Revista ITECKNE - Universidad Santo Tomás, Seccional Bucaramanga, Colombia, Vol. 18 Nº 2 julio - diciembre de 2021

Sistema de valoración funcional para sistemas de aeronavegación no tripulados a partir de la calidad de la información

Functional assessment system for unmanned aerial navigation systems from the quality of information

Leonardo Serna-Guarín[1]; Juan David Grajales-Bustamante[2]; Miguel Becerra[3]

[1] Institución Universitaria ITM, Medellín, Colombia, leonardoserna@itm.edu.co
[2] Institución Universitaria ITM, Medellín, Colombia, juangrajales@itm.edu.co
[3] Institución Universitaria Pascual Bravo, Medellín, Colombia, miguel.becerra@pascualbravo.edu.co

Fecha de recepción: 22 de diciembre 2020. Fecha de aprobación: 24 de marzo de 2021

Resumen- **Los sistemas de aeronavegación no tripulados son utilizados en múltiples aplicaciones militares y no militares. Sin embargo, estos sistemas son susceptibles de ser intervenidos por delincuentes informáticos parcial o totalmente. En este artículo se propone un *framework* basado en el modelo JDL para la evaluación de la seguridad de los drones y se establecen criterios de evaluación de desempeño y de calidad de la información para cada nivel de la fusión, en conjunto con un sistema de mapeo de estas métricas, con el fin de determinar la dependencia de los datos entre diferentes niveles, contemplando la valoración contextual del usuario.**

Palabras clave- **Calidad de la información; fusión de datos; vehículo aéreo no tripulado (UAV); seguridad de datos.**

Abstract- **Unmanned aerial navigation systems are not used in many military and non-military applications. However, these systems are susceptible be operated by hackers partially or completely. Therefore, in this article based on the JDL model for safety assessment of the drone's *framework* it is proposed. Metrics for each level of the merger in conjunction with a mapping system in order to determine the dependence of data between different levels are proposed, considering the contextual user ratings.**

Keywords- **Information quality; data fusion; unmanned aerial vehicle; data security.**

1. INTRODUCCIÓN

Los drones son utilizados en TI tanto para aplicaciones específicas como de entretenimiento. Su tecnología ha llevado estos dispositivos al desarrollo de múltiples soluciones, por lo cual su uso se torna transversal en muchas disciplinas, entre las que cuenta el uso militar (e.g. detección de targets y recolección de información en campos de batalla) y en el uso comercial (e.g. monitoreo de procesos industriales, monitoreo del medio ambiente, agricultura, vigilancia); sin embargo, presenta desafíos propios de su arquitectura, tales como: censado, peso, autonomía, calidad, seguridad y privacidad, tanto para el manejo de la información captada, como también para los datos de control del dispositivo, entre otras medidas de desempeño [1][2].

La utilización de drones implica tener presente aspectos de vuelo seguro donde se destacan características que deben ser monitoreadas, tales como: integridad del dispositivo equipado para eventos de pérdida en la comunicación,

Citar este artículo como: L. Serna-Guarín, J.D. Grajales-Bustamante, M. Becerra. Sistema de valoración funcional para sistemas de aeronavegación no tripulados a partir de la calidad de la información. *ITECKNE*, 18 (2), 2021 pp. 108- 120 DOI: https://doi.org/10.15332/iteckne.v18i1.2547

capacidad de retorno a su lugar de partida o base de manera autónoma, evasión de objetos para evitar colisiones, navegación en áreas seguras evitando invadir espacios aéreos restringidos, consumo de energía, altitud, velocidad, línea de visión, inclemencias del tiempo, multitudes y el sonido o ruido entre otros [2][3]. El monitoreo realizado por estos dispositivos demanda múltiples sensores y cámaras, cuya información es procesada y/o enviada a los mandos o estaciones de control usando sus sistemas de comunicación a través de redes de sensores inalámbricas (*WSN*, por sus siglas en inglés) los cuales podrían ser insuficientes si se encuentran soportados únicamente en protocolos y *hardware* debido a la incertidumbre en las áreas en que son implementadas, por lo que las *WSN* pueden presentar decisiones poco confiables [4]. De igual forma, los datos censados pueden ser ambiguos, imprecisos e incompletos, o una combinación de estos [5]. Esta situación genera incertidumbre en los sensores, y a su vez ambigüedad e inconsistencia presente en el ambiente y la incapacidad de distinguir entre ellos [6]. Para disminuir la incertidumbre en la información, la literatura reporta ampliamente el uso de la fusión de datos, la cual es considerada como un paso crítico en el diseño de una *WSN* como base de la transferencia de datos en vehículos aéreos no tripulados, ya que permite incrementar la confianza y fiabilidad de las mediciones, disminuir la carga de información y el envío de paquetes redundantes en los sistemas de transmisión, incrementa el tiempo de vida útil de la red, mejora la detección mediante la ampliación de la cobertura espacial y temporal y reduce la ambigüedad de los datos [7].

Algunos autores [8] definen la fusión de datos como un "proceso multifacético y multinivel que manipula la detección automática, asociación, correlación, estimación y la combinación de los datos y la información de una o varias fuentes". Igualmente, en las *WSN* se utiliza el término de calidad de los datos con diferentes significados. Los autores en [9] expresan la exactitud, la consistencia, el tiempo de vida y la completitud para estimar la calidad de la información en la fusión de datos sobre una red de sensores. Adicionalmente, en [10] se utiliza la calidad de la fusión (*QoF,* por sus siglas en inglés) y la eficiencia para la implementación de un sistema de fusión de datos en paralelo, con el fin de obtener propiedades de autoadministración en una *WSN*. Por otra parte, se habla de calidad de las *WSN* basado en métricas de enrutamiento en términos de eficiencia de la transmisión, teniendo en cuenta diferentes variables como el consumo de energía y el tráfico [11][12][13]. Así mismo, varios autores definen la calidad usando el término de Calidad del Servicio (*QoS*, por sus siglas en inglés) para un grupo de varias métricas de calidad, y definen esta [14] como "la capacidad de proporcionar con seguridad que los requerimientos de servicio de las aplicaciones puedan ser satisfechos". En [15] los autores establecen *QoS* del enrutamiento basado en el retardo, la energía y el ancho de banda, manteniendo un balance entre la energía y la calidad de los datos. Otros autores [16] mencionan el *QoS* en las redes inalámbricas de sensores y actuadores (*WSANs*, por sus siglas en inglés) basados en la confiabilidad, los retardos de tiempo, la robustez, la disponibilidad y la seguridad; adicionalmente, utiliza el retardo, el jitter y la pérdida de paquetes para medir el grado de satisfacción del servicio. Es así como se han venido haciendo investigaciones en protocolos de comunicación con el fin de reducir el consumo de energía, incrementar la vida útil de las baterías, disminuir el reenvío de paquetes y otras características requeridas por aplicaciones particulares [14][17][18].

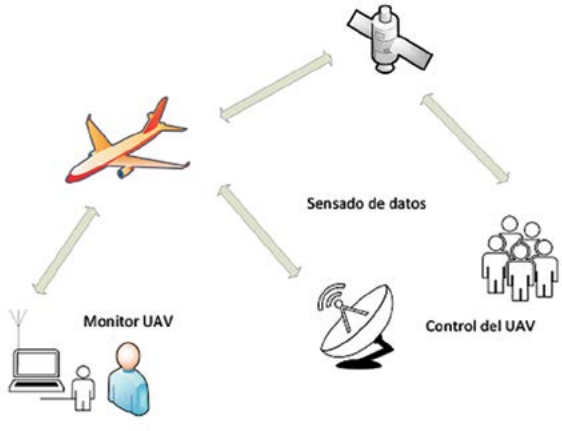
Por lo anterior, se hace necesario establecer de manera formal la calidad de la información en las *WSN* que soporta la comunicación de un vehículo aéreo no tripulado (UAV, por sus siglas en inglés) de forma tal, que se puedan realizar análisis más confiables y optimizar el desempeño de los sistemas y la interacción hombre máquina. En este artículo, se propone un *framework* basado en el modelo JDL para la evaluación de la seguridad de los drones y se establecen criterios de evaluación del desempeño y de calidad de la información para cada nivel de la fusión, en conjunto con un sistema de mapeo de estas métricas, con el fin de determinar la dependencia de los datos entre diferentes niveles, contemplando la valoración contextual del usuario.

