A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks

ABSTRACT

Unmanned aerial vehicles (UAVs) have initially been utilized in military applications to engage in air-to ground combats, surveillance, and target tracking in hostile environments. Surveillance primarily concerns collection, analysis, and management of critical information in critical sites (airport area, nuclear site, etc.). Tracking is the operation of following mobile targets (suspected persons or vehicles) and monitoring their behaviors. Nowadays, UAVs are also used in civil applications to explore inaccessible zones (e.g., disaster areas) and deliver data to and from areas with no network infrastructure (3G, 4G, etc.) [1]. An UAV network is a wireless ad-hoc network that facilitates UAV-to-UAV and/or UAV-to-ground communications in order to deliver vital information for environmental monitoring, emergency, rescue and recovery operations, and disaster assistance. Setting up an ad-hoc network consisting of UAVs is very challenging because they differ from mobile ad-hoc networks (MANETs) and vehicular ad-hoc networks in terms of mobility, connectivity, routing, services, and applications.

EXISTING SYSTEM

In Existing System, Unmanned aerial vehicles (UAVs) networks have not yet received considerable research attention. Specifically, security issues are a major concern because such networks, which carry vital information, are prone to various attacks.

DIS ADVANTAGES

- Lethal cyber-attacks that can target an UAV network.
- GPS spoofing, jamming, and black hole and gray hole attacks are more.

PROPOSED SYSTEM

In Proposed System, a set of detection and response techniques are proposed to monitor the UAV behaviors and categorize them into the appropriate list (normal, abnormal, suspect, and malicious) according to the detected cyber-attack. We focus on the most lethal cyber-attacks that

can target an UAV network, namely, false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks. Extensive simulations confirm that the proposed scheme performs well in terms of attack detection even with a large number of UAVs and attackers since it exhibits a high detection rate, a low number of false positives, and prompt detection with a low communication overhead.

ADVANTAGES

- Attack detection even with a large number of UAVs and attackers.
- It exhibits a high detection rate, a low number of false positives, and prompt detection with a low communication overhead.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.

Database : MySQL 5.0

Database Connectivity : JDBC