Enhanced Security Mechanisms for the Selected Cyber Attacks in UAV Networks

N VANITHA and G PADMAVATHI
Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, University, Coimbatore, Tamil Nadu, India
Department of Information Technology,Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, Indiavanitha969@gmail.com, ganapathi.padmavathi@gmail.com

ABSTRACT

A vehicular ad-hoc network (VANET) presents wireless communication with vehicles and vehicles to road side kit's. In VANET the frequent path failures, the high mobility, frequently disconnected topology and network traffic density which may affect the reliability of data transmission and routing. These problems are solved using the UAV supported VANET architecture having U2V/V2U communication. Unmanned Aerial Vehicles (UAV), which can fly unconventionally or can be activated remotely without carrying any individual personnel. Unmanned Aerial Vehicles (UAVs) have been extensively used for several applications. Ad-hoc networking between UAVs (FANET- Flying Ad-hoc Networks) can crack the troubles happening from a fully infrastructure supported UAV networks [2]. This work proposes a decentralized multi-layer UAV ad-hoc network supported vehicular ad-hoc network architecture along with explore the system components. This work analyses and compares the various false data dissemination attacks and impact of those attacks on various architectures. This paper proposes four step methodologies in order to monitor detect and block FDDA attacks on proposed architecture of UAV network. The network and threat models are simulated using NS3 and the data sets are analyzed and optimized using machine learning techniques to detect and block the FDDA attacks on the enhanced architecture.

Introduction

A vehicular ad-hoc network (VANET) provides wireless communication among vehicles and vehicles to road side equipment's. In VANET the frequent path failures, the high mobility, frequently disconnected topology and network traffic density which may affect the reliability of data transmission and routing. These problems are solved using the UAV assisted VANET architecture having U2V/V2U communication. Unmanned Aerial Vehicles (UAV) systems, which can fly autonomously or can be operated remotely without carrying any human personnel. To date, Unmanned Aerial Vehicles (UAVs) have been extensively used for numerous applications. UAVs can openly connect to ground stations or satellites to transfer data. Multiple UAVs can communicate and cooperate with each other and then construct an ad-hoc network. Ad-hoc networking between UAVs (FANET- Flying Ad-hoc Networks) can solve the problems arising from a fully infrastructurebased UAV networks. Along with these rapid developments of UAV applications, the spread of attacks are also increasing. Among the various cyber-attacks, False Data Dissemination attack is one of the serious security threats that affect the UAV networks. The UAV's infrastructures are significantly damaged by False Data Dissemination attacks through their vulnerable exploitation in the nodes and applications. Moreover, these threats are seriously increasing by the introduction of the Internet of Things (IoT).

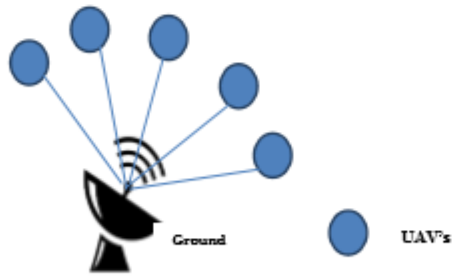

Figure 1. Simple UAV network

Applications

UAVs have a great prospective to build numerous applications in both military and civilian domains. Applications include, Military, Civilian, Healthcare, emergency etc

Research Motivation

The damages caused by False Data Dissemination attacks during the past 15 years created serious security threats and large financial losses in the world.Some of the infections and damages caused by False Data Dissemination attacks are listed in table.1.1 below.

Table 1: Potential Damages caused by False Data Dissemination Attacks

Year	Name of FDDA	Infection
2004	Target killing Place: US	Innocent civilians:20% High level targets:2%
2006	Propaganda	Psychological warfare
2010	Stuxnet	Cyberwar
2016	Spoofing sensor	Financial Loss: £670 million

To avoid expensive damages caused by False Data Dissemination attacks, False Data Dissemination attacks defense schemes are very important for the safety and security of the systems connected to the network. To overcome the problems of False Data Dissemination attacks and provide effective defense mechanism, clear knowledge on False Data Dissemination attacks is necessary.

Objectives

The primary objective of the research work is to design and device a defense mechanism for achieving better detection and mitigation of False Data Dissemination attacks on UAV Networks.

