Anatomy Of Unmanned Aerial Vehicle Hijacking With Signal Spoofing

Sait Murat Giray
Communication and Information Systems
Turkish Naval Forces Command
Ankara, Turkey
giray.s1778@dzkk.tsk.tr

Sait Murat Giray
Computer Engineering
Middle East Technical University
Ankara, Turkey
giray.murat@metu.edu.tr

Abstract—An important aspect about unmanned aerial vehicle (UAV, drone) hijacking to emphasize is being highly targeted cyber attack in terms of cyber warfare terminology[1] that covers exploitation, offense, defence and asymmetrical war power as a whole. An attempt of hijacking is a combination of cyber and electronic operations/efforts rather than a single click takeover as it requires several tools and different techniques from cyber and electronic warfare domains simultaneously in a series of actions to achieve its objective particularly when the target is a military vehicle. Multi-stage nature of modern cyber attacks based on the coordination of individual offensive actions [2] encompasses a fully executed UAV capturing assault. GPS spoofing is in the center of these scenarios and an obvious threat against civilian signals but also must be seriously handled in military domain too. Anatomical analysis of UAV hijacking attack delivers insights about vulnerabilities, methods to exploit, mechanisms to detect, how to deter the attack and evaluates the impacts.

Keywords—GPS spoofing; cyber warfare, electronic warfare, UAV hijacking

I. INTRODUCTION AND MOTIVATION

Cyberspace is a combination of hardware, software, networks and communication assets. Therefore cyber domain embraces both virtual and pyhsical worlds and becomes more significant for nation states and their (un)official agencies, public, private and military service branches as well as terrorist organizations and other groups each day. Now it is considered as the "fifth area of opeation" after land, air, sea and space [3]. Global Positioning System (GPS) is a satellite navigation capability that provides accurate location and timing services and widely used for both civilian and military purposes. The definition of an unmanned aerial vehicle (UAV) is expressed as "a powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and carry a lethal or non-lethal payload" in [4]. Today several vehicles in a wide range from small toy-like drones to full-fledged military UAVs are considered as autonomous aircrafts.

There are various studies about GPS vulnerabilities, spoofing and jamming [5] [6] [7]; impacts of such attacks [8][9][42]; detection mechanisms, countermasures [10] [11] [12] and security challenges of UAVs [13]. Most of the studies and works in the literature concentrate on exploitations based on satellite signals or basic architectural system flaws although a few of them spend time on GPS receiver units and vulnerabilities present in the control software, hardware and communication stack [14]. In the light of recent UAV hijack incidents and drone hacking cases [15][16][17] from both civilian and military domain, it is reasonable to assume that a complete UAV hijacking adventure requires an extensive set of cyber and electronic warfare knowledge, experience and equipment(hard/software). Even though this is a strong supposition for civilian UAVs operating on clear access GPS signals that is what it takes to grab yourself a military toy. The focus of this study is the anatomy of seizing drones with spoofing. The plot of a UAV **"take it down and make it mine attack"** is investigated with regards to electronic and cyber warfare since it is deemed achievable by merging tools and techniques from these two families into a single assault. Differences between GPS spoofing and jamming are examined and contributed to this study but profound technical details or any specific attack procedure is not covered since the scope focuses on the anatomy and probability of such scenarios along with the role of unsecure or deceivable space based satellite navigation systems.

My contribution here is two folds: First, I provide an analysis of UAV hijacking attack with an anatomical approach by paying attention to aspects from cyber and electronic domain. Second I outline a model in a step-by-step manner in which such attacks can be observed to see vulnerabilities and deficiencies; how to exploit them; countermeasures, risk mitigation and finally the impacts of attacks. Anatomical investigation of a UAV hijacking by spoofing with regards to cyber and electronic warfare aims to provide insights and to help designers, practitioners, administrators and operators of these assets.

II. GLOBAL POSITIONING SYSTEM

A. GPS Terminology and Basics

The Global Positioning System (GPS) is a space-based radio-navigation system using satellites to provide precise position, velocity and timing information to receivers [18]. Although one satellite is considered sufficient to determine time, at least four satellites are required for an accurate navigational calculation [11]. Time data from satellites are compared with internal receiver clock before calculating the distances between the receiver and GPS satellites in the view area[19]. GPS satellites broadcast encrypted military (P-Code)

and clear civilian (C/A:Coarse/Acquisiton) signals. GPS spreading code is a publicly known unique satellite code [20]. Accuracy of civilian signals dramatically increased after selective availability was cancelled in 2000 [32].