2. ANTECEDENTES

Los desarrollos tecnológicos de drones contienen elementos electrónicos dotados de un sistema de comunicaciones para el control y la búsqueda de trayectoria, y su manipulación involucra control en su uso (en algunos modelos) por los gobiernos de cada país a razón de la utilización de un espacio público, tanto en el aspecto físico como en el ámbito espectral; esta tecnología puede no ser compatible o interferir en otras bandas de frecuencia ya asignadas por los organismos gubernamentales [19][20].

En la Fig. 1 se detalla un sistema básico de comunicaciones para la operación de un UAV.

Fig. 1. COMPONENTES BÁSICOS DEL SISTEMA DE COMUNICACIONES



Fuente: Los autores.

3. ASPECTOS LEGALES

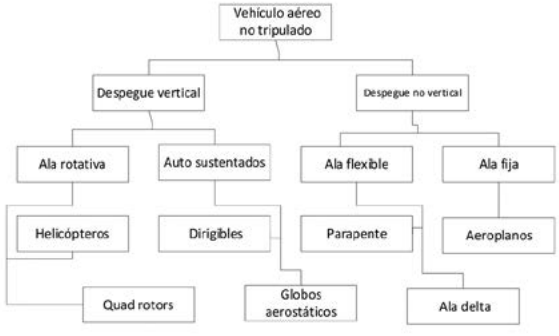
Actualmente, cada país desarrolla su legislación en el pilotaje de drones con el fin de asegurar su manipulación por el impacto que un dispositivo puede causar y por la violación en aspectos de privacidad. En este sentido, cada estado se establece para proteger su existencia, defenderse a sí mismo, proteger a sus ciudadanos y a sus bienes de todo peligro, no obstante, la legislación existente solo considera aeronaves a los elementos capaces de transportar personas o cosas [21] y su uso militar ha incrementado notoriamente en los Estados Unidos (U.S, por sus siglas en inglés) donde se utiliza para la recolección de datos, proveer algunos servicios en cualquier momento, ubicación y otros aspectos relacionados con el ambiente y estrategias de operación [22][23][24].

Dentro de la variedad de aplicaciones que se realizan con estos dispositivos, el autor [25] expone la cantidad de operaciones bélicas y el ataque a personas realizado por drones y por su utilización indiscriminada. No obstante, la armada de los Estados Unidos declara en la Resolución 1540 aspectos que tienen que ver con el uso restringido de los vehículos aéreos no tripulados en cada país, y destaca el debido control que estos dispositivos requieren alrededor del derecho internacional [26] [27] y aunque su uso y regulación se extiende de manera paulatina, hoy forma parte del debate en diferentes países [28][29].

4. SISTEMA DE COMUNICACIONES

Los *UAV* comprenden el despegue vertical y el despegue horizontal, y su sistema de comunicaciones cumple las funciones de monitoreo y control. La función de monitoreo mide el posicionamiento del dron y su sistema básico se constituye como una arquitectura MIMO (múltiple entrada múltiple salida) o una SISO (entrada simple y salida simple). En la Fig. 2, los autores [30] detallan la clasificación de algunos *UAV*.

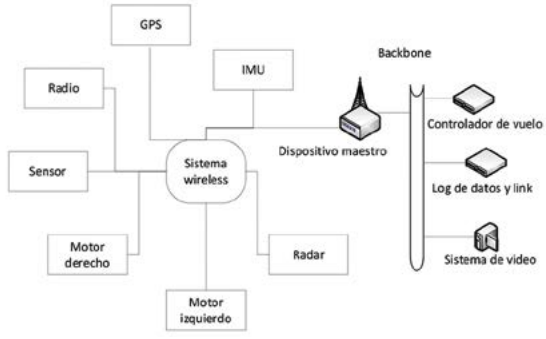
Fig. 2. CLASIFICACIÓN DE ALGUNOS VEHÍCULOS AÉREOS NO TRIPULADOS



Fuente: Los autores.

Algunos *UAV* están compuestos por un sistema clásico de comunicaciones como Wi-Fi, Bluetooth o Zigbee, desde el cual se sensan los dispositivos y se controlan los actuadores; todo esto se hace a través de una interfaz de comunicaciones y un par de antenas que permite la comunicación entre la unidad de control y el *UAV* [31]. Sin embargo, existen diferentes *hardware*, protocolos y sensores que pueden ser combinados para crear diversos sistemas de control soportados con un *software* a la medida. El monitoreo y control, la operación de varios subconjuntos del sistema y la operación de los sensores, combinan aspectos de distancia y tamaño en el sistema de comunicaciones [32][33]. De igual forma, se tienen plataformas que funcionan sobre sistemas móviles [34], redes WiMax, arreglos de antenas sobre Wi-Fi y arquitecturas que se integran a la computación en la nube [35][36][37]. El sistema inalámbrico, generalmente, opera a bajas frecuencias debido a que genera menor consumo y mayor grado de penetración en áreas densas; los controles de los drones suelen operar desde los 30 Mhz hasta los 900 Mhz y el rango de los 2.4 Ghz y 5 Ghz es utilizado por los controles Wi-Fi a través de tabletas o aplicaciones móviles [38]. En la Fig. 3 se ilustra los componentes que conforman la infraestructura general de control y de comunicaciones.

Fig. 3. ARQUITECTURA GENERAL DEL SISTEMA DE COMUNICACIONES



Fuente: Los autores.

4.1 Seguridad en el sistema de comunicaciones

El mayor inconveniente en la operación de los drones es la experticia para funcionar sin la intervención humana y el riesgo que implica la intervención del sistema de comunicaciones por un agente no deseado como el ruido o los ataques al canal [39]. De igual forma, se requieren algoritmos de alta precisión para el pilotaje, la disponibilidad, el mantenimiento y la seguridad [40][41]; estas son condiciones críticas respecto a la operación en ambientes públicos. La tecnología y los algoritmos son fundamentales para el censado y la administración del dispositivo con rutinas de control en tiempo real, adicionalmente, debe ser tolerante a fallas para mitigar los eventos catastróficos, considerando que la operación de un comando por enlace satelital tarda aproximadamente 1, 2 segundos. Aunque los *UAV* cuenten con una topología dinámica y una capacidad variable en los enlaces para el control de congestión y una interrelación entre el *hardware* y el *software* [22][42][43], su operación requiere de condiciones que aseguren el sistema de comunicaciones, aún en el caso de perder el enlace con

el sitio de control, teniendo en cuenta un modelo por capas (Fig. 4) y establecer protección adecuada en cada nivel para el normal funcionamiento [44].

Fig. 4. MODELO POR CAPAS DEL SISTEMA DE COMUNICACIONES

Fuente: Los autores.

El sistema de comunicaciones debe involucrar unos aspectos de aseguramiento que fortalezcan los pilares básicos de la seguridad, como la **integridad** que determina la transmisión sin errores de los datos, la **continuidad** donde no hay interrupción en la comunicación entre dispositivos, **disponibilidad** que mide el porcentaje de tiempo que el sistema está habilitado para la transferencia de datos, una **evaluación** que determine el grado de vulnerabilidad a los ataques intencionales y que alteran la información puesta sobre el medio, la **retransmisión** por ataques y la **confidencialidad** que mide el grado de privacidad de la transferencia de datos entre el dispositivo controlado y el controlador que se enmarca en un sistema en el que se propende por garantizar su funcionalidad [45].

Identificación y valoración de la seguridad en el sistema de comunicaciones

Valorar la seguridad de un sistema de comunicaciones requiere establecer diferentes técnicas [45][28][44], estas se pueden resumir en unos factores que se relacionan dinámicamente entre sí y brindan seguridad al entorno de comunicación, tal como se ilustra en la Fig. 5.

Fig. 5. FACTORES DE SEGURIDAD

Fuente: Los autores.