The secondary objectives of the thesis are:

- Improve the detection and classification accuracy
- Reduce the communication overhead
- Decrease False Positives
- Efficiency
- Minimize Energy consumption

Significant Contributions of the research

- Provides a brief study on specific cyber-attacks on UAV, especially FDDA on UAV Networks.
- Highlights of the related works
- Describes the proposed decentralised multi-layer UAV assisted VANET architecture along with attack model that can occur in such network for improved performance.

- Describes an agent-based intrusion monitoring, detection and mitigation techniques based on Rule based Extreme Learning Machine(ELM).
- Experimental set up using NS3 simulation results and analysis.

Review of Literature

S.No.	AUTHOR	TITLE	JOURNAL NAME	YEAR	Techniques Used	LIMITATIONS
1	R. Mitchell and I. R. Chen	Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications	IEEE Trans. Syst	2014	Behaviour Rule based Intrusion detection frame work	Detection latency, Attack model, Defender's response
2	Hichem Sedjelmaci , Sidi Mohammed Senouci and Nirwan Ansari,	Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology	IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATIONSYSTEMS	2017	Security Game Frame work has been established. A Bayesian game formulation between the IDS and attackers	Only for UAV aided network Not for UAV alone
3	Alireza Abbaspoura, Kang K. Yena, Shirin Noeib, Arman Sargolzaeic	Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network	ScienceDirect Procedia Computer Science	2016	Embedded Kalman filter (EKF) with Neural Network	Detecting attacks in the sensors
4	Hichem Sedjelmaci , Sidi Mohammed Senouci and Nirwan Ansari	A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks	IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS	2016	IDS Agent UDA and response scheme	Detection rate is 93 % only
5	Sang-Hyeon Kim, Lebsework Negash, Han-Lim Choi	Cubature Kalman Filter Based Fault Detection and Isolation for Formation Control of Multi-UAVs	SCIENCE DIRECT IFAC-PapersOnLine	2016	Cubature Kalman Filter(CKF) based fault detection scheme And Scalar testing algorithm	Isolates the faulty node

Proposed Upgraded Architecture

Proposed architecture is Multi-Layer UAV Ad Hoc Network supported Vehicular ad hoc network architecture. It is a decentralized architecture.

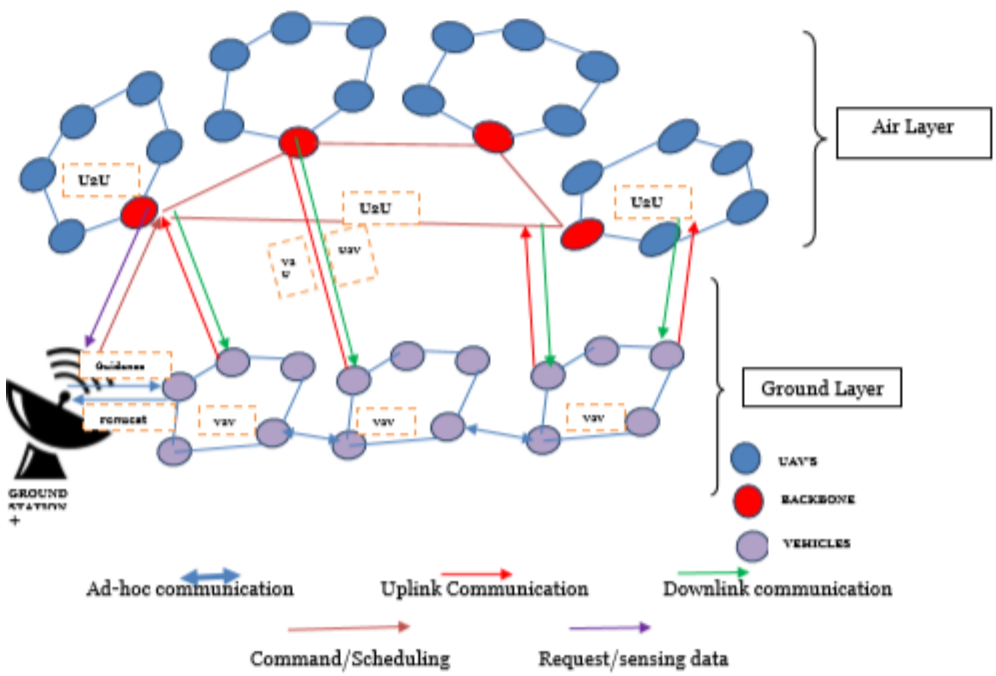

Figure 2: Decentralized Multi-Layer UAV Ad Hoc Network supported Vehicular ad hoc networks

UAVs will facilitate ground vehicles explore the realm of interest and enhance the property of the vehicular network. Figure 2. depicts the cooperative networking architecture of the multi-layer UAV assisted vehicular network, that may be a decentralized architecture, composed of an aerial multi-UAV subnet work and a ground vehicular subnet work. In this section, we tend to principally investigate the twolayer networking. Three varieties of communication links are presented within the multi- layer UAV ad-hoc network assisted vehicular ad hoc network, as well as U2U links, V2V links, and U2G links,respectively [4].