B. Dependency on GPS

GPS and GPS dependent applications penetrated our lifes deeply as using them has a low cost and it is virtually available worldwide. GPS services on different areas include but not limited to navigation (air, land, sea); search and rescue missions, public and community services, vehicle and person tracking (anti-theft, custodial, fleet control) owing to precise location information. Besides being an exact position source, GPS also delivers time synchronization utilized in finance, telecommunication, broadcasting and energy grid management [21]. Since those services are employed in a vast range from daily practices such as driving to recently opened shopping mall to sensitive commercial transactions and mission critical weapon command and control systems, this system is definitely a valuable target.

Today civilian authorities and sectors are taking advantage of GPS much more than military [21]. Reference [19] expresses GPS as an "invisible utility" since nowadays GPS dependent applications are serving to millions of people with different purposes even without being noticed. GPS capability is free to use other than the cost of equipment and software to receive signals and render as desired but this technology suffers from the historical trade-off between free(dom) and security/safety. Basically if something is public and free then it is most likely vulnerable and security is not the major concern of the designers.

C. Inherent GPS Vulnerabilities

Military use of satellite based navigation is assumed to be secure because several system and network level security measures such as encryption and cryptographic authentication are deployed but GPS is unsecure for civilians by design. A built-in liability of GPS system which exposes it to signal attacks and disruptions is its weak signal power of 10^{-16} Watts (-160dBW) on the ground [5] upon which GPS receivers calculate navigational solution .

GPS signals are primarily vulnerable from three fronts. Unintentional interferences such as other Radio Frequency (RF) sources and ionospheric disturbance; intentional interferences being jamming, spoofing and meaconing; human factors like inadequate training, over reliance and design deficiencies [21]. There is a distinction between unintentional interferences like atmospheric effects, signal delays, clock errors that cause position errors and intentioanl ones that leads to total loss of signal or operation on fake signals as specified in [5]. Vulnerabilities exist not only in signal structure and overall system design but also in operating system control software. Reference [14] highlights that the spoofed signals can carry malicious code to exploit receiver software in order to have root access (GPS receiver is a small computer) or perform a denial of service cyber attack by navigation data manipulation.

III. UNMANNED AERIAL VEHICLE

A. Benefits and Characteristics

Recently unmanned aerial vehicles gained popularity and practised upon several extents such as information gathering, counter/intelligence, surveillance and as an assault and active defence vehicle when weaponized. Although it sounds like they mostly have military use and so supposedly secure, interesting civilian applications and deployments are also imminent as individual security guards and surveilance tools [22]. Modern UAVs deliver new operational capabilities in deploying, operating and retrieving equipment and data into/from operation areas those are once considered dangerous and out of human reach [13]. Since drones are free from human restrictions like speed, capacity, predictability, strength, power and durability they are good for furtive operations. UAVs assure great services particularly in military such as equipment transportation, surveillance, reconnaissance, direct attack and combat support [23].

UAV deployments increased in geographical mapping, search and rescue missions, vehicular tracking and surveillance operations [24][25]. Recent developments in technology enabled versatile and very small (size of a humming bird) [26] drones. They are good choices if the task is clandestine and in a remote area. A drone can easily carry biological and chemical agents onboard or peep at a private area [27]. Small sized UAVs and toy drones can easily evade radio wave based detection mechanisms [28] such as air-defence sytems and radars.

B. Weaknesses

Main challenges of UAV security [27] are small size, weight constraints and weak computational power. Since UAVs are quite complex vehicles which comprises of several sub-systems, sensors and long distance interactions, their security is hard to conceptualize and realize too. Moreover there exists a trade-off between security of drones and their functionalities, expected benefits and costs. UAV architecture is described by [23] in physical, computer and communications layers. A security practitioner should see that first layer is the material base that requires physical protection; second layer includes control software and interfaces those are targeted by cyber warfare and finally third layer has links and networking features which are the most vulnerable section since they interact with outside. It is not wrong to expect threats from both electronic and cyber domains in this layer.