El robo de datos con fines de lucro es común y obedece generalmente a conflictos laborales, por lo que se recomienda la desactivación de cuentas de usuario [46]. Los controles de acceso establecen autoridad sobre sitios y documentos, de esta parte se han de establecer roles con los diferentes niveles permitidos a cada perfil de usuario. La autenticación identifica la clase de usuario que se loguea o ingresa a un sitio y controla los usuarios no autorizados al área de ingreso. El cifrado fortalece la información para que esta no sea fácilmente identificable por usuarios ajenos al sistema de comunicación [46] y en las redes inalámbricas generalmente no se tiene en cuenta dicho aspecto.

La protección básica de los dispositivos inalámbricos involucra varios aspectos, como: ocultar SSID, el filtrado de direcciones MAC, el cifrado WEP, desactivar DHCP, configurar firewall y establecer un modo de red, la administración remota se debe considerar, utilizar cifrado WPA o WPA2, cambiar la clave de acceso periódicamente; revisar los registros del Router frecuentemente, actualizar el firmware de los dispositivos y, finalmente, realizar pruebas de vulnerabilidad a la propia red [47].

Modelos de seguridad en UAVs

Diferentes modelos se han propuesto en la literatura para fortalecer la seguridad en los vehículos aéreos no tripulados. Los autores [48] proponen un *agent-based self-protective method* (ASP-UAVN) para UAVN que se basa en el *Human Immune System* (HIS). En ASP-UAS, la ruta más segura desde el *UAV* de origen hasta el *UAV* de destino se elige de acuerdo con un sistema de autoprotección. En este método, se emplean agentes múltiples que utilizan un sistema inmunológico artificial (AIS) para detectar el *UAV* atacante y elegir la ruta más segura. En [49] los autores presentan una arquitectura *software* segura basada en *blockchain* para la red de *UAV* utilizando 5G-TI para mitigar los problemas de seguridad; la arquitectura propuesta no solo proporciona seguridad de red y datos, sino que también protege los datos una vez capturados en la cadena de bloques. Otra técnica en [50], plantea un modelo de defensa-ataque basado en árboles para el análisis de seguridad de redes multi-UAV;

en esta, se diseña a *tree-based attack–defense model* que describe cada movimiento del defensor con respecto a las estrategias del atacante, usando este árbol de ataque-defensa se formula un esquema teórico de juego para la evaluación de riesgos. Así mismo, los autores [51] proponen un sistema para garantizar la seguridad y confidencialidad de los datos donde se desarrolla una estructura jerárquica para la distribución de claves y el intercambio de información que garantice la confidencialidad e incremente la seguridad de todo el sistema, la principal característica es proporcionar flexibilidad a la red al permitir que los nodos sirvan como cabezas de clúster de forma periódica y dinámica; los nodos de clúster ordinarios usan *identity-based-encryption* (IBE) para generar confianza y negociar claves con el canal, debido a la naturaleza de recursos limitados del UAV, los nodos utilizan técnicas de cifrado selectivo para la transferencia de mensajes, en lugar de IBE.

Finalmente, los autores [52] presentan un enfoque colaborativo de autonomía humana de geolocalización para ayudar a los sistemas de control de *UAV* a detectar ataques de suplantación de GPS, se diseña un banco de pruebas interactivo y un experimento para evaluar esta técnica; utilizando el Modelo Oculto de Markov (HMM, por sus siglas en inglés), los patrones de comportamiento del operador y las estrategias del experimento se modelaron a través de estados ocultos y transiciones entre ellos revelando dos estrategias dominantes de detección de piratería.

Estos sistemas no han concluido ser una estrategia definitiva en el aseguramiento de la comunicación y por eso, en este trabajo se propone un modelo que permita identificar patrones de comportamiento anormal y que puedan ser el resultado de una intervención o violación del sistema que termine en la desestabilización de este.

5. METODOLOGÍA

5.1 Modelos de fusión de datos en UAV

El desarrollo de modelos en fusión de datos ha surgido con el fin de remediar deficiencias en el diseño de estos sistemas y la ausencia de estándares en general, como: el área de ingeniería, de evaluación de desempeño, paradigmas de arquitecturas, entre otros. Actualmente, la literatura reporta diferentes modelos generalizados clasificados por datos, rol y actividad, los cuales son una guía para el diseño de estos sistemas de fusión de datos/información, siendo algunos más utilizados que otros de acuerdo con sus ventajas y desventajas en aplicaciones específicas. En [53][54][55] se describen algunos modelos de fusión de datos, siendo el más utilizado el modelo JDL el cual se describe a continuación.

Modelo basado en los datos

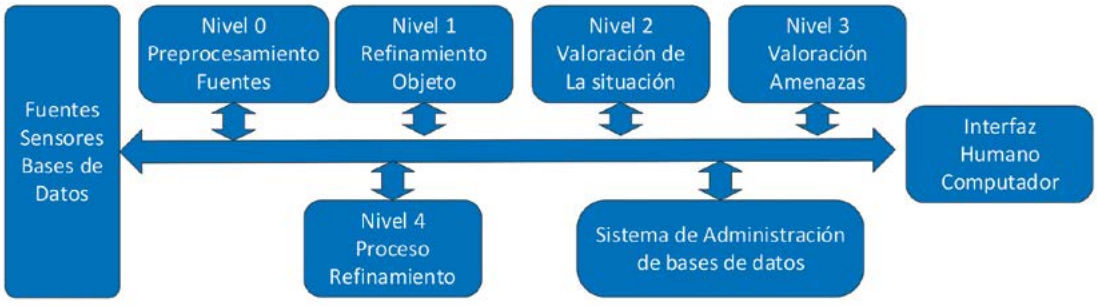
Joint Directors of Laboratories (JDL): este modelo fue propuesto por el autor [56] como un modelo de 4 niveles y posteriormente ajustado a 5 niveles [57][55]. Este es considerado como el modelo más popular, utilizado de guía para el diseño en sistemas de fusión de la información. Este consiste en un bus de datos que conecta 5 niveles de procesamiento como se ilustra en la Fig. 6.

Calidad de la información en las redes

La literatura evidencia que no existe una consistencia en el uso de métricas de calidad en los sistemas de fusión de datos, ya que las métricas utilizadas son elegidas a criterios particulares de los investigadores considerando sus aplicaciones (Tabla I), lo cual hace difícil comparar y reutilizar sistemas y técnicas de fusión de datos.

En [67] se describe un modelo de confiabilidad efectiva (ERM – *Effectiveness realiability model*) para la evaluación de los *IFS* (*Information Fusion System*) que refleja la incertidumbre de las valoraciones cualitativas dadas por expertos que evalúan la efectividad de los *IFS*, basado en la capacidad de la fusión del Target, de la situación y de la toma de decisiones, el cual utiliza el sistema denominado DECR (*Discounting Evidence Combination Rule*) que permite determinar conjuntos de confiabilidad efectiva (valorado en 5 valores discretos y ponderaciones) y entrega la valoración de conflictos.

Fig. 6. MODELO PROPUESTO EN LA ARQUITECTURA JDL



Fuente: Los autores.