Features of proposed architecture

- Scalable
- No single point failure
- Robust
- Minimizes network overhead

Security challenges and attacks in UAV network architecture

Security plays a major role in UAV to VANET communication. This work particularly focuses on cyberattacks classifications based on their nature specific to UAV assisted Vehicular ad-hoc networks. False data dissemination attack is most dangerous cyber-attack that affects the UAV network. A malicious UAV might broadcast a special natural phenomenon like environmental conditions or forest fires to its neighbor's. Such attack is defined as a false information dissemination attack. This paper concentrates on most dangerous cyber-attack (i.e.) false data dissemination attack [6].

These attacks can be classified into following types, Figure 3 shows the classification of cyber-attacks on UAV ad hoc Networks,

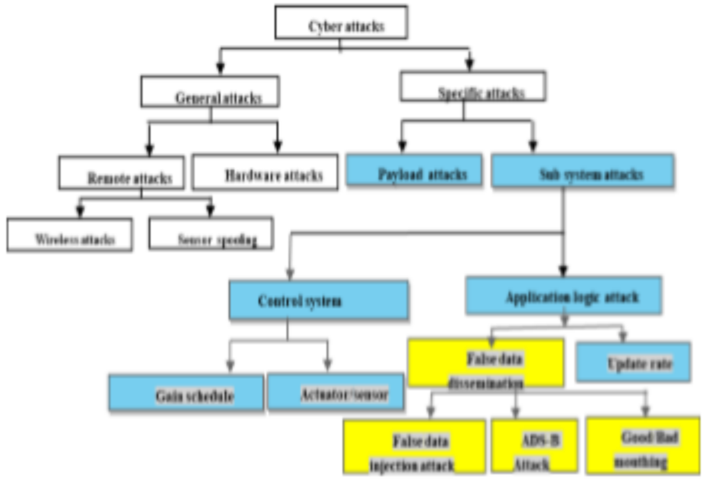

Figure3. Classification of Cyber-attacks in UAV ad-hoc network

A. False data injection attack

The resister injects forged information measure data into UAV network routing messages. The bandwidth misleading attack is outlined as an interruption, within which the resister injects forged bandwidth data into UAV network routing messages. The goal of this attack is to disrupt the routing method of knowledge transmission [5].

1. High bandwidth misleading attack
2. Low band width misleading attack

B. The ADS-B attack

According to [05] and [06], an ADS-B attack moreover aims to televise a forged location or spoof the GPS coordinates (i.e., GPS spoofing) of an objective UAV. Therefore, the survivability of genuine drones is affected [07]. ADS-B can provide more accurate UAV's location information at faster update rate, and broadcasts the useful information at a fixed radio frequency. These signals are vulnerable to spoofing [9], [10].

C. Bad/Good mouthing attack

A malicious intrusion detection agent, might also offer fake discovery information to corrupt the network performances [5],[12].

1. Bad mouthing (also known as slandering, unfairly negative recommendation)
2. Good mouthing (also known as ballot stuffing/ Self-promoting, unfairly positive recommendation)

Table 2. Describes the impact and parameters affected by the false data dissemination attacks on architecture of UAV networks [11],[12],[13].

TABLE 2: Impact of False Data Dissemination attack on Architecture of UAV networks