C. Motivations Behind Hijacking

Drones are resourceful and useful in airborne offensive and intelligence operations [13] and UAV development demands great amount of brain, time and material investment. The motto of drone hijacking in the contemporary fashion should be "Do not take it down but make it mine" and it is nice and profitable to seize an already developed and operational UAV for the following reasons:

- Self-protection (Neutralize a threat element)
- Opponent Indimidation (Not the powerless you think)
- Capability Demonstration (More than the eye sees)

- Proof of concept (Nobody thinks it is possible)
- Resource Preservation (Man/hours and dollars spent)
- Reverse Engineering (Capturing technical details, deriving data and purpose)
- Propaganda Delivery (Fooling adversary before the local and international community.)
- (Counter)Intelligence Gathering (What are you looking for?)
- Extortion on Assets (Exchange money or other privileges for not revealing secrets)
- Active Assault on Original Owner (Hope you like your own dog food)

Taking possession of a drone that belongs to some other authority may serve as an example and a serios warning with respect to the cyberspace superiority [29] that depends on forestalling interruption to own resources while busting enemy forces. A drone can be converted into a weapon to inflict great amount of damage and carry a message to opponents as a function of aerial aggression [28]. If you let a weapon delivery drone slip out of your hands then there is a strong possibility that the adversary who gains control will drive it back to you with utterly reversed missions. A compromised arsenal carrying UAV may act as a kamikaze bomber just as hijacked passenger planes did in 9/11 incident. As the experts say; "a captured aircraft will help adversaries copy stealth design techniques, coating materials, engine technology, and UAV command-and-control systems and will also help them develop countermeasures" [17]. UAVs turned out to be a good way to deliver arms [30] and perfect machines to spread biological and chemical agents effectively [31]. Therefore it is rational to imagine a waiting list of malicious parties those are craving for a drone somewhere in the world.

IV. SPOOFING, JAMMING AND MEACONING IN HIJACKING ATTACKS

A. The Fundemantals of Intentional Interferences

Jamming essentially forces a receiver to lose track of authentic GPS signals by blocking them and gives opportunity for spoofed signals to show up on the stage. Reception of GPS signals are prevented by sending signals in same frequency but with more power [5] and potential jamming signal types are narrowband, broadband and spread spectrum as detailed in [21]. On the other hand meaconing includes capturing genuine GPS signals, applying a delay and then retransmit to the receiver. The last but the most dangerous is spoofing and it is one of the main threats in satellite navigation services which is simply producing and/or forging GPS signals in order to fool receiving units in terms of position, time and velocity.

False GPS signals are transmitted to take over GPS receivers' position-velocity- time (PVT) solution and success in a spoofing attack is highly achievable for civilian GPS units due to predictability of signal since its observables like GPS message (code tracking) and code range [12] are publicly known and easy to forge while encrypted military signal make it almost impossible to imitate. Steps of spoofing investigated and expressed in [32] as acquiring and tracking C/A signal; producing and calibrating a fake signal; aligning counterfeit one with the original GPS feed and increasing its output to suppress real GPS signal and take over UAV. Spoofing attack itself presents several challenges before being successfully executed but the prize is worthy of all the efforts. One not only disrupts the UAV operation but also seizes a drone. This is the spot where "dont take it down but make it mine" motto makes its debut.

Spoofing and jamming are quite different in terms of their purpose and the way they are executed. Actually spoofing in its most primitive form demonstrates almost the same effect with jamming because it causes signal loss and easily noticed. On the other hand more resourceful spoofing attacks aim to take over GPS signal lock rather than blocking it. In other words jamming violates the availability of the signal while spoofing hurts integrity of the navigation solution. Reference [33] conveys a clear classification of spoofing attacks based on their complexity; Simple attacks produce counterfeit signals and transmits them without paying attention to consistency with authentic GPS signals while intermediate attacks synchronize with broadcasted GPS signals but require more information about the signal such as signal output power, navigation data, direction and satellite reception angles. Finally sophisticated attacks not only synchronize with target GPS signals but also with any other signals originating from other spoofers and signal sources around. It requires multiple antennas as it allocates each antenna for a particular signal and/or receiver unit.

Simple attacks are easy to detect and not effective at all while intermediate attacks are harder to sense when compared with simple spoofing owing to extra signal data used to produce a better fake signal. The most difficult to catch is the advanced one since that kind of attackers are meticilous and ambitious to spend enough resources to fulfill their tasks. Apparently this would be a highly targeted attack against a very particular receiver. Only cyrptography based authentication shall provide security against the last one [34] in which an attacker directs its victim to a desired location gradually. An interesting analogue for spoofing is given by [19] as spoofers deceive a UAV to land onto a location where it thinks home base just like "ship-wreckers used to lure vessels onto rocks with false lighthouse lights."