Tabla I.
MÉTRICAS DE CALIDAD *WSN*

Autor	Métricas de calidad	Comentario
[58]	Precisión, oportunidad, completitud y relevancia.	*WSN* móvil
	Utiliza un solo parámetro de calidad que es producido por cada sensor basado en un histórico de *outliers* y al estado actual del nodo. Esta medida de la calidad está compuesta del estado de salud del nodo y los descriptores de medida del comportamiento de la señal.	Detección de *outliers*
[59]	Exactitud, completitud, oportuno y consistencia.	Control de juego de pong
	Rendimiento, retardo y tasa de pérdida de paquetes. Caracterización de la *QoS*: Confiabilidad, oportuno, robustez, disponibilidad y seguridad.	Calidad del servicio depende de la aplicación e.g. hay aplicaciones que no admiten retardos en la transmisión de la información.
[60]	Incertidumbre, confiabilidad, completitud, relevancia.	Utiliza la lógica difusa para expresar la ambigüedad de la incertidumbre.
	Exactitud, confiabilidad, rendimiento, costo, oportuno, completitud, relevancia y usabilidad. Detecciones falsas. Acreditadas al ruido y a artefactos.	Orientado a la detección de eventos. Fusión características FCG, ECG y ruido
[61][62]	ROC	EEG
	Exactitud, confidencialidad, relevancia, credibilidad.	Mediador online responsable de garantizar las restricciones
[63][64]	Valor de la información (dependiente del contexto) Calidad de la información (independiente del contexto)	Calidad en las *WSN*
	Métricas de valoración como min, máximos o funciones umbrales y árboles hasta que un único valor es obtenido y las funciones que son aplicadas en los brazos del árbol son seleccionadas por los usuarios.	Linked Data quality assessment and fusion
[65]	Estimación, exactitud, grado de divergencia.	Detección de fallas
	Datos: Consistencia, exactitud, redundancia, copia potencial. Desempeño de la fusión: precisión, eficiencia, diferencia y desviación de la confiabilidad.	Enfoque orientado a la fusión de datos en la WEB
[66]	Relatividad del dominio, independencia, actualidad, completitud, consistencia, redundancia, tamaño del dato, calidad de la página WEB con diferentes métricas. Calidad del servicio: retardo ejecución de la búsqueda, confiabilidad de la fuente de datos, tiempo de respuesta del servidor, evaluación del usuario. Estimación de la calidad usando la distancia de Kendall.	Enfoque orientado a la fusión de datos en la WEB
	Precisión, calidad en tiempo real, estabilidad y confiabilidad del algoritmo.	Método basado en lógica difusa para la evaluación de la calidad de la fusión de la información

Fuente: Los autores.

En [68] [69] ha sido discutido la calidad de la información en los sistemas de fusión de datos, proponiendo un set de criterios de calidad y complementado por una metodología de aplicación sobre bloques funcionales para el modelado de estos a través de los criterios de calidad. Sin embargo, tiene algunas limitaciones como la ausencia de una estrategia que permita establecer un mínimo bloque funcional de una aplicación para poder modelar, a partir de los criterios de calidad y aún no ha sido valorado en múltiples ambientes, como el de los *WSN* y UAV. Por otro lado, el modelado a partir de los criterios de calidad no son utilizados para afectar el sistema, ya que solo es aplicado como estrategia para tener trazabilidad de la calidad de la información que es entregada al usuario final. Para dar solución a algunas de estas limitaciones en este trabajo se propone un *framework* basado en el modelo JDL y la calidad de la información, con enfoque a los sistemas UAV.

5.2 Modelo propuesto de fusión de datos

La Fig. 7 muestra el *framework* propuesto, el cual presenta los criterios para la valoración de la calidad de la información y el desempeño enmarcado en cada uno de los niveles del modelo JDL. Nosotros tomamos como referencia para este ambiente el trabajo de mapeo del modelo JDL en ciber-defensa realizado por [70] y [71]. Cada nivel tiene una funcionalidad y la calidad de la información se evalúa por un conjunto de criterios a partir de métricas de calidad que dependen de la disponibilidad de la medida. A

continuación se describe la funcionalidad de cada uno de los niveles:

- Nivel 0 se encarga del pre-procesamiento de la información captada por los diferentes sensores del dron, tales como imágenes, geolocalización por GPS, alarmas, además de múltiples medidas de los sistemas de comunicación capturadas por sensores de flujo de red, las cuales son valoradas por medio de diferentes métricas, como: niveles de S/N, número de pings, consistencia de los comandos, completitud de la información, ajustes en la configuración, bps, redundancia, *outliers*, completitud, tráfico, localización física, sistema operativo, lista de parches aplicados (*software* de nivel de aplicación instalado), utilización de la CPU y la memoria, aplicaciones en ejecución, datos de acceso a la cuenta del usuario final, datos de registro de seguridad, clasificación de los datos almacenados en el sistema. Intrusión (tipo y ubicación del IDS, dirección de origen, dirección de destino, método de ataque, momento del ataque). Atacante (dirección (es) de origen). Flujos de datos (direcciones de origen y destino, tipo de tráfico (protocolos utilizados), volumen de tráfico, cifrado utilizado) (Fig. 7).

- Nivel 1: se encarga de la detección de eventos, lo cual permite identificar targets de seguridad, como: estabilidad en la navegación del dron, estimación de posición, identificación del dron, identificación de obstáculos, identificación de intrusiones, métodos y objetivos de ataque.

- Nivel 2: describe la situación del dron en términos de seguridad, considerando relaciones de los objetos identificados en el nivel 1 y el contexto. Particularmente, permite determinar capacidad del atacante frente a capacidad defensiva. Adicionalmente, se define el estado del dron frente a los ataques y todos sus controles.

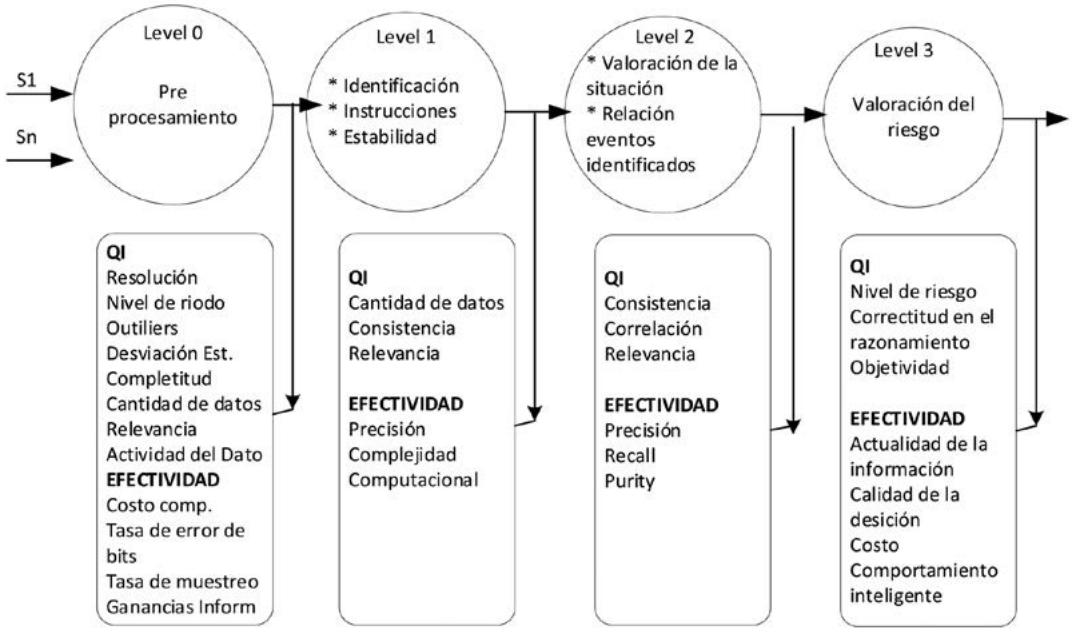
- Nivel 3: en este se valora el nivel del riesgo y el impacto frente a la situación establecida en el nivel 2. Se hacen predicciones futuras que permiten al usuario final establecer qué acciones ejecutar para conservar la seguridad del entorno y del dron, basado en vulnerabilidades, oportunidades del atacante y acciones futuras del atacante junto con los posibles daños.

- Nivel 4: se realiza el refinamiento del proceso, en este caso se lleva a cabo seleccionando fuentes de datos, ajustando parámetros libres de los algoritmos de procesamiento, detección y predicción, basado en las medidas de calidad de la información local y global propuestas en este trabajo.

- Nivel 5: en este nivel el experto humano interpreta la información entregada por el sistema y puede hacer ajustes en el proceso.

En la siguiente sección se muestra el desarrollo de esta propuesta usando sistemas de inferencia difusos para los niveles 0, 1, 2, 3 y la calidad de la información.

Fig. 7. MODELO PROPUESTO



Fuente: Los autores.

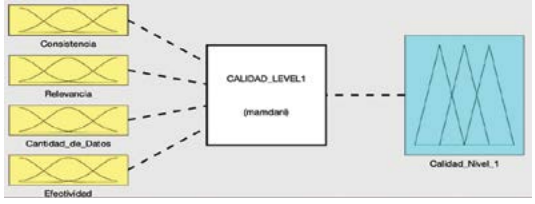
La calidad de la información es establecida por criterios asociados a sus respectivas métricas. Para cada nivel son propuestos un set de criterios de calidad de la información. Los criterios del nivel 2 y 3 están basados en la seguridad del dron considerando la funcionalidad de estos niveles respecto a la valoración de la situación y el riesgo a través de relaciones entre los eventos identificados. Las métricas de estos niveles se consideran de alto nivel y se pueden llevar a cabo por medio de mediciones directas, así como también aplicando cuestionarios o preguntas claves a los operadores para su medición mediante un sistema experto. Los criterios de calidad son establecidos a partir de las métricas de calidad que se encuentran de acuerdo con el contexto. El alcance de este trabajo ejemplifica sólo los criterios de calidad.

