. Its last hourly ping signals to the Inmarsat satellite suggested that the flight headed towards the southern Indian Ocean, which was speculated from the Doppler effect of drifting frequency caused by the high-speed moving signal source. Even though the international team immediately shifted the search and rescue effort towards the Indian ocean, it was hard to locate the blackboxes under the ocean bed because the batteries for signalling their location lasted no longer than 90 days. When the batteries are turned off, a large area was still unexplored. After spending tremendous amount of resources on an international search and rescue, the flaperon, or a piece of the wings of a Boeing 777 plane was found on 29 July 2015 at Reunion Island: MH370 (a Boeing 777) is the only one of such planes that went missing recently in the Indian ocean. The flaperon floated there from the crash site potentially by the ocean currents [6]. On September 3, 2015, French authority confirmed that the flaperon is indeed from MH370 [7]. Despite this finding, without the blackboxes it is not yet known when one could get hold of the critical flight data recorded from the crash site. The search has to continue.

Fig. 1. Still no signal. EPA/Luong Thai Linh

## II. Combining black box with cloud computing technology: a recent proposal

Invented in the 1950s, blackboxes are still being used widely as the primary sources of forensic information for aviation safety and security. Since the MH370 tragedy, the International Telecommunication Union (ITU) is adopting a *live streaming* proposal [8] in its guidance for future aviation communications [9]. With widely used remote communication capabilities, smart-phone owners can already detect the location of the phone and wipe data out if they are lost, it is less imaginable that engineers cannot do the same for flights using an advanced technology.

Tracking one smart-phone seems to be easy but it is not. Millions of smart-phone owners, distributed globally, may need this capability simultaneously. To be able to fulfil this simple requirement it requires vendors to invest significantly in *cloud computing*, the on-demand technology to employ large amount of computation resources when needed.

Each airplane produces both digital and analog data from thousands of on-board sensors, multiplied by millions of flights

around the globe, a full scale tracking of every aircraft using satellite communication alone could be expensive, but it is not entirely unfeasible. In fact, we have already seen several good signs towards solving this problem.

In the rest of the article, I will look at the live streaming proposal from an engineering perspective, that is, first to enumerate a list of fundamental requirements for the technology to be applied to aviation in order to enhance safety without sacrificing security, and to speculate on some of the challenges from technology and beyond.

## III. Engineering challenges to live streaming blackboxes

Obviously, one engineering challenge is the *performance in communication and computation*. As shown earlier, the sheer amount of computation required is substantially higher than a typical cloud computing application. Sensors on-board the airplanes are collecting large amount of continuous flight data in real time. Live streaming them requires substantial communication bandwidth for satellites as well. However, we have already seen good signs of achievements to tackle this challenge. For example, Kapoor et al [10] used the flight data on Azure cloud to predict the wind speed with a better precision than the weather simulators. Augmenting simulation with real-life data like the speed fluctuations of a neighbouring flight could be used to pre-warn the pilot about impending danger in weather conditions. One step further, combining the transponder radar data from volunteers to *crowd source* observatory flight data could complement what has been downstreamed from the on-board flight data. With the advent of deep learning and big data engineering initiatives, proactive and accurate forensic analysis [11] of flight data could become affordable and common place very soon.

A less obvious, but perhaps more important engineering challenge is *cybersecurity and human behaviours*. Airplanes and their stakeholders such as pilots, passengers, traffic controllers form a socio-technical system. Depending on a boundary of monitoring and diagnosing [12] solutions, the engineering challenge can manifest in multiple dimensions.

For example, the Germanwings flight incident taught us that individual human behaviour can be unpredictable. What if a trained pilot cuts off all communication channels to blind out the entire monitoring mechanism, just as the Germanwings pilot managed to lock out the co-pilot from access to the cockpit? Although our trust in pilots may not be totally lost due to this single incident, one needs to be more prepared for a worst case scenario as such. A proposal to monitor this is to employ a technology similar to the design of bitcoins, that is, through verification of multiple sources of information so widely distributed that it is hard to contaminate by malicious attempts. Even if the communication to the cockpit is cut, the external transponder and the engine data may not be tampered by anyone on-board at the same time.