B. Spoofing Mitigation

Requirements of a succesful attack are sending appropriate spoofing signal with correct timing and making the receiver release legitimate signal and lock on counterfeit one [17]. Considered as the first and one of the most comprehensive warning about civil GPS weaknesses, Volpe Report [35] proposed detection and protection mechanisms against GPS spoofing based on the design and the way the system works as discrimination of arrival, amplitude and cyrptographic authentication. In addition to these, several other spoofing detection methods are offered in [11] and [43] such as observing average signal strength and comparing it with received signal to find significant differences in the received and expected signal strength over time; checking time intervals to see if periods are constant (counterfeit) or variable (authentic); monitoring identification codes of GPS satellites and counting signals to discover fake signals.

Cryptogaphy schemes deliver viable options to secure satellite navigation systems. There are two main types of key based encryption widely known. First one depends on a secret (symmetic) key while the other one uses a public-private (asymmetric) key pair [36]. As stated in [20] using a system wide symmetric key requires both physical and cyber protection of the key and incurs high deployment and management costs. Therefore it fits better into military applications. On the other hand asymmetic key structure presents a good choice for civilian use and a service using this scheme was introduced in [37].

Mitigation methods expressed in [5] are putting a backup navigation/positioning system (inertial navigation) in place; allocating more carrier frequency and increase availability (L1, L2, L5); introducing regulations to apply sanctions for intentional interferences and monitoring integrity of system (RAIM). Cryptographic signal authentication and signing navigation messages or spectrum codes were proposed as spoof-resistance in [32].

V. ANATOMICAL APPROACH ON ATTACK MODELLING WITHIN CYBER AND ELECTRONIC WARFARE

Any unauthorized and unintented access to a system and its resources shall be categorized as an intrusion. Anatomical investigation of an intrusion goes by in a step-by-step manner and outlines an attack.

A. Vulnerability Discovery

One of the most important requirements of anatomical breakdown is identifiying the weaknesses of the target system that open paths to exploitation and leads to loss of control. Therefore vulnerability discovery (target identification) constitutes the first stage. This step is crucial and inevitable for planning attack procedures and identifying required skill set and tools.

Reference [38] makes a clear seperation of three major communication paths in UAVs those are candidate attack vectors for malicious parties as RF links with ground control station (GCS), satellite communication (SATCOM) with GPS satellites and wireless information exchange channels with other UAVs. An adversary may perform attacks against these three locations in an effort of reaching to a targeted UAV. A case study depicted in [44] shows how a cyber attack model attributed to classic computer networks can be utilized to break in UAV communications by a mobile attack drone and a botmaster within Botnet concepts. Furthermore another major location that is capable of presenting flaws to the attackers is the embedded hardware and software [27].

Since each deficiency presents particular risks, it makes sense to categorize them based on the levels they exist. From this point of view, GPS system can be pushed to failure or exploited at the Master Control Station (MCS)/Ground Control Station (GCS) where data messages are produced, uplinks between the MCS/GCS and GPS satellites through which those messages are uploaded; at the signal tranmission channels between satellites and receivers; during reception of GPS signals on receiver units and processing of these data within receiver. First two items are categorized as "system level failures", the third one is an "operation environment impact" and the last two elements are "user level flaws" [39].

B. Attacks on UAVs

Second stage is performing attacks against three pillars of security: confidendiality, integrity and availability (CIA). A cyber security threat model detailed in [38] gives a broader perspective on criteria-attack pairs in which UAV system components and communication ends are under the risk of malicious software, network hacking and human based threats in terms of confidentiality; integrity attacks of disrupting, compromising, capturing and replaying signal feed and finally availability of the system is threatened by signal jamming, spoofing and Denial of Service (DoS) attacks. Three muskeeters of security are partially or completely in jeopardy when UAV hijack attack is underway.

Since a GPS receiver is a small computer with its hardware, software and networking capabilities, types of attacks one can carry out against UAVs are similar to those in traditional computers. Denial of services and flooding the drone by taking advantage of insufficient processing capacity and reduced hardware onboard; taking control of the drone by exploiting wireless communication vulnerabilities; violating the integrity and confidentiality of data gathered in UAV through bugs and vulnerabilities in the operation system stack as well as wireless connectivity; escalating privileges and remote shutdown are primary threats included in cyber warfare as reminded by [27]. Also replay attacks poses a threat even in the presence of encryption [20] and three technics are proposed with their drawbacks to detect them [13] are using external sensors to keep track of deviation from correct position, checking time anomalies against spoofed signal delays and evaluating Doppler shift changes in GPS receiver.

