International Journal of Future Generation Communication and Networking
Vol. 9, No. 10 (2016), pp. 299-310
http://dx.doi.org/10.14257/ijfgcn.2016.9.10.26

Technology Trends Analysis of Airbone Network

KiHwan Kim[1], HyunHo Kim[1], SangGon Lee[2], HoonJae Lee[2] and YoungJae Ryu[3]

[1]*Department. of Ubiquitous IT, Dongseo University*
47, Jurye-ro, Sasang-Gu, Busan 617-716, KOREA
ghksdl90@naver.com, feei_@naver.com
[2]*Division of Information and Engineering Dongseo University*
nok60@gdsu.dongseo.ac.kr, hjlee@dongseo.ac.kr
[3]*ADD*

Abstract

Development with IT technology has wide effect for military sector. For this reasons, the important sources is 'First see, and first determine, and first attack' in modern and future warfare. And there are also importance with patriot robot such as drone for understand the movement pattern with enemy. Therefore, in develop country; they process with sensor system, delicate attack system, informationization and identification proactively. For now, the connection between equipment is essential in the war environment, so the secure with these things is important. But this is planned with using network structure based on TCP/IP, So there is a raised problem that plan which I mentioned has difficult to deal with attack from using structural weakness. In this paper, the attack type which is possible in the Airborne Network is made an inquiry and it analyze.

Keywords*: Communication, Data Link, Radio communication, Security, Evil Twin Attack*

1. Introduction

In present, Information is important source which determine benefit of person or group. Therefore, most people make effort to get speedy and accurate information compared to others. So, there are trying to make benefit with steal other information of one's or group, and this is not only problem between countries. There is an example of monitor and eavesdropping from NSA to collect submarine cable [1, 2], And we can recognized that this is so hot for information war between country with point of that this has goal with important character. But information war happens with military war for hot status.

Modern military network use different wave with different frequency band (*i.e.*, Link 16, TTNT, CDL, MADL/SADL, Optical/Laser, and SATCOM, *etc*.) for specific mission, so they have limited interoperability and independent louting function [3]. Because if plan and information is leaked, they cannot not protect our nation people from exterior power.

American air force defined the Airborne Network like the next.[14] The war implementation platform is the element which the mobility is essential. And the link shape is changed according to the connected state of the movement of the information provider and node. Therefore, the high packet loss rate and connection cannot occur often and the centralized module network service cannot be trusted. Because it can be forward deployed in the area of which the equipment of the friendly force is hostile, especially the connection to the wide area has to be guaranteed.

ISSN: 2233-7857 IJFGCN

In this study, we deal with dangerous factor of airborne network security and problem with each dangerous factor.

2. Weak Point with Airborne Network

A basic risk of network environments is proportional to the network size. As the network size becomes larger more, it can have an effect on the other system due to data caused by the bug in which one or more device is physically damaged or which is latent or purpose intentional. The airplane moves to the overspeed. Therefore, its own network infrastructure is created every the airplane. By using the mobile node the MIP(MIP:Mobile Internet Protocol) in order to comprise the home node, connect with the IP network. MIP makes make the mobile node which maintains the home internet protocol address while Internet is accessed possible.

Airborne network means expansion area which support safety network using various telecommunication functions in poor condition for telecommunicates and expanded network [4]. Therefore, to compensate safe telecommunicate transmission, they have to satisfy following conditions with Table1.

Table 1. Main point with Military Network Security

Types	Condition
Delivering security	This is difficult to eavesdropping and have strong encryption, Even though they cannot decode, Detection/Search/Perception provide important information and location about enemy, platform and movement of equipment.
Strong delivery	Sun flare, network has to be operating normally, even though there is disorder with delivery communication by hard weather or jamming from enemy. If signal cannot through shower or spread from enemy's wideband jamming, link and NCW model will stop.
Delivery ability	This is ability with how fast digitalized image can deliver (*e.g.*, if deliver 10Megabyte recce image or search for 2megabit/sec digitalized video feed, 9600 bit/sec channel is almost useless) In NCW area, platform can address or access with other platform or system specifically.
Signal format or telecommunication protocol compatibility	It is essential to communicate with other different platform or other system in NCW environment There are problems with using each other signal modulation and digital protocol and also there are problems with compatibility with same signal modulation and telecommunication protocol.