El modelo propuesto consta de la valoración de la calidad de la información por nivel, global y las salidas obtenidas de cada nivel. Las salidas del nivel 2 y 3 son obtenidas usando relaciones de variables de seguridad usando reglas en el motor de inferencia de los FIS. De igual forma la valoración de la calidad de la información fue realizada usando FIS y las reglas establecidas relacionando los criterios de calidad de entrada para valorar la calidad local.

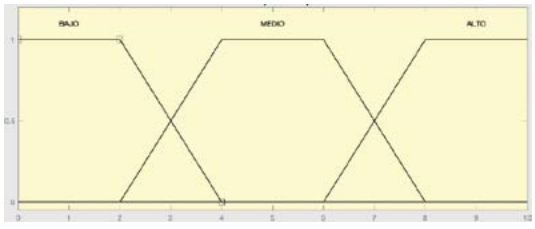
5.3 Valoración de la calidad de la información

Se construyó un FIS (*IFS*) como el que se muestra en la Fig. 8 (a) para la valoración de la calidad de la información en cada nivel del modelo (i.e. valoración local), relacionando los criterios de calidad que se muestran en la Tabla II. Los conjuntos difusos establecidos para cada criterio obedecen a la estructura mostrada en la Fig. 8 (b), la cual consta de tres conjuntos difusos trapezoidales con rango entre 0 y 10. La valoración global se lleva a cabo usando la misma estructura de las valoraciones locales, pero usando como entradas los resultados entregados en la valoración de la calidad de la información de cada nivel como se muestra en la Fig. 9.

Fig. 8. VALORACIÓN DE LA CALIDAD DE LA INFORMACIÓN POR NIVEL



a. FIS CALIDAD DE LA INFORMACIÓN ESTRUCTURA NIVEL 1.



b. ESTRUCTURA CONJUNTOS DIFUSOS.

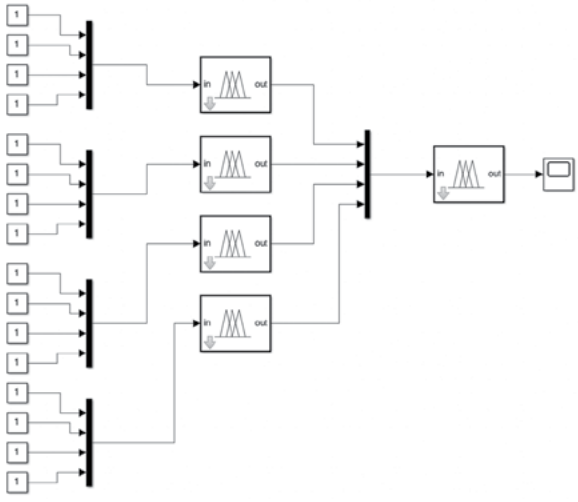
Fuente: Los autores.

Tabla II.
CRITERIOS DE CALIDAD DE LA INFORMACIÓN POR NIVEL

Nivel 0	Nivel 1	Nivel 2	Nivel 3
Resolución	Consistencia	Correctitud razonamiento	Correctitud razonamiento
Outliers	Relevancia	Objetividad	Objetividad
Completitud	Cantidad de datos	Efectividad	Efectividad
Cantidad de datos	Efectividad	Correlación	
Efectividad			

Fuente: Los autores.

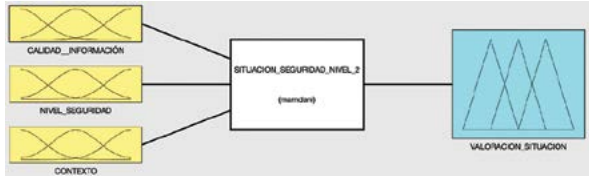
Fig. 9. VALORACIÓN GLOBAL DE LA CALIDAD DE LA INFORMACIÓN



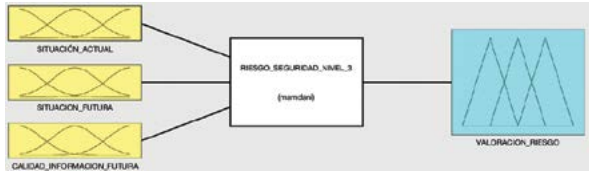
Fuente: Los autores.

De forma similar es realizada la valoración de la situación y la valoración del riesgo como se ilustra en la Fig. 10.

Fig. 10. VALORACIÓN DE LA SITUACIÓN Y EL RIESGO



a. VALORACIÓN DE LA SITUACIÓN



b. VALORACIÓN DEL RIESGO

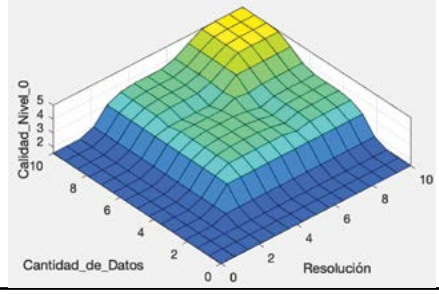
Fuente: Los autores.

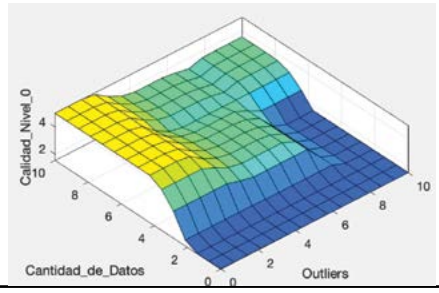
IITECKNE Vol. 18 Número 2 • ISSN 1692-1798 • ISSN Digital 2339 - 3483 • diciembre 2021 • 108 - 120

6. RESULTADOS

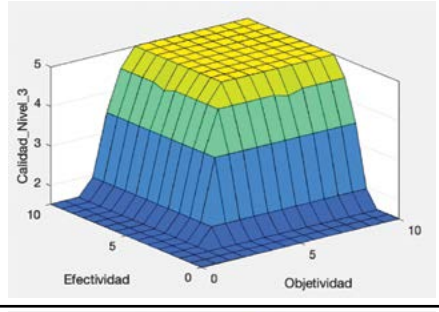
Los resultados entregados por los FIS son expresados por medio de diagramas de superficie, los cuales dan cuenta de la coherencia entre las reglas establecidas entre las variables de entradas para valorar su salida. En la Fig. 11 se muestran algunas de las combinaciones de los criterios de calidad utilizados en cada nivel 0 y 3. Como se puede observar al incrementar cualquiera de los criterios el valor de la calidad mejora a excepción con los *outliers* que estos al incrementar decrementan la calidad.

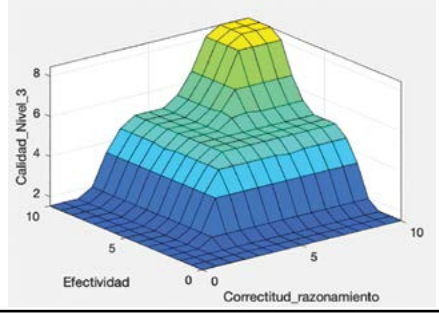
Fig. 11. DIAGRAMAS DE SUPERFICIE NIVEL 0 Y 3





NIVEL 0



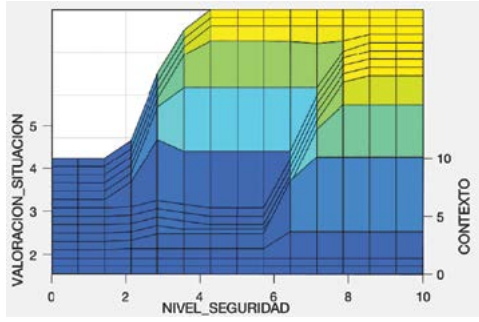


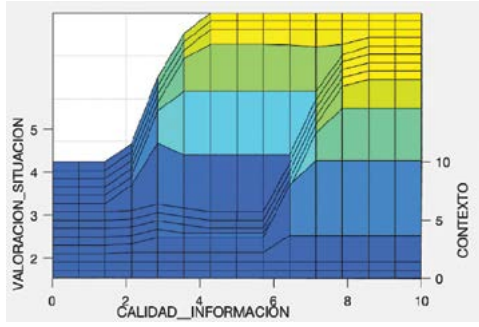
NIVEL 3

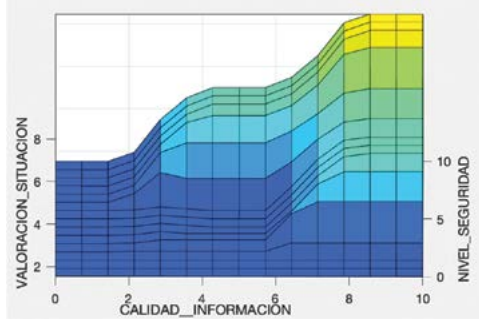
Fuente: Los autores.