An extreme case about UAV hijacking would be a scenario in which attackers actually infiltrate to the design, implementation and prodcution phases to create backdoors, inject malicious code or any other vulnerabilities in the control software and communication protocols of the drone. Then they can use fake GPS signals as a trigger to activate their malware to takeover the UAV. Nowadays it sounds quite feasible as nations are sponsoring and employing computer experts form both side of the community (white and black hats). It is a head start and reduces the burden of attackers particularly for military UAV hijacks as it sounds easier to sneak into a contractor server than cracking the encrypted military GPS signal. Attacks on the control software of the military GPS receivers may deliver better chances to malicious parties so intentional inferences combined with cyber warfare tools must be considered as the real front to defend.

C. Countermeasure Deployment

Third step of the model is deploying countermeasures against the attack. Although one of the most favorable protection would be applying cryptograhy based signal authentication for C/A signals [37] [9], it is not feasible in near future because the time and money required to apply such design, hardware and software modifications are onerous. Another option is having multiple GPS receivers in one UAV

unit in which control system evaluates and compares the values from different receivers to check whether any noticeable discrepancy exists before calculating navigation solution. In a similar scenario with multiple GPS receivers onboard; only one or a few of them actually contribute to PVT solution while the rest of them function as decoy units to make attack surface more complex. An attacker will need multiple antennas and a complicated spoofing attack to deceive the control system and the efforts may not penetrate the system as the attack might be generating fake signals for GPS units those in fact play no role in navigation of the UAV.

A (pro)active intrusion detection and prevention system in a satellite navigational system would be one that uses one or more of several detection mechanisms introduced till now and as a reaction it may turn-off some of the GPS receivers of which are believed to be compromised; send a warning message to MCS/GCS about the attempt and log the counterfeit signal characteristics if possible for further analysis. The way Google uses extra sensors in their autonomous vehicles for measuring navigational data and cross-checking against GPS is a good model for all GPS dependent unmanned vehicles [9].

D. Possible Impacts of Spoofing and UAV Hijacking

Fourth step of the model is investigating the impacts of these attacks. GPS vulnerabilities genrally affect any time sensitive applications such as telecommunication industry and financial services; position dependent applications like navigation and tracking as well as location based services such as mobile billing. Then a question arises: What can one achieve with spoofing? The answer to this question includes but not limited to unintentional and involuntary behaviours of manned (airplanes) and unmanned aerial vehicles (UAVs), target modification for missiles and avoidance, sabotage on location or timing based services such as stock exchanges and equipment deployments. This is just the beginning of a long list of malicious effects of GPS spoofing particulary taking into account how deep GPS is penetrated our daily lifes. After a UAV is compromised and hijacked, then the very same UAV can act as a mobil stealth spoofer against other targets since "overhead attacks are trivial even if the signal phase synchs with real GPS and an antenna can distinguish direction." [14]. Motivations provided in section III and recent incidents are good examples of the impacts of UAV hijacking.

Although there are not too many UAV targeting attacks recorded or revealed till today, latest events are convincing enough to warn us about the fragility of both civilian and military drones againts electronic and cyber warfare tactics and techniques. Those real life examples include satellites hacked by terorists as in [40], capturing unencrypted UAV video feed with a very cheap software [15], malicious code injected into the systems of a US military base which is a GCS for surveillance and reconnaisance drones [16] and quite famous Iranian UAV hijacking [41].

The case between Iran and USA in which Iran distributed the photos of an undamaged American military drone that is allegedly captured with cyber warfare methods is quite intriguing. GPS spoofing is in the center of this incident. Another case study [9] is performed by the researchers of the University of Texas at Austin in which a drone that belongs to United States Department of Homeland Security is deceived to believe that it should land by confusing its navigation system. The former one is an extreme incident considering the proliferation of unmanned airborne vehicles in the abovementioned areas while the latter one is a compelling proof-of-concept case since the drone is hacked by using a special software and generic hardware with moderate cost.