Thus, there can be various problems if they cannot satisfy main conditions in Table 1, and following are other problems which can be happen.

Each situation is repeated in the war like the Figure 1. The electric field information corresponds and the cognitive domain is expressed as the headquarters directed the electric field in the physical zone. The cyber domain does the electric field in which it falls physically and role that it is the headquarters on a real time basis. However, the way

in which it can check whether the corresponding information is the forgery and falsified information is restricted. Therefore, the awareness and physical conduct area everyone who is the accident the integrity about the cyber area and reliability is important.

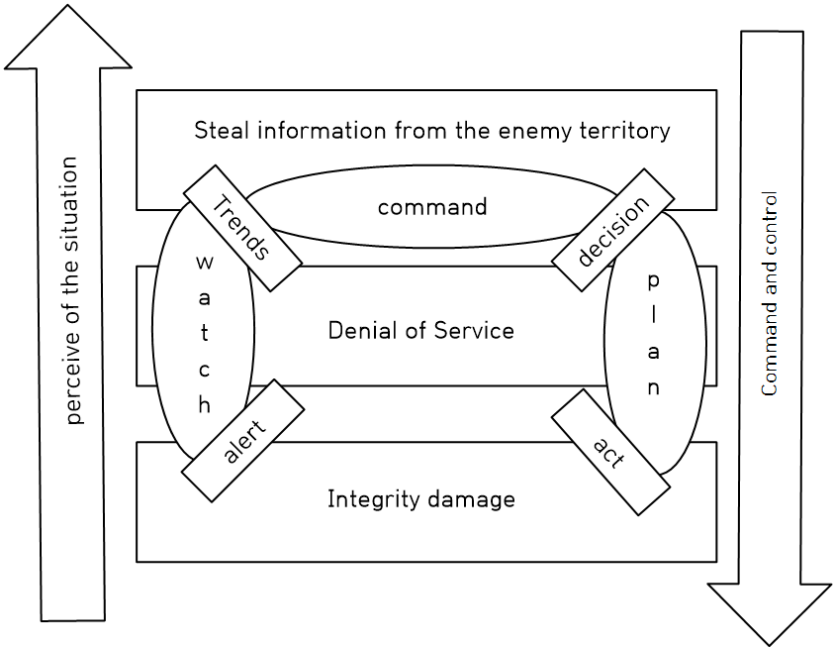

Figure 1. The War Domain Region Information

2.1. Limited Identifier Structure

IP address is original information which comes from to identify each equipment. And this is used for communication for each equipment which departed for physically with using IP table in network later. But if they communicate with center of IP, they should have to consider problems with difficult to identify delicate equipment and counterpart power against weak point of TCP/IP planning.

There are predictions that there will be wide range of network if used with IP for each other military equipment. Therefore, there can be possibility with IP segregation problem cause by using dedicated telecommunication for arm of service and size. Also, in case of wide distance vehicle, ship, combat aircraft are needed to be check IP regularly, and in case of load of visual art equipment, there can be too much traffic.

TCP/IP Protocol usually suppose fix host and plan and they suppose support of host movement for except case, they handle this for condition that induce additional mobile support agent(Inefficiency of louting route, Addition with proxy function : Serious resource waste). And command and control center which has mission about recognition of mission and control use central network structure (can make too much traffic), as CDR-1 mentioned, if they constitute louting area for B Class, they can allocate about 65534 numbers of equipment. If they connect all military equipment, they will be large range of connection, in this point, the equipment which can load visual are equipment and has large range of distance such as vehicle, ship, combat aircraft need to be managed.

2.2. Support Mobility According with Center Concentration Ways

TCP/IP Protocol is planned with suppose of fix environment which provided from stable power in cable conditions, so there are problems with supporting mobility. To deal with this problem, they suppose mobile host for exception and use mobile

support agent. But mobile support agent plus ineffective proxy function with louting route so this triggers serious resource waste.

The solutions from mobile support agent are mobile IP agent which used for modern mobile terminal. But, mobile IP has supposed that they are not change network for more than ones' in seconds. Therefore, in case of high mobility of combat aircraft, there need to some repeat with possible range of using louting equipment and they have to be used equipment with fix IP.

2.3. Vertical Host Base Protocol

As similar with TCP, in case of controlling traffic in network, there are more inefficiency and limitation with handling error and performance than just handle with network itself.