Since flights over oceans may not be at a close distance to any ground masts or terrestrial stations, compared to wireless communications between cell phones and base stations, currently it would only be possible to relay the information using satellites. Today's communication satellites at the geostationary orbit such as Inmarsat 4A F4 or Kepler space telescope could use the $K_a$ band frequency between 26.5 – 40 GHz, which offers a higher bandwidth communication up to 4.3 Mbps. The cost of transmitting flight data is relatively high at the first glance. However, if the bandwidth is dedicated and shared amongst 100K operating flights, each flight could have 430bps, 25.8Kbpm (bits per minute), or 1.55Mbph (bits per hour). Since one does not need to track flights per second, and physical objects must obey the law of inertia, it is still feasible to transmit only the meaningful changes [13] frame-by-frame at a lower bandwidth. Experts deduced the possible search area for the missing MH370 through the Doppler shift effect of the received ping signals from its engine, made by Boeing 777-200ER. Therefore, today's advanced air planes such as MH370 are already equipped with transponders to send the ping signals of the engine to satellites. To implemented the proposal by piggy backing on the existing physical satellite communications, one needs to consider how much more information (apparently not all data of current FDR) would be required to implement the proposal.

In addition to the flight data, cross-validating the *integrity* of the data using multiple sources could greatly enhance the trustworthiness of the live streamed flight data. The tasks of verifying the live streamed flight data itself may require cloud computing and an investment from the entire aviation industry to avoid a single-point of failure by design. It might be achievable by borrowing the design of monetised digital currency (e.g., bitcoins), through which the system accepts the transactions by verifying the hash of a chain of historical transactions uniquely associated with the digital currency. However, the incentives for verifying the data of other flights need to be justified by the aviation industry including insurance companies.

Apart from the integrity issues, *confidentiality* of communications requires a good separation or insulation of the *network traffic* of on-board entertainment system and the essential cockpit satellite network. Protecting the most valuable assets, i.e. lives of passengers, from any potential attacks shall be preferred over the offering of network features to customers.

For business it is attractive to gain passengers from competing airlines by offering the luxury feature of 'indispensable' network to everyday users. For the engineers who produce and maintain the airplanes, however, one must consider effective ways to *availability*. To monitor the network traffic, good news associated with the enabling of cloud computing technology: one could push the logs of the network traffic data into the cloud for live or offline intrusion detection analysis. Such network traffic blackboxes have similar bandwidth and computational limitations as traditional live streaming blackboxes, however, engineering trade-offs have to be made on how much traffic needs to be logged and analyzed. Even if imperfect perhaps, the awareness of the existence of such security controls may already help thwart many attempts of network security attacks.

Since the 9/11 terrorist attacks, the door between the cockpit and the passenger cabinet is mandated to be locked so that the pilots inside the cockpit can prevent outsiders from

entering. The Germanwings incident, however, suggests the implemented requirement is not fit for the purpose when one of the pilots inside the cockpit cannot be trusted. Had the other pilot known that under emergency the access restriction of cockpit could be overridden, the incident could have been prevented. Consistency between the conditions envisaged at design time and those that occur in reality may not be respected at runtime by attackers on purpose, or by human operators by accident. Either intentional or accidental cases call for a requirements-driven auto-piloting which could monitor and detect misbehaviour of operators through advanced *self-adaptive* behaviour. At the same time, it is uncertain or debatable whether the flight using auto-piloting or remote control is as trustworthy as the human pilots on-board.

Last but not least, a big question is *social and economic trade-offs*. Engineers must be fully aware of the limitations imposed by the business of aviation, while comparing different solutions. The number of passengers, the availability of satellite networks, the nature of weather around the plane, and inevitably human errors of pilots, terrorists on flight and warlords on the ground, the risk factors are enormous. Any engineering enhancement for an airplane could bear a number of concerns from social and economical responsibilities.