False Data Dissemination attack	Architecture	Impact of FDDA attacks	Parameters affected
False Data Injection	Centralized	Ground station will get false information about UAV and it disseminate the false information to all UAVs. Communication overhead occurs in the ground station Packet drop rate increases due to false bandwidth injection Overall network performance	Communication Latency Throughput Handoff and Roaming Transmission Robustness Data traffic, Delay jitter Bandwidth (data rate)
	Decentralized	Network congestion Packet loss Packet collision Backbone UAV also attacked by false data injection Attack on backbone UAVs the whole group will not get correct information from another group of UAV's Overall network performance will get reduced	Throughput not much effected compared to centralized architecture Communication Latency and between groups or in layer. Mobility pattern changes Transmission robustness Data traffic, Delay jitter Bandwidth (data rate)
	DecentralizedMulti-Layer UAV ad-hoc network assisted VANET	Network congestion Packet loss Packet collision Backbone UAV also attacked by false data injection	Throughput Communication Latency. Mobility pattern changes Data traffic, Delay jitter Bandwidth (data rate)
Spoofing GPS	Centralized	Problem in identifying the particular UAV UAVs moved out from the communication range Ground station will broadcast the false position of UAV. UAV crash	Communication Latency Throughput Degree of Mobility Handoff and Roaming Transmission Robustness Delay jitter Node Survivability
coordinates	Decentralized	Mobility pattern will be changed Attacked UAV will be out of range Not possible to identify the attacked UAV by Ground station or backbone UAV's Backbone UAV's GPS coordinate get spoofed then whole network information spoofed by others Particular UAV's survivability affected. Group survivability affected because of backbone UAV's GPS coordinate spoofing.	Mobility Throughput Packet delivery Handoff and Roaming Transmission Robustness Data traffic, Delay jitter Bandwidth (data rate) Communication Latency
	Decentralized Multi-Layer UAV ad-hoc network assisted VANET	Node out of range Particular UAV's survivability affected Group survivability affected because of backbone UAV's GPS coordinate spoofing	Mobility Throughput Packet delivery Handoff and Roaming Transmission Robustness Data traffic, Delay jitter Bandwidth (data rate) Communication Latency

Good/Bad Mouthing	Centralized	False detection of attacker Increased False Positive and False Negative Sends the false detection response to Ground station and it will broad cast the good node as malicious node to all UAVs and vice versa Overall network performance	Communication Latency Throughput Data traffic Handoff and Roaming Transmission Robustness Packet delivery
	Decentralized	Sends false attacker information to UAV's, Backbone UAV's and Ground Station as a response. Not sharing of information Information not reachable for intended recipient in a group Information not reachable for an intended group Information will be taken by malicious node.	Communication Latency Throughput Handoff and Roaming Transmission Robustness Packet delivery
	Decentralized Multi-Layer UAV ad-hoc network assisted VANET	Ground station will get false information about UAV and it disseminates the false information to all UAVs and vehicles. Communication overhead occurs in the air layer and ground layer Over all network performance will get effected	Communication Latency Throughput Handoff and Roaming Transmission Robustness Packet delivery Packet Loss

Causes of Attacks on Architectures of UAV Network

These attacks cause, increased overhead routing, propagation delays, low packet delivery success rates and traffic. Table 3 summarizes the attacks and its effects on the goals of security on Multi-Layer UAV Ad Hoc Network Architecture.

The security goals of UAV communications include availability, confidentiality, integrity, authentication, and non-repudiation [7].

TABLE 3: Principles of security and attacks on various architecture of UAV

Attacks/Security Principles	Confidentiality			Integrity			Availability			Authentication			Non-Repudiation		
	CA	DA	PA	CA	DA	PA	CA	DA	PA	CA	DA	PA	CA	DA	PA
GPS Spoofing attack					✓	✓	✓	✓		✓				✓	✓
False data injection attack	✗	✗	✗	✗	✗	✗		✗	✗		✗	✗	✗	✗	✗
Good/Bad Mouthing	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓

*CA-Centralized Architecture *DA-Decentralized Architecture * PA-Proposed Architecture