In rules of vertical, most of main abilities are showed with vertical host, so there need to change with enormous number of host, but this has difficulty with real status. So there are problem with share management for each resources.

3. Type of Attack

There are three types of cyber-attack with confidentiality, availability, integrity. The following Table 2 shows about these things.

Table 2. Data Type of Attack Case

Types		Explanation
Confidentiality	Date	This makes data for not leak or possess with people who are not authorized for personal or confidential information.
	Privacy	This makes effect with how they collect or store with information which related with personal or how they control or leak for some information for someone.
Availability	Availability	They has effect of suitable operation for suitable point with system, and they compensate for provide service to sanctioned user.
Integrity	Date	They compensate that they can change using only sanctioned specific ways with information and program.
	System	They compensate to processing with non-damaged function which suitable for system, and process with suitable function without any un-sanctioned control by intentional or accident.

Each by class problem because of the TCP/IP type

The IP routing problem

The originality address of the airplane has the connection with its own departure ISP. Therefore the problem happens the plane cross when advancing to the area among the flight. In case these preserve the corresponding address among the fly, the cohesion scaling will be reduced and they will increase the overhead for new ISP.

- The physical layer problem

Specific physical security requirements are embedded within the Figure 2 design.

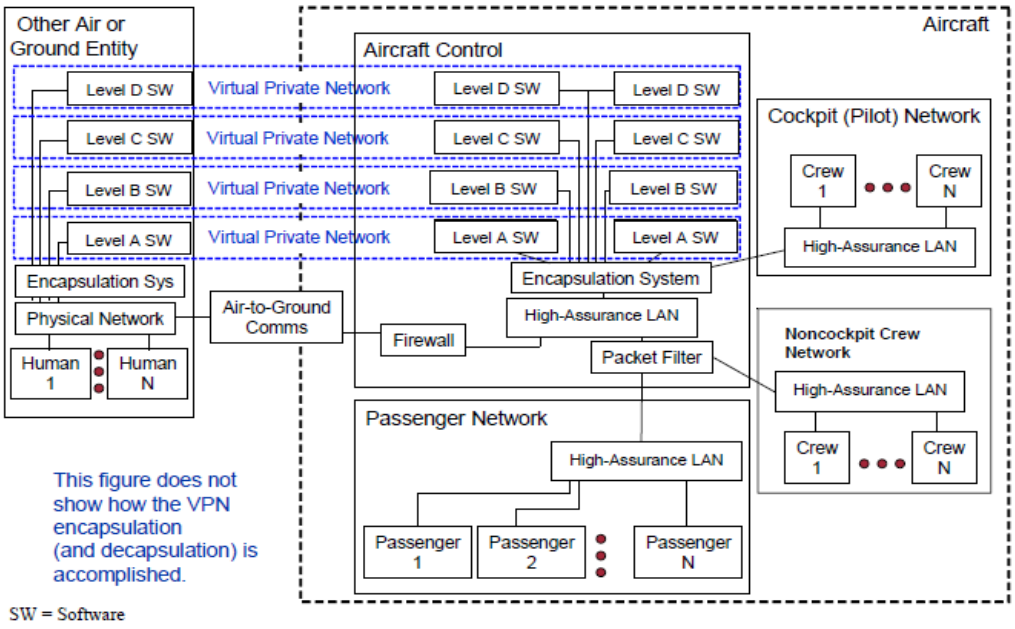

Figure 2. Secure Generic Airborne Network Design (High-Level View)

Those requirements are that aircraft control and the cockpit (pilot) networks or their devices must not be physically accessible by aircraft passengers. If there is any possibility of passengers physically accessing the cockpit (pilot) network, then the high-assurance LAN within the cockpit must be connected to the aircraft control network via the packet filter. Otherwise, the high-assurance LAN in the cockpit can use the same physical high-assurance LAN as aircraft control. HAGs are high-assurance devices that need to be physically protected from areas that are accessible by passengers.

The noncockpit crew network devices should also not be accessible by passengers in general, but the design could accommodate situations in which passengers are not always physically excluded from the area where those devices are located. If physical separation is not possible, crew members must be very careful to not leave open applications running in situations when the crew member is not present (*i.e.*, situations where passengers may access applications that have been opened with crew member authentications).