## IV. Conclusion

With the advance of technology in the area of cloud computing and Internet of Things since the aftermath of MH370, engineers may soon be able to overcome all the challenges to implement the proposed idea of live streaming of flight data. Transmitting the critical information from flight data and recording it to computers in the cloud is not only feasible, but also arguably more reliable than waiting for the flight data recorders to be found from the debris after the incidents happen. Due to the current limitations on the bandwidth of satellite communications, however, only the most critical data of the flight should be streamed. The full picture of flight situations needs to be simulated using the power of cloud computing to piece together the missing information in near real-time, and be verified and validated with the big data coming from on-board flight data recorders of the planes nearby both in space and in time. In this vision, all flying airplanes can be treated as part of the Internet of Flying Things.

However, engineers alone cannot fully solve all problems for the aviation safety and security. Critical as the data are, Internet security requires to be hardened to prevent tampering with the live streamed data or misinterpreting what is going on. When the transmission lags behind due to physical communications constraints, safe operation on-board can only be independent of the ground for a non-negligible amount of time.

## Acknowledgement

This work was made possible by the support of a grant (NPRP 05-079-1-018) from the Qatar National Research Fund (QNRF). The statements made herein are solely the responsibility of the author. The author thanks Michael A. Jackson for comments on the early draft of the paper.

## References

[1] planecrashinfo.com, "Aviation accident statistics." [Online]. Available: http://www.planecrashinfo.com/cause.htm

[2] "Missing Malaysia plane: What we know," *BBC*, Jan. 2015. [Online]. Available: http://www.bbc.co.uk/news/world-asia-26503141

[3] "MH17 crash: Airlines divert flights from eastern Ukraine." [Online]. Available: http://www.bbc.co.uk/news/business-28356745

[4] J. Rowlatt, "Flight QZ8501: What we know about the AirAsia plane crash." [Online]. Available: http://www.bbc.co.uk/news/world-asia-30632735

[5] "Alps plane crash: What happened?" [Online]. Available: http://www.bbc.co.uk/news/world-europe-32035121

[6] "Mh370 search: Does debris solve the mystery?" [Online]. Available: http://www.bbc.co.uk/news/world-asia-33713885

[7] "MH370: Reunion wing debris 'certainly' from missing flight." [Online]. Available: http://www.bbc.com/news/world-asia-34145127

[8] Y. Yu, "If we'd used the cloud, we might know where MH370 is now." [Online]. Available: http://theconversation.com/if-wed-used-the-cloud-we-might-know-where-mh370-is-now-24542

[9] D. Damon, "How Cloud Computing Could Help Locate the Missing MH370 Plane, an Interview with Dr Yijun Yu from The Open University," Apr. 2014. [Online]. Available: http://www.bbc.co.uk/programmes/p01wl74m

[10] A. Kapoor, Z. Horvitz, S. Laube, and E. Horvitz, "Airplanes aloft as a sensor network for wind forecasting," in *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, ser. IPSN '14. Piscataway, NJ, USA: IEEE Press, 2014, pp. 25–34. [Online]. Available: http://dl.acm.org/citation.cfm?id=2602339.2602343

[11] L. Pasquale, Y. Yu, M. Salehie, L. Cavallaro, T. T. Tun, and B. Nuseibeh, "Requirements-driven adaptive digital forensics," in *Requirements Engineering Conference (RE), 2013 21st IEEE International*. IEEE, 2013, pp. 340–341.

[12] Y. Wang, S. A. McIlraith, Y. Yu, and J. Mylopoulos, "Monitoring and diagnosing software requirements," *Automated Software Engineering*, vol. 16, no. 1, pp. 3–35, Mar. 2009. [Online]. Available: http://link.springer.com/article/10.1007/s10515-008-0042-8

[13] Y. Yu, T. T. Tun, and B. Nuseibeh, "Specifying and detecting meaningful changes in programs," in *Proceedings of the 2011 26th IEEE/ACM International Conference on Automated Software Engineering*, ser. ASE '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 273–282. [Online]. Available: http://dx.doi.org/10.1109/ASE.2011.6100063