En las Figs. 12 y 13 se muestran los diagramas de superficie que relacionan las variables de entrada para la valoración de la situación y la valoración del riesgo respectivamente. En estas gráficas se observa un comportamiento coherente, donde al incrementarse los valores de las variables de entrada, se incrementa el valor de salida de manera consistente para valorar la seguridad del dron. La valoración del riesgo es establecida considerando la valoración de la situación, la calidad de la información futura y la valoración de la situación futura. Estos valores pueden ser establecidos usando máquinas de aprendizaje. El alcance de este trabajo cubre las relaciones que se realizarían con los resultados entregados por estos sistemas. En resumen, se observa que todos los diagramas son coherentes y demuestran su funcionalidad en términos de las inferencias entregadas por los sistemas difusos.

Fig. 12. DIAGRAMAS DE SUPERFICIE VALORACIÓN DE LA SITUACIÓN

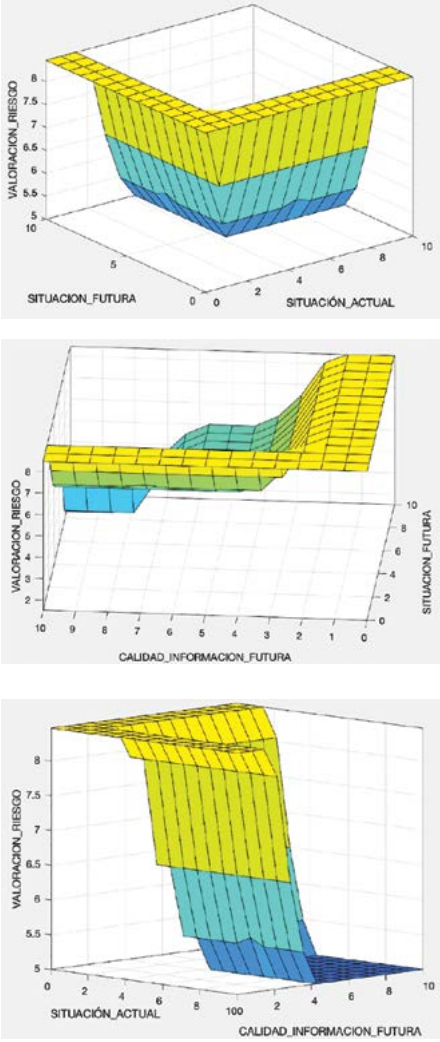






Fuente: Los autores.

Fig. 13. DIAGRAMAS DE SUPERFICIE VALORACIÓN DEL RIESGO



Fuente: Los autores.

7. DISCUSIÓN Y CONCLUSIONES

En este artículo hemos propuesto un modelo de valoración de la seguridad de los drones basado en criterios funcionales y la calidad de la información. El modelo propuesto cuenta con 6 niveles funcionales y sistema de valoración de la calidad de la información local y globalmente. Este *framework* propuesto es un proceso de 6 pasos: en el nivel 0 se hace el pre-procesamiento de la información captada por los diferentes sensores del UAV; para el nivel 1 y 2, se encarga de la detección de eventos, como la estabilidad y la posición; en el nivel 3 se valora el riesgo y el impacto basado en la relación de la situación actual, la situación futura y la calidad de la información futura; en el nivel 4 se realiza el refinamiento ajustando parámetros a los algoritmos planteados; por último, en el nivel 5 se encuentra el experto humano, quien interpreta las datos y puede hacer ajustes adicionales al sistema. El nivel 6 corresponde al sistema de valoración de la calidad de la información.

El modelo propuesto demuestra su funcionalidad basada en los criterios queridos para la construcción de las relaciones, lo cual puede considerarse una mejora a la seguridad reduciendo el nivel de riesgo. Este método permite identificar el momento en que los delincuentes informáticos puedan interceptar mensajes o involucrarse en el sistema de comunicación. Así mismo, se reducen de forma considerable las posibilidades de que alguien llegara a comprometer la integridad y confidencialidad de los dispositivos sin ser detectado por el modelo.

La propuesta de fusión de datos enmarcada en el modelo JDL fue realizada para la valoración de la seguridad en los sistemas de navegación no tripulada. Esta permite identificar puntos críticos en los sistemas de comunicaciones de los UAV, y establece criterios de medición de la calidad de la información basada en perspectivas del usuario. Este modelo construido puede ser utilizado en las múltiples aplicaciones de los drones, con el fin de sostener una mejor seguridad y control de estos sistemas. Como trabajo futuro se puede valorar el sistema en ambientes de prueba con diferentes tipos de dron y en grupos.

8. REFERENCIAS

[1] A. Rosenfeld and O. Maksimov, "Optimal cruiser-drone traffic enforcement under energy limitation," *Artif. Intell.*, vol. 277, p. 103166, 2019, DOI: https://doi.org/10.1016/j.artint.2019.103166

[2] X. Zhu, T. J. Pasch, and A. Bergstrom, "Understanding the structure of risk belief systems concerning drone delivery: A network analysis," *Technol. Soc.*, vol. 62, no. April, p. 101262, 2020, DOI: https://doi.org/10.1016/j.techsoc.2020.101262

[3] R. Nouacer, M. Hussein, H. Espinoza, Y. Ouhammou, M. Ladeira, and R. Castiñeira, "Towards a *framework* of key technologies for drones," *Microprocess. Microsyst.*, vol. 77, 2020, DOI: https://doi.org/10.1016/j.micpro.2020.103142

[4] H. Wang, X. Liao, T. Huang, and G. Chen, "Distributed parameter estimation in unreliable *WSN*s: Quantized communication and asynchronous intermittent observation," *Inf. Sci. (Ny).*, vol. 309, pp. 11–25, 2015, DOI: https://doi.org/10.1016/j.ins.2015.03.007

[5] X. Wu and H. Zhu, "Formal analysis of a calculus for *WSN*s from quality perspective," *Sci. Comput. Program.*, vol. 154, pp. 134–153, 2018, DOI: https://doi.org/10.1016/j.scico.2017.08.007

[6] C. Zhang, O. Li, Y. Yang, G. Liu, and X. Tong, "Energy-efficient data gathering algorithm relying on compressive sensing in lossy *WSN*s," *Meas. J. Int. Meas. Confed.*, vol. 147, 2019, DOI: https://doi.org/10.1016/j.measurement.2019.106875

[7] M. M. Fouad, N. E. Oweis, T. Gaber, M. Ahmed, and V. Snasel, "Data Mining and Fusion Techniques for *WSN*s as a Source of the Big Data," *Procedia Comput. Sci.*, vol. 65, no. Iccmit, pp. 778–786, 2015, DOI: https://doi.org/10.1016/j.procs.2015.09.023

[8] X. E. Pantazi, D. Moshou, and D. Bochtis, "Utilization of multisensors and data fusion in precision agriculture," in *Intelligent Data Mining and Fusion Systems in Agriculture*, Elsevier, 2020, pp. 103–173

[9] A. Coen-Porisini and S. Sicari, "Improving data quality using a cross layer protocol in wireless sensor networks," *Comput. Networks,* vol. 56, no. 17, pp. 3655–3665, 2012, DOI: https://doi.org/10.1016/j.comnet.2012.08.001