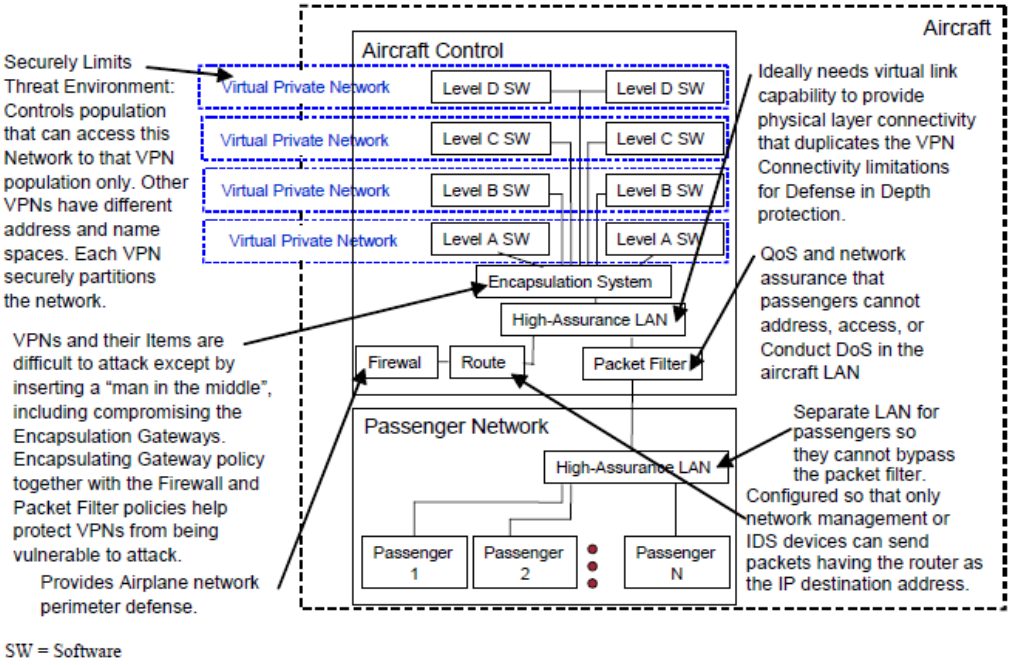

Figure 3. How Design Addresses Network Risks

The capsulization gateway

Encapsulation gateways support IPsec in accordance with reference 99 (see section 8.3.1). The encapsulation gateways must be configured so that all packets sent to their nonenclave IP interfaces must be dropped unless they use the IPsec's ESP. Encapsulation gateways communicate together using the ESP in tunnel mode. Network managers or IDS devices communicate with encapsulation gateways via the ESP in transport mode. Because of the authentication provisions contained within the ESP, encapsulation gateways should be configured so that they only accept communications from outside of the VPN enclave they support from three types of devices only: other encapsulation gateways, network managers, or IDS devices. They should be configured so that they ignore (*e.g.*, drop) all non-IPsec packets coming from outside of the VPN. Packets sent to the VPN that they support must be IPsec in tunnel mode. The encapsulating gateway does not put any restriction upon packets sent within the VPN that it forwards. However, all packets addressed to the encapsulating gateway itself (from either outside of the VPN or within the VPN regardless) must be sent in IPsec or else they will be ignored (*i.e.*, dropped).

3.1. Attack which has Center of Data Forgery and Alteration

Wireless network has center of Access Point (AP) so they handle this for one network are from date link layer with demote smart phone, notebook, and tablet. To manage these things, they sore table with MAC, IP information so they use this for date transmission or control. But they cannot certify repeatedly for this already certified equipment, so they can induce for connect with fake network like Figure 4 for reason that they handle first with equipment which have high signal sensitivity without methods that certify louting equipment [5, 6].