Detailed Research Plan including Methodology

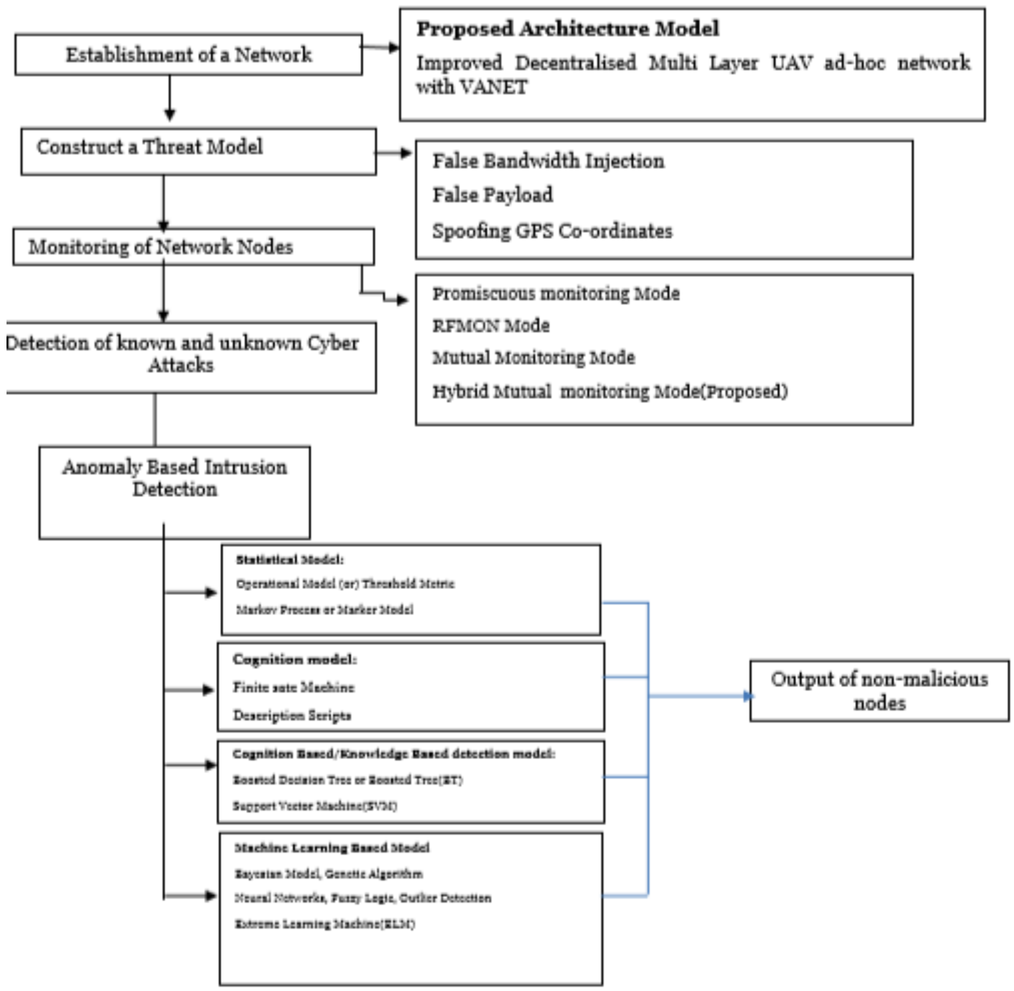

Figure 4. Methodology for Detection and blocking of FDDA attacks

Significant Contributions of the Work

Contribution1: Detection of False bandwidth injection in the Protocols. Backward Feature Elimination, OS-ELM,GA based Optimized Containment Algorithm

Contribution 2: Detection of payload attacks. PCA, CNN, RandomizedLas Vegas algorithm

Contribution 3: Detection of GPS co-ordinate spoofing of a vehicle. Random Forest, ELM autoencoder and Embedding,Blacklist Algorithm

Contribution 4: Detection of good and bad mouthing. kernel PCA, RIPPER,Automated Node Containment Algorithm

A Four-Step Methodology is proposed to meet the objectives of the work. The whole research part is discussed in four phases based on the four-step methodology.