These incidents ring warning bells after such expert opinion: "It's theoretically possible to take control of a drone by jamming the P(Y) code and forcing a GPS receiver to use the unencrypted, more easily spoofable C/A code to get its directions from navigational satellites." [41]. Also solid proof is presented by [32] to show that civialian drones can be spoofed and controled by attackers and there is quite a suspicion on the security of the military UAVs even though they are deemed to be invulnerable for such interferences.

VI. CONCLUSION

Although military uses encrypted GPS signals with more specialized and hardened software and hardware in their receivers which are more resistant to attacks and inferences, this protection should not be necessarily accepted as ultimate security. Nowadays most dangerous and powerful players in cyber space are nations, nation-sponsored groups, strong transnational organizations, (un)official foreign intelligence and military services. Those listed parties have resources and means to match and defeat the countermeasures and defense mechanisms. Therefore it would be a mistake to completely ignore threats on mission critical and presumably secure military UAVs for secure GPS signals. In addition to that recent UAV hacks and hijack incidents in the so-called secure military domain stand as a proof of this opinion. Cryptographic authentication in GPS signal seems as the best but most unlikely solution particularly for civilian users. Therefore the weaknesses must be admitted by the manufacturers and consumers and an awareness needs to be created about GPS vulnerabilities, basic detection and protection methods and the necessity of backup systems at least for critical systems and UAVs of the future. Attribution in cyberspace is always a problem since attackers generally use intermediary victims to perform an attack to their real targets. Detecting the source of GPS spoofing signal, performing onboard recovery when a UAV is spoofed and remediating after an attack are subjects waiting for further discussion.

DISCLAIMER

The statements, ideas and opinioins expressed in this paper are those of and the responsibility of the author and neither should be ascribed to nor approved by Turkish Naval Forces Command and/or Middle East Technical University.

REFERENCES

[1] US Army, "Cyberspace Operations Concept Capability Plan 2016-2028", TRADOC Pamphlet 525-7-8, 2010.

[2] J.Eom, Y. Han, S. Park and T.Chung, "Active Cyber Attack Model for Network System's Vulnerability Assessment," Information Science and Security, 2008. ICISS. International Conference, pp.153,158, 10-12 January 2008.

[3] The Economist, "Cyberwar: War in the Fifth Domain", 1 July 2010

[4] D.Glade, "Unmanned Aerial Vehicles: Implications for Military Operations", Occasional Paper No. 16, Center for Strategy and Technology, Air War College,pp. 17-19. 2000.

[5] A.Dempster, "How Vulnerable is GPS?",Transportation, 2001.

[6] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer", in Proc. ION GNSS 2008, pp. 2314-2325, September 2008.

[7] N.O. Tippenhauer, C.Pöpper, K.B. Rasmussen and S.Capku, "On the requirements for successful GPS spoofing attacks. ", In Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11). ACM, New York, NY, USA, pp.75-86, 2011.

[8] J.S.Warner and R.G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing", Journal of Security Administration, 2002.

[9] T. Humphreys, "Statement On The Vulnerability Of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing.", July 2012.

[10] Z.Zhang, M. Trinkle, L. Qian, H. Li, "Quickest detection of GPS spoofing attack," Military Communications Conference, 2012 - MILCOM 2012 , pp.1-6, 29 October 2012.

[11] J.S.Warner and R.G.Johnston, "GPS spoofing countermeasures.", Homeland Security Journal, 2003.

[12] H.Wen,P.Y.R. Huang, J. Dyer, A. Archinal and J. Fagan. "Countermeasures for GPS signal spoofing.",In ION GNSS, pp. 13-16, 2005.

[13] C. Constantinides and P. Parkinson, "Security challenges in UAV development." Digital Avionics Systems Conference,2008,DASC 2008. IEEE/AIAA 27th, pp.1-C, 26-30 October 2008.

[14] T.Nighswander, B.Ledvina, J.Diamond, R.Brumley and D.Brumley. "GPS software attacks",In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), ACM, New York, NY, USA, pp.450-461,2012.

[15] C. Arthur, "SkyGrabber: the $26 software used by insurgents to hack into US drones", Guardian, 17 December 2009.

[16] Associated Press, "Computer virus infects drone plane command center in US", Guardian, 9 October 2011.

[17] D.Majumdar,"Iran's captured RQ-170: How bad is the damage?", Defense News, 9 December 2011.

[18] Federal Radionavigation Plan-FRnP, Interagency GPS Executive Board, Washington, DC, 1999.

[19] D. Hambling, "GPS fail: how a little black box could cause chaos" New Scientist, Volume 209, Issue 2803, pp.44-47,12 March 2011.