[10] A. R. Pinto, C. Montez, G. Araújo, F. Vasques, and P. Portugal, "An approach to implement data fusion techniques in wireless sensor networks using genetic machine learning algorithms," *Inf. Fusion*, vol. 15, pp. 90–101, Jan. 2014, DOI: https://doi.org/10.1016/j.inffus.2013.05.003

[11] D. Wang, J. Liu, and D. Yao, "An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks," *Comput. Networks*, vol. 178, no. March, 2020, DOI: https://doi.org/10.1016/j.comnet.2020.107313

[12] S. Qu, L. Zhao, Y. Chen, and W. Mao, "A discrete-time sliding mode congestion controller for wireless sensor networks," *Optik (Stuttg).,* vol. 225, no. July 2020, p. 165727, 2021, DOI: https://doi.org/10.1016/j.ijleo.2020.165727

[13] S. S. Marouf, M. C. Bell, P. S. Goodman, J. Neasham, J. Neasham, and A. K. Namdeo, "Comprehensive study of the response of inexpensive low energy wireless sensors for traffic noise monitoring," *Appl. Acoust.,* vol. 169, p. 107451, 2020, DOI: https://doi.org/10.1016/j.apacoust.2020.107451

[14] M. Jalil Piran *et al.,* "Multimedia communication over cognitive radio networks from *QoS*/QoE perspective: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 172. Academic Press, Dec. 15, 2020, DOI: https://doi.org/10.1016/j.jnca.2020.102759

[15] T. Murugeswari and S. Rathi, "Priority and interference aware multipath routing based communications for extreme surveillance systems," *Comput. Commun.*, vol. 150, pp. 537–546, Jan. 2020, DOI: https://doi.org/10.1016/j.comcom.2019.11.050

[16] M. Faheem and V. C. Gungor, "MQRP: Mobile sinks-based *QoS*-aware data gathering protocol for wireless sensor networks-based smart grid applications in the context of industry 4.0-based on internet of things," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 358–374, May 2018, DOI: https://doi.org/10.1016/j.future.2017.10.009

[17] W. Rehan, S. Fischer, and M. Rehan, "Anatomizing the robustness of multichannel MAC protocols for *WSN*s: An evaluation under MAC oriented design issues impacting *QoS*," *Journal of Network and Computer Applications,* vol. 121. Academic Press, pp. 89–118, Nov. 01, 2018, DOI: https://doi.org/10.1016/j.jnca.2018.06.013

[18] N. Sharma, B. M. Singh, and K. Singh, "*QoS*-Based Energy-Efficient Protocols for Wireless Sensor Network," *Sustain. Comput. Informatics Syst.*, p. 100425, Aug. 2020, DOI: https://doi.org/10.1016/j.suscom.2020.100425

[19] M. Huttunen, "Civil unmanned aircraft systems and security: The European approach," *J. Transp. Secur.,* vol. 12, no. 3–4, pp. 83–101, Dec. 2019, DOI: https://doi.org/10.1007/s12198-019-00203-0

[20] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Physical Syst.*, vol. 1, no. 2, p. 7, 2017, DOI: https://doi.org/10.1145/3001836

[21] S. S. Wu, "Product Liability Issues in the U.S. and Associated Risk Management," in *Autonomes Fahren*, Springer Berlin Heidelberg, 2015, pp. 575–592.

[22] T. Rakha and A. Gorodetsky, "Review of Unmanned Aerial System (UAS) applications in the built environment: Towards automated building inspection procedures using drones," *Automation in Construction,* vol. 93. Elsevier B.V., pp. 252–264, Sep. 01, 2018, DOI: https://doi.org/10.1016/j.autcon.2018.05.002

[23] J. Nelson and T. Gorichanaz, "Trust as an ethical value in emerging technology governance: The case of drone regulation," *Technol. Soc.*, vol. 59, Nov. 2019, DOI: https://doi.org/10.1016/j.techsoc.2019.04.007

[24] R. Luppicini and A. So, "A technoethical review of commercial drone use in the context of governance, ethics, and privacy," *Technol. Soc.,* vol. 46, pp. 109–119, Aug. 2016, DOI: https://doi.org/10.1016/j.techsoc.2016.03.003

[25] K. Hartmann and C. Steup, "The Vulnerability of UAVs to Cyber Attacks-An Approach to the Risk Assessment," 2013.

[26] R. Merkert and J. Bushell, "Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control," *J. Air Transp. Manag.*, vol. 89, Oct. 2020, DOI: 10.1016/j.jairtraman.2020.101929

[27] S. Ings, "The power of drones," *New Sci.*, vol. 248, no. 3302, p. 33, Oct. 2020, DOI: https://doi.org/10.1016/s0262-4079(20)31756-5

[28] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, Sep. 2020, DOI: https://doi.org/10.1016/j.iot.2020.100218

[29] Z. Lv, "The security of Internet of drones," *Comput. Commun.*, vol. 148, pp. 208–214, Dec. 2019, DOI: https://doi.org/10.1016/j.comcom.2019.09.018

[30] A. Barrientos, J. Del Cerro, P. Gutiérrez, R. San Martín, A. Martínez, and C. Rossi, "Vehículos aéreos no tripulados para uso civil. Tecnología y aplicaciones," *Grup. Robótica y Cibernética, Univ. Politécnica Madrid*, pp. 1–29, 2009, Accessed: Nov. 13, 2020. [Online]. Available: https://www.academia.edu/24038031/Vehículos_aéreos_no_tripulados_para_uso_civil_Tecnología_y_aplicaciones.

[31] T. Malatinec, V. Popelka, M. Huba, and P. Hudačko, "Laboratory model helicopter control using a lowcost Arduino *hardware*," in *Proceedings of the 2014 15th International Carpathian Control Conference, ICCC 2014*, 2014, pp. 326–331, DOI: https://doi.org/10.1109/CarpathianCC.2014.6843621

[32] A. I. Khan and Y. Al-Mulla, "Unmanned aerial vehicle in the machine learning environment," in *Procedia Computer Science,* 2019, vol. 160, pp. 46–53, DOI: https://doi.org/10.1016/j.procs.2019.09.442

[33] F. Outay, H. A. Mengash, and M. Adnan, "Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: Recent advances and challenges," *Transp. Res. Part A Policy Pract.*, vol. 141, pp. 116–129, Nov. 2020, DOI: https://doi.org/10.1016/j.tra.2020.09.018

[34] F. H. Tseng, T. T. Liang, C. H. Lee, L. Der Chou, and H. C. Chao, "A star search algorithm for civil *UAV* path planning with 3G communication," in *Proceedings - 2014 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2014*, Dec. 2014, pp. 942–945, DOI: https://doi.org/10.1109/IIH-MSP.2014.236

[35] S. Mahmoud and N. Mohamed, "Broker architecture for collaborative UAVs cloud computing," in *2015 International Conference on Collaboration Technologies and Systems, CTS 2015*, Aug. 2015, pp. 212–219, DOI: https://doi.org/10.1109/CTS.2015.7210423

[36] J. Chen, J. Wang, K. F. Tong, and A. A. Allann, "A GPS/Wi-Fi dual-band arc-shaped slot patch antenna for *UAV* application," in *2013 Loughborough Antennas and Propagation Conference, LAPC 2013,* 2013, pp. 490–493, DOI: https://doi.org/10.1109/LAPC.2013.6711948

[37] "A triple band arc-shaped slot patch antenna for *UAV* GPS/Wi-Fi applications - IEEE Conference Publication." https://ieeexplore.ieee.org/document/6717462 (accessed Nov. 13, 2020).