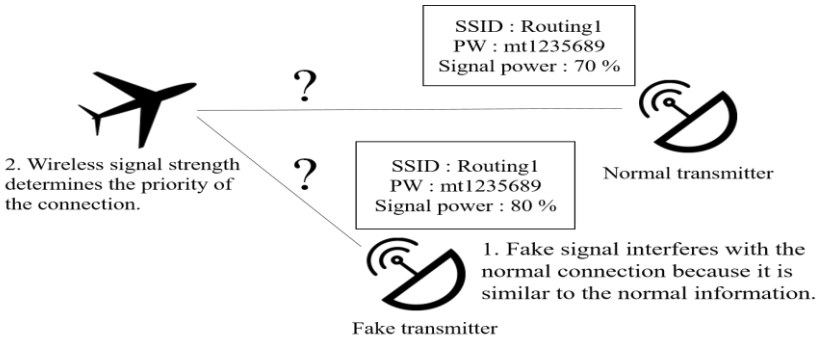

Figure 4. Evil Twin Attack

Representatively, wireless network attack is divided with Evil Twin Attack and Man in the Middle Attack. Firstly, in case of Evil Twin Attack, this can be classified with negative and positive attack. Negative attack is mimicking network or collecting packet so this has not any direct effect to sender/receiver date. On the other hand, positive attack mimic network so they transmit malware which can trigger systematic problem, and unrecognizable data, so they transmit powerful signal intentionally to disconnect with normal network. This makes direct effect to date of sender/receiver.

Man in the Middle Attack recognized that two people connect with other person, but indeed, two people connect with mediator so he eavesdropping transmitted date and manipulated and transmitted to other sided and attack [7].

3.2. Evil Twin Attack which Interfere with Reception Service

● ARP spoofing: It is easy to modulate MAC in wireless network, so it is possible to try to mediator attack with intercept ARP message [8].

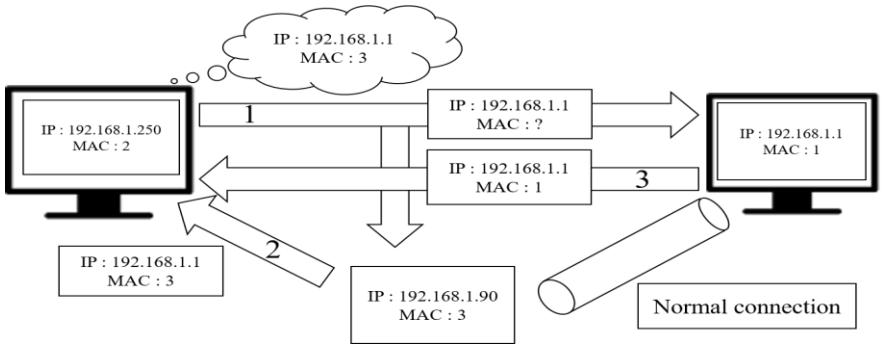

Figure 5. ARP Spoofing Example

● Brute force attack: Under Figure 6 is the painting explaining the brute-force attack. And the brute-force attack tells to store the normal packet which the normal equipment transmits and repeat the saved normal packet and transmit.

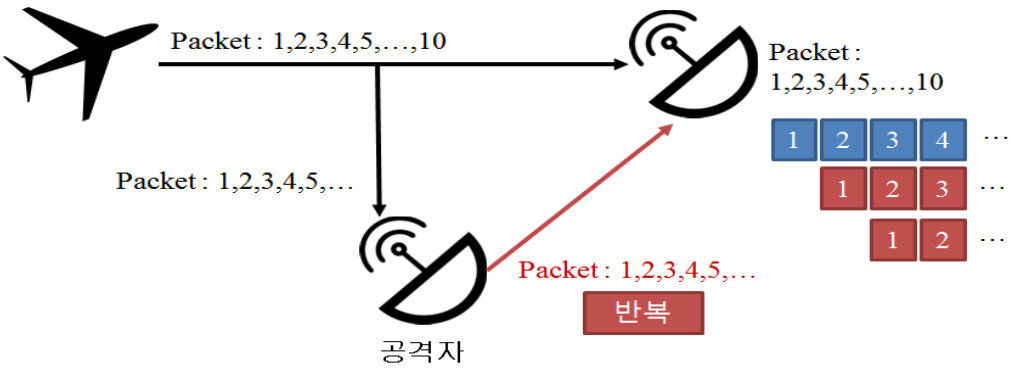

Figure 6. Brute Force Attack

● Smurf Attack: Direct Broadcast: It is possible to deliver information to member of group who using one transmission. So, this is attack method which abuse ICMP packet and Direct Broadcast [9]