[20] P.Papadimitratos and A.Jovanovic,"Protection and fundamental vulnerability of GNSS," Satellite and Space Communications, 2008. IWSSC 2008, IEEE International Workshop, pp.167-171, 1-3 October 2008.

[21] D.Hoey and P.Benshoof, "Civil GPS Systems and Potential Vulnerabilities" Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS *2005)*, Long Beach, CA, pp. 1291-129. September 2005.

[22] *E.* Ackerman,"Japanese Security Firm to Start Renting Surveillance Drones",IEEE Spectrum, 29 December 2012.

[23] W.R.Dufrene Jr, "Mobile military security with concentration on unmanned aerial vehicles", In *Digital* Avionics Systems Conference, *DASC 2005.* The 24th (Vol. 2, pp. 8-pp). IEEE, 2005.

[24] X.C.Ding, A. Rahmani and M. Egerstedt, "Optimal multi-UAV convoy protection",Conference on Robot Communication and Configuration, Volume 9, Pages 1–6, April 2009.

[25] J. Tisdale, Z. Kim, J. Hedrick, "Autonomous UAV path planning and estimation", IEEE Robotics and Automation Magazine, Volume 16, Issue 2, pp.35–42, 2009.

[26] M.Boyer, "AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA, 17 February 2011.

[27] E.Deligne,"ARDrone corruption.",Journal in Computer Virology pp.1-13, 2012.

[28] Lele, Ajay and A.Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles.", Journal of Defence Studies 3, no. 3, pp.54-65,2009.

[29] J. Eom, N.Kim, S.Kim; T.Chung, "Cyber military strategy for cyberspace superiority in cyber warfare," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on,pp.295-299, 26-28 June 2012.

[30] D.M. Gormley, "UAVs and Cruise Missiles as Possible Terrorist Weapons." New Challenges in Missile Proliferation, Missile Defense, and Space Security, Monterey, Calif.: Monterey Institute of International Studies, Center for Nonproliferation Studies, Occasional Paper 12, pp.3-9,2003.

[31] E.Eitzen, "Chapter 20—Use of Bio Weapons," in Medical Aspects of Chemical and Biological Warfare (Washington, DC: Walter Reed Army Medical Center), pp. 440-442,1997.

[32] P.S.Daniel., et al. "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks." ION GNSS Conference Nashville, TN, September 2012.

[33] T.H.Kim, C.S.Sin,S.Lee, "Analysis of effect of spoofing signal in GPS receiver," Control, Automation and Systems (ICCAS), 2012 12th International Conference on, pp.2083-2087, 17-21 October 2012.

[34] T.E.Humphreys, M.L.Psiaki and P.M.Kintner,Jr,"GPS Spoofing Threat",2009.

[35] J.V. Carroll, "Vulnerability assessment of the us transportation infrastructure that relies on the global positioning system." Journal of Navigation 56.2,pp.185-194,2003.

[36] S.J.Gustavus, "Symmetric and asymmetric encryption." ACM Computing Surveys (CSUR) 11.4, pp.305-330, 1979

[37] G.K.Hein, F.A.Rodriguez, and J.A.Wallner, "Authenticating GNSS: Proofs against Spoofs, Part 2. Inside GNSS", pp 71-78, October 2007.

[38] A.Y. Javaid, S.Weiqing, V.K. Devabhaktuni and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system", In Homeland Security (HST), 2012 IEEE Conference on Technologies for, pp. 585-590. IEEE, 2012.

[39] Ochieng ,Washington Y., et al. "GPS integrity and potential impact on aviation safety.", Journal of Navigation 56.1, pp. 51-65,2003.

[40] S. Northcutt, "Are Satellites Vulnerable to Hackers?", SANS Technology Institute, 15 May 2007.

[41] A.Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible.", Wired,December 2011.

[42] P.Papadimitratos and A.Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures", In Military Communications Conference, 2008. MILCOM 2008, IEEE, pp. 1-7, 2008.

[43] Iqbal, M.Usman and S.Lim, "Legal and ethical implications of GPS vulnerabilities." J. Int'l Com. L. & Tech. 3 (2008): 178.

[44] T. Reed, J. Geis and S. Dietrich, "SkyNET: a 3G-enabled mobile attack drone and stealth botmaster", Proceedings of the 5th Usenix Workshop on Offensive Technologies (WOOT 2011), August 2011.