[38] J. B. Hill, "Unmanned aerial systems," in *AUVSI Unmanned Systems 2015,* 2015, pp. 119–139, DOI: https://doi.org/10.2307/j.ctv7cjw3j.29

[39] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques," *Ad Hoc Networks*, p. 102324, Oct. 2020, DOI: 10.1016/j.adhoc.2020.102324

[40] M. Rieke, T. Foerster, J. Geipel, and T. Prinz, "HIGH-PRECISION POSITIONING AND REAL-TIME DATA PROCESSING OF UAV-SYSTEMS," *ISPRS - Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. XXXVIII-1/, pp. 119–124, Sep. 2012, DOI: https://doi.org/10.5194/isprsarchives-xxxviii-1-c22-119-2011

[41] X. Song, S. Liao, X. Wang, C. Lu, M. Wang, and C. Miao, "A High Precision Autonomous Navigation Algorithm of *UAV* Based on MEMS Sensor," in *Proceedings of the 2019 IEEE International Conference on Unmanned Systems, ICUS 2019*, Oct. 2019, pp. 904–908, DOI: https://doi.org/10.1109/ICUS48101.2019.8996061

[42] X. Wang, Q. Zhou, and C. T. Cheng, "A UAV-assisted topology-aware data aggregation protocol in *WSN*," *Phys. Commun.*, vol. 34, pp. 48–57, Jun. 2019, DOI: https://doi.org/10.1016/j.phycom.2019.01.012

[43] D. Zhang and H. Duan, "Switching topology approach for *UAV* formation based on binary-tree network," *J. Franklin Inst.*, vol. 356, no. 2, pp. 835–859, Jan. 2019, DOI: https://doi.org/10.1016/j.jfranklin.2017.11.026

[44] Q. L. Han, L. Ding, and X. Ge, "Special issue on recent advances in security and privacy-preserving techniques of distributed networked systems," *Information Sciences*, vol. 545. Elsevier Inc., pp. 277–279, Feb. 04, 2021, DOI: https://doi.org/10.1016/j.ins.2020.08.014

[45] "Network Security Bible, 2nd Edition Wiley." https://www.wiley.com/en-co/Network+Security+Bible,+2nd+Edition-p-9780470570005 (accessed Nov. 13, 2020).

[46] B. Z. He, C. M. Chen, Y. P. Su, and H. M. Sun, "A defence scheme against Identity Theft Attack based on multiple social networks," *Expert Syst. Appl.*, vol. 41, no. 5, pp. 2345–2352, Apr. 2014, DOI: https://doi.org/10.1016/j.eswa.2013.09.032

[47] A. Orebaugh and B. Pinkard, "Nmap OS Fingerprinting," in *Nmap in the Enterprise*, Elsevier, 2008, pp. 161–183.

[48] R. Fotohi, E. Nazemi, and F. Shams Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, p. 100267, 2020, DOI: https://doi.org/10.1016/j.vehcom.2020.100267

[49] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of *blockchain*-enabled softwarization for secure *UAV* network," *Comput. Commun.*, vol. 161, no. May, pp. 304–323, 2020, DOI: https://doi.org/10.1016/j.comcom.2020.07.042

[50] S. Garg, "Tree-Based Attack – Defense Model for Risk Assessment in Multi-*UAV* Networks," no. December 2019, pp. 35–41.

[51] S. Haque, *Security and Privacy in Communication Networks - SecureComm 2017 International Workshops, {ATCS} and SePrIoT, Niagara Falls, ON, Canada, October 22-25, 2017, Proceedings*, vol. 239. Springer International Publishing, 2018.

[52] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and M. Pajic, "Operator Strategy Model Development in *UAV* Hacking Detection," *IEEE Trans. Human-Machine Syst.*, vol. 49, no. 6, pp. 540–549, 2019, DOI: https://doi.org/10.1109/THMS.2018.2888578

[53] S. Rodríguez, J. F. De Paz, G. Villarrubia, C. Zato, J. Bajo, and J. M. Corchado, "Multi-agent information fusion system to manage data from a *WSN* in a residential home," *Inf. Fusion*, vol. 23, pp. 43–57, 2015, DOI: https://doi.org/10.1016/j.inffus.2014.03.003

[54] M. M. Fouad, N. E. Oweis, T. Gaber, M. Ahmed, and V. Snasel, "Data Mining and Fusion Techniques for *WSN*s as a Source of the Big Data," in *Procedia Computer Science*, 2015, vol. 65, pp. 778–786, DOI: https://doi.org/10.1016/j.procs.2015.09.023

[55] M. M. Almasri and K. M. Elleithy, "Data fusion models in *WSN*s: Comparison and analysis," 2014, DOI: 10.1109/ASEEZone1.2014.6820642

[56] C. Haas, "A model for data fusion in civil engineering," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 4200 LNAI, pp. 315–319, DOI: https://doi.org/10.1007/11888598_29

[57] "(PDF) Revisions and extensions to the JDL data fusion model II." https://www.researchgate.net/publication/306535574_Revisions_and_extensions_to_the_JDL_data_fusion_model_II (accessed Nov. 13, 2020).

[58] E. C. H. Ngai and P. Gunningberg, "Quality-of-information-aware data collection for mobile sensor networks," *Pervasive Mob. Comput.*, vol. 11, pp. 203–215, 2014, DOI: https://doi.org/10.1016/j.pmcj.2013.07.012

[59] O. Kreibich, J. Neuzil, and R. Smid, "Quality-based multiple-sensor fusion in an industrial wireless sensor network for MCM," *IEEE Trans. Ind. Electron.*, vol. 61, no. 9, pp. 4903–4911, 2014, DOI: https://doi.org/10.1109/TIE.2013.2293710

[60] F. Hermans, N. Dziengel, and J. Schiller, "Quality estimation based data fusion in wireless sensor networks," in *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS '09*, 2009, pp. 1068–1070, DOI: 10.1109/MOBHOC.2009.5337006

[61] D. Izadi, J. Abawajy, and S. Ghanavati, "Quality control of sensor network data," in *Lecture Notes in Electrical Engineering*, 2011, vol. 122 LNEE, pp. 467–480, DOI: https://doi.org/10.1007/978-3-642-25553-3_58

[62] D. I. Curiac, "Towards wireless sensor, actuator and robot networks: Conceptual *framework*, challenges and perspectives," *Journal of Network and Computer Applications*, vol. 63. Academic Press, pp. 14–23, Mar. 01, 2016, DOI: https://doi.org/10.1016/j.jnca.2016.01.013

[63] E. J. Wright and K. B. Laskey, "Credibility models for multi-source fusion," 2006, DOI: 10.1109/ICIF.2006.301693

[64] X. Zhao, Y. Jia, A. Li, R. Jiang, and Y. Song, "Multi-source knowledge fusion: a survey," *World Wide Web*, vol. 23, no. 4, pp. 2567–2592, Jul. 2020, DOI: https://doi.org/10.1007/s11280-020-00811-0

[65] C. Bisdikian, "On sensor sampling and quality of information: A starting point," in *Proceedings - Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2007*, 2007, pp. 279–284, DOI: https://doi.org/10.1109/PERCOMW.2007.88

[66] "Hard and soft computing methods for capturing and processing phonocardiogram | Request PDF." https://www.researchgate.net/publication/287289778_Hard_and_soft_computing_methods_for_capturing_and_processing_phonocardiogram (accessed Nov. 13, 2020).

[67] Y. Feng, W. Biyao, and W. Jun, "Effectiveness evaluation of information fusion system oriented to Fusion ability," in *Proceedings - 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer, MEC 2013*, 2013, pp. 1399–1403, DOI: https://doi.org/10.1109/MEC.2013.6885286

[68] G. L. Rogova, "Information Quality in Information Fusion and Decision Making with Applications to Crisis Management," in *Fusion Methodologies in Crisis Management,* G. Rogova and P. Scott, Eds. Cham: Springer International Publishing, 2016, pp. 65–86.

[69] I. G. Todoran, L. Lecornu, A. Khenchaf, and J. M. Le Caillec, "A methodology to evaluate important dimensions of information quality in systems," *J. Data Inf. Qual.,* vol. 6, no. 2, 2015, DOI: https://doi.org/10.1145/2744205

[70] S. Schreiber-Ehle and W. Koch, "The JDL model of data fusion applied to cyber-defence — A review paper," in *2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications (SDF)*, Sep. 2012, no. September 2012, pp. 116–119, DOI: https://doi.org/10.1109/SDF.2012.6327919

[71] N. A. Giacobe, "Application of the JDL data fusion process model for cyber security," in *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2010*, Apr. 2010, vol. 7710, p. 77100R, DOI: https://doi.org/10.1117/12.850275