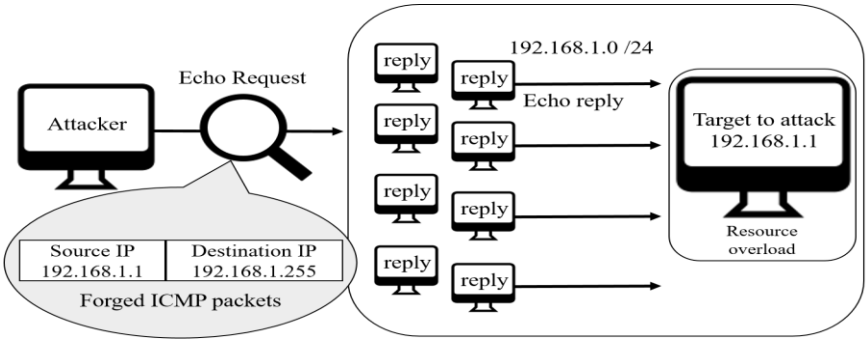

Figure 7. Smurf Attack Example

● Radio wave attack: This has high rate of condition that happen modulation or physical interfere with radio wave compared to wire conditions. In recants, the area where banned for unconditional used Unmanned aerial vehicle (UAV) use equipment which named freezing gun, so they expose to antenna so as to make non operated conditions [10].

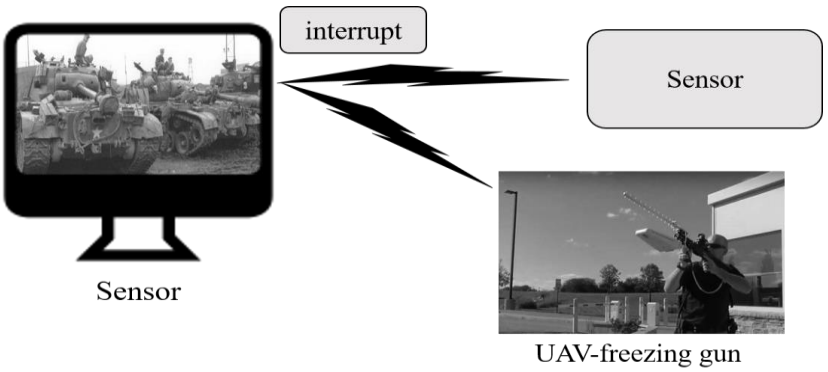

Figure 8. Wireless Transition Attack

4. The Weakness Classification

The harm is determined according to the way that the cyber-attack abuses the weakness of the attack objective and various network layers. In the case of the public network, the wireless network is mainly used. And the way in which it defends this physically completely doesn't exist. Therefore, use the method in which it receives encrypted data in which plain text data are not with the transmission and minimizes the damage according to data leakage. If the classification about the attack is divided into three types, it can divide into Adversary Objectives, Attack Classes and Attack Vectors.

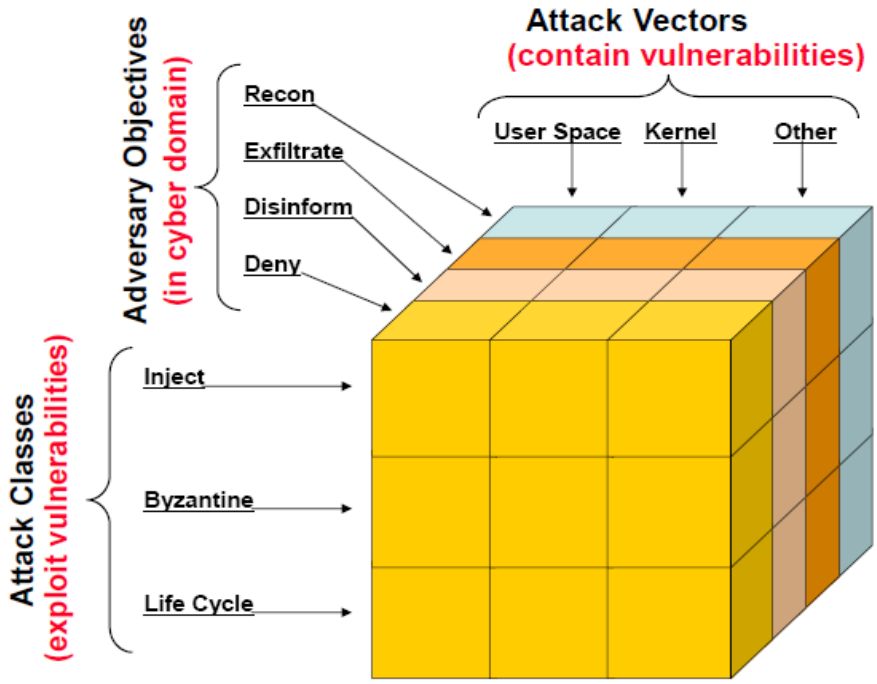

Figure 9. Weakness Classification Cube

Adversary Objectives is the element determining the action limit about the target system. And it can divide with Deny, Disinform is false but believable Provide information. It is illustrated by Alter video feed to insert or remove selected objects or people. Exfiltrate is Steal information from a network. It is illustrated by Download battle plan or monitor blue force tracking. Reconnaisance is Learn about network. It is illustrated by Run port scan to find vulnerable hosts.