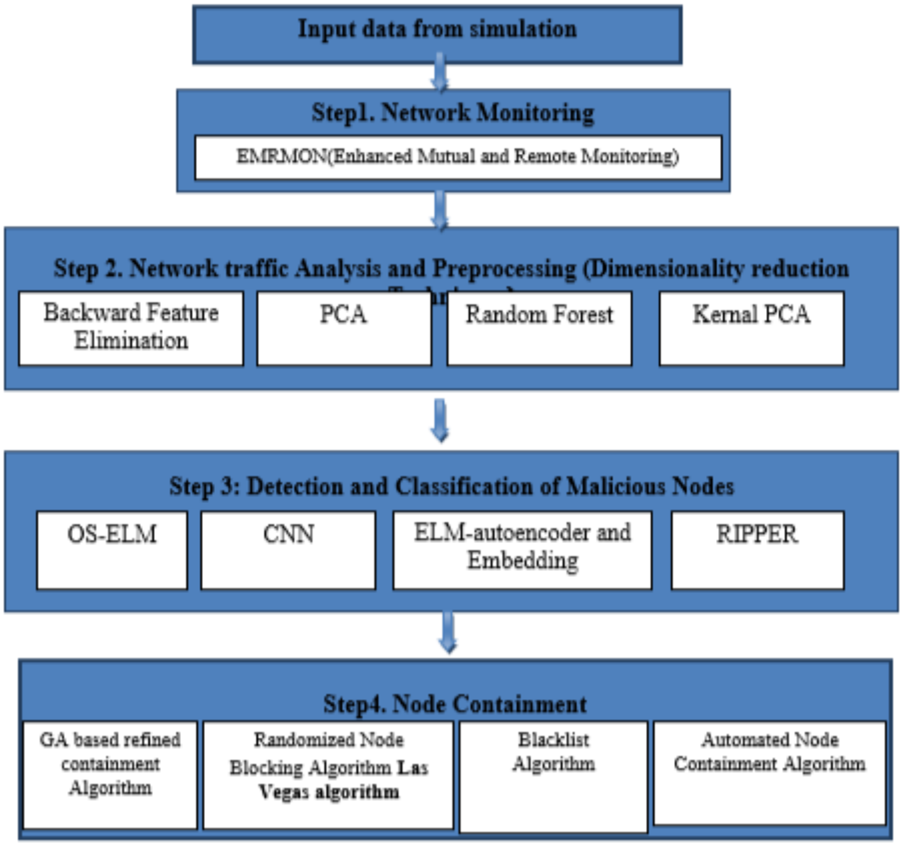

Figure 5. The Proposed Four-Step Methodology

Conclusion and Future work

This research work is proposed to detect known and unknown FDDA attacks based on their characteristics (i.e.) disseminating the false data. We have to use NS3 Tool to simulate the network model and threat model and generate traffic to get dataset. Then apply our four step methodology to monitor, detect and block the malicious node that performs FDDA attack in future.

References

[1]Jun Li, Yifeng Zhou, and Louise Lamont. (2013). Communications Research Centre Canada: Communication Architectures and Protocols for Networking Unmanned Aerial Vehicles. 3701 Carling Ave. Ottawa, ON. K2H 8S2 Canada, 1415-1420.

[2] Ivan Maza, Anibal Ollero Boeing. Research & Technology Europe. Enrique Casado and David Scarlatti: Classification of multi-UAV Architectures, 1-24.

[3] Yi Zhou, Nan Cheng, Ning Lu, and Xuemin (Sherman) Shen (December 2015), IEEE vehicular technology magazine: Multi-UAV-Aided Networks, 36-44.

[4] N. Goddemeier, K. Daniel, and C. Wietfeld(June 2012). IEEE J. Sel. Areas: Role-based connectivity management with realistic air-to-ground channels for cooperative UAVs Commun, 30(5), 951–963.

[5] HichemSedjelmaci, Sidi Mohammed Senouci and Nirwan Ansar. (March 2017). IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS SYSTEMS: A Hierarchical Detection and Response System to Enhance Security against Lethal Cyber-Attacks in UAV Networks, 1-13.

[6] Kim, A., et al. (2012). Infotech@ Aerospace: Cyber-attack vulnerabilities analysis for unmanned aerial vehicles, 1-30.

[7] Daojing He, Sammy Chan, and Mohsen Guizani. (August 2017), IEEE Wireless Communication: Communication Security of Unmanned Aerial Vehicles, 134.

[8] Yogesh Anil Nijsure., et al. (May 2016). IEEE Transactions on Vehicular Technology: Adaptive Air- to – Ground Secure Communication System Based on ADS-B and Wide-Area Multilateration, 65(5).

[9] ThabetKacem, et al., IEEE 19th International Conferencce on intelligent Transportation Systems: Secure ADS-B Framework ADS-Bsec, 2681-2686.

[10] Zhiyuan Shen, Han Wang,(November 2017). IEEE Computer Society: An ADS-B Spoofing Attack Detection Method based on LASSO Ensemble Emprical Mode Decomposition, 2015.

[11] Z.Bankovic, J.C.Vallejo, D.Fraga. J.M. Moya. (December 2014). Researchgate.net: Detecting BadMouthing Attacks on Reputation Systems Using Self-Organising Maps.

[12] Zakirullah, M. Hasan Islam, Adnan Ahmed Khan.(July 2014). IEEE 5th International Conference(ICCCNT): Detection of Dishonest Trust Recommendations in Mobile AdHoc Networks.

[13] Farah Khedim, Nabila Labraoui, MohemedLehsaini. (April 2015). IEEE 12th International Symposium: Dishonest Recommendation Attacks in Wireless Sensor Networks: A Survey.