The Attack Vectors is the method in which it determines the attack objective about the comprised element of system. This kind of action It can divide by 'Kernel', 'Userspace', and three 'Other's. Kernel is Primary component of an operating system. For example Network stack, device drivers, virtual memory manager, AIDR. ‘Userspace’ is Area of an operating system where applications are located. For example Applications, middleware, network services, shared libraries, toolchain, AIDR. ‘Other’ is Reside outside the domain of an operating system. For example BIOS, NICs, hypervisors, AIDR.

Attack Classes is the physical, the active attacking the vulnerable point. Injection is Malicious code or data is injected over the network, from a file, or from some other input source. For example Worms, viruses, rootkits. Byzantine is One or more hosts is misbehaving with the intent of adversely affecting other hosts.[11,12] For example Message spoofing and replay, sybil/jellyfish/wormhole attacks. Lifecycle is

Malicious code or data are pre-inserted into software images or updates prior to deployment. For example Backdoors, trojans.

5. Each Area Security Method and Connection

Security of Air-to-ground and Air-to-Air

Air-to-ground COMSEC should ensure that the signals in space used for wireless communication are encrypted at the OSI reference model's physical layer. This would provide protection from eavesdropping by nonauthorized entities and discourage attacks that inject false communications into the data stream. However, these links will remain potentially vulnerable to availability attacks caused by hostile jamming, unless mitigation techniques such as antijamming (AJ) or low probability of intercept/low probability of detection (LPI/LPD) waveforms are used. This study recommends further research using AJ waveforms for air-to-ground communications.

- connect of Air-to-ground

This report recommends that the signals in space (*e.g.*, radio or satellite communications) used for ground-to-air communications must use transport security cover (*i.e.*, encryption of the wireless signal in space occurring at the OSI physical layer). This hinders nonauthorized entities from eavesdropping upon these communications and discourages attempts to potentially inject false communication signals into the data stream (*e.g.*, possible man-in-the-middle attacks). However, these links will remain potentially vulnerable to availability attacks caused by hostile jamming unless mitigation techniques such as AJ waveforms or LPI/LPD waveforms are used.

6. The Security Structure According to the System of Aviation

6.1. ACARS System

In aviation, ACARS is a digital datalink system for transmission of short messages between aircraft and ground stations via airband radio or satellite. The approach to the application layer security is not prepared but this system can apply based on ATN security service. The separate network security plan is not provided and the airplane is made and it is not prepared but LAN security is applied for the restricted and physical domain.

6.2. ATN (CLIP) System

ATN system is providing the security service for the application layer and the separate security service for the network layer is not provided but it can apply the link authentication and password selectively. The airplane is made and the security service is not provided for LAN security but restricted and physical on area can be approached. In ATN message security view, ATN authentication protocol has to be provided for the message security and the safe hash algorithm like HMAC-SHA has to be applied and IPSec is applied. IKEv2 is applied and the key is established in the step logic of the situation and ATN key establishment condition recognition information hosts the air security keylock establishment which if not, is allocated to the prior. Universally, the air key establishment uses much the method that it is shared on the dictionary.

6.3. IP Near Term System

The restrictive SWIM security service is provided for the application layer and it is based on ATN security service in case of U.S.A. The IPSec gone the router for the

network security is applied and the link authentication and code is selectively supported. The airplane is made and LAN security isn't applied but the restrictive physical access is applied.

6.4. IP Long Term System

The restrictive SWIM security service is applied for the application layer security and it is based on ATN security service. The DiD level IPSec has to be applied considering the cost and the security service of the network layer provides the link authentication and password selectively. The airplane is made and the airplane control or fire wall, and *etc*. can be applied for LAN security.[13]

7. Conclusions

According to Pentagon definition, the Airborne network is spoken as the part which is important to the military and future war. Moreover, because the equipment using the wireless network like the robot and drone takes advantage of the wireless network, the security is highly regarded. Therefore, the attack type occurring in the public network was made an inquiry and this dissertation analyze. In the analyzed result network layer, the fact that the weakness is existing according to the attack type could be known. And the kind of attack was various but the Evil Twin, ARP Spoofing, Smurf Attack, and Wireless Transition Attack was remarkably analyze. In case the network is expanded in order to solve this, VPN for the network partition, more setting fire-protection wall, and IPsec protocol security is needed. And the packet Filter and QoS policy controlling the fire wall and access have to guarantee the support for the VPN traffic with the solution about the availability.

Acknowledgments

This research was supported by the ADD and it also supported by Basic Science Research Program through the National Research Foundation of Korea (NRF 2016 Project) funded by the Ministry of Education, Science and Technology.

References

[1] http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/
[2] https://wikileaks.org/nsa-201602/
[3] K. Kwak, Y. Sagduyu, J. Yackoski, B. Sadjadi, A. Namazi, J. Deng and J. Li, “Airborne Network Evaluation: Challenges and High Fidelity Emulation Solution”, IEEE Communications Magazine, **(2014)**.
[4] M. Dempsey, “Joint Concept for Command and Control of the Joint Aerial Layer Network”, U.S. Army, **(2015)**.
[5] K. Kim, Y. Lee and H. Lee, “An Analysis of Security Problem against Wireless Network in Smartphone”, Korea Institute of Information Communication Engineering, **(2014)**.
[6] Y. Jung, “An Evil Twin Detection Method using IP and MAC Address”, Ajou University, **(2013)**.
[7] S. Cho and H. Lee “A Countermeasure against the Abatement Attack to the Security Server”, Journal of the Korea Institute of Information and Communication Engineering, vol. 20, no. 1, **(2016)**, pp. 94-102.
[8] D. Kim and M. Park, “Ad hoc Containment with Arp-Spoofing”, Korea Information Science Society, **(2013)**.
[9] K. Choudhary and M. Shilpa, “Smurf Attacks:Attacks using ICMP”, International Journal of Computer Science and Technology, vol. 2, iss. 1, **(2011)**.
[10] http://www.gizmag.com/battelles-dronedefender-beam-gun-uavs/39885/
[11] P. Chatzimisios, C. Verikoukis, I. Santamaria,M. Laddomada,O. Hoffmann, “Mobile Lightweight Wireless Systems: Second International ICST Conference”, Mobilight 2010, May 10-12, 2010, Barcelona, Spain, Revised Selected Papers, vol. 45, **(2010)**.
[12] I. Askoxylakis, “A dynamic key agreement mechanism for mission critical mobile ad hoc networking”, International Conference on Mobile Lightweight Wireless Systems. Springer Berlin Heidelberg, **(2010)**.

[13] U.S. Department of Transportation , "Networked Local Area Networks in Aircraft: Safety, Security, and Certification Issues, and Initial Acceptance Criteria", National Technical Information Service (NTIS), **(2008)**.
[14] https://en.wikipedia.org/wiki/Airborne_Networking

Authors

Ki Hwan Kim, he received his BS degree in Information Communication Engineering at Dongseo University from Republic of Koear, in 2014. Currently, He is continued Master course in Ubequertus IT at Dongseo University from Republic of Korea. His research interests include cryptography, Information Security, Network Security.

HyunHo Kim, he received his BS and MS degrees in Information Communication Engineering and Ubequertus IT from Dongseo University, Pusan, Republic of Korea, in 2013, 2015. Currently, He's continued Ph.D course in Ubequertus IT at Dongseo University from Republic of Korea. His research interests include Digital Forensic, Information Security, Network Security.

SangGon Lee, he received his BEng, MEng, and PhD degrees in electronics engineering from Kyungpook National University, Rep of Korea, in 1986, 1988, and 1993, respectively. He is a professor in the Division of Computer & Information Engineering, Dongseo University. He was a visiting scholar at QUT, Australia, from August 2003 to July 2004 and at the University of Alabama at Huntsville, USA, from July 2012 to Jun 2013. His research areas include information security, network security, wireless mesh/sensor networks, and the future Internet.

HoonJae Lee, he received his BS, MS, and PhD degrees in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include Password Theory, Network Security, Side Channel Attack, Information Communication/Information Network

