# A SECURE COMMUNICATION FRAMEWORK FOR LARGE-SCALE UNMANNED AIRCRAFT SYSTEMS

*Jiang Bian, Division of Biomedical Informatics, University of Arkansas for Medical Sciences Little Rock, AR, 72205*
*Remzi Seker, Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114*
*Mengjun Xie, Computer Science, University of Arkansas, Little Rock, AR 72204*

## Abstract

The application areas for Unmanned Aircraft (UA) Systems (UAS) are constantly expanding. Aside from providing an attractive alternative in applications that are risky for humans, smaller UAS become highly attractive for applications where use of larger aircraft is not practical. This paper presents the UAS Collaboration Wireless Network (UAS-CWN), a secure and reliable UAS communication mesh-network. This solution is proposed for the circumstances where a large number of UAS are deployed to cooperatively accomplish a mission such as surveillance in hostile environments. The proposed UAS-CWN system provides high fault-tolerance through use of information dispersal algorithm and meanwhile reduces the risk of information exposure to the adversaries via security-enhancing mechanisms. Our evaluation shows promising results. Especially, a UAS-CWN with high security-level settings can withstand losing 30% of the total number of unmaned aircrafts while steadily achieving above 96% data recovery rate.

## I. Introduction

Unmanned Aircraft Systems (UAS) can be used in hostile environments for various missions including surveillance and intelligence gathering. Rapid industry advancements in power and electric motor technologies, as well as impressive improvements in applied artificial intelligence research will soon enable the mass production of small-sized, low-cost, and fully/semi-automated UAS and their applications in carrying out complex and long-term missions in hostile environments. However, using hundreds even thousands of UAS effectively at once introduces unique data dissemination challenges.

Imagine a large number of fully automated drones are deployed to collect intelligence in a hostile territory such as a battlefield. The available satellite uplink bandwidth, which usually is less than 10Mbps, limits the number of drones that can communicate with the base station. Therefore, it is challenging to transmit the gathered information to the base station in real time. A strategy is to store the information locally on each drone during its mission, and collect all the information when the drones are back. However, it is very likely that a number of drones are destroyed during the mission either by accident or by adversaries. Furthermore, the security of the information collected by the drones need to be assured such that when the drones are captured, the adversaries shall not be able to extract any sensitive information.

Following our previous work on anti-tampering wireless sensor networks [1, 2], in this paper, we introduce the UAS Collaboration Wireless Network (UAS-CWN), a secure and reliable UAS communication mesh network. The proposed protocol is well suited for deploying a large number of drones simultaneously to conduct surveillance missions in hostile environments. Through the UAS-CWN system, unmanned aircrafts work cooperatively to achieve high fault-tolerance, while minimizing the risk of information exposure to adversaries.

The rest of the paper is organized into five sections. Section 2 briefly describes our motivations and overviews the proposed UAS-CWN system. In Section 3, we present the threat model of the UAS-CWN formulated from security concerns related to Wireless Sensor Networks (WSNs) and the security issues raised specific to the UAS environment. We will detail the design of the UAS-CWN system in Section 4 and discuss how potential threats identified in the threat models can be addressed. In Section 5, we use a generative network model to simulate a UAS-CWN, and propose to use complex network analysis techniques to study the characteristics of UAS-CWNs. We conclude our work with the

978-1-4673-6253-5/13/$31.00 ©2013 IEEE

importance of developing a UAS-CWN like system for UAS security in Section 6.

## II. The UAS Collaboration Wireless Network

### *A. Motivation*

Unmanned aircraft systems have been widely used for targeted surveillance and military operations in adverse environments. Adverse environments are not restricted to those in the military-context only. Using unmanned aircrafts in extreme weather conditions, such as having them fly into large storms in order to collect data for modeling and prediction purposes is another example of deploying UAS in adverse environments. The advancements made in technologies for powering UAS such as solar-powered UAS with battery reserves may allow the UAS to carry long-term surveillance missions [3, 4]. Moreover, the recent surge of research on air-vehicle autonomy [5] has drawn increasing amount of interest due to its military applications. UAS are shifting from simple remotely piloted aircrafts to fully autonomous and self-controlled aircrafts [6, 7]. Combining these factors, it is not hard to imagine an explosion in large-scale UAS missions involving hundreds if not thousands fully automated UAS [8]. However, an individual UA is vulnerable to hardware failures, software malfunctions, as well as other threats be it environmental or originating from the adversaries. Therefore, given the potential opportunities of large-scale UAS deployment, it is reasonable to formulate cooperative tactics to maximize the chance of success for a given mission.

Wireless Sensor Network (WSN), due to its resource constrained nature, is an emerging technology where a collection of nodes organized into a cooperative communication and collaboration network [9]. Applications of WSNs include surveillance in military battlefields and applications for homeland security [10-13]. A typical WSN contains multiple sensors (nodes) and a base station. The sensors monitor the environmental data such as temperature, sound, pressure, and motion, while the base station either collects and fuses local data and then transmits it to a predefined location or simply relay the data for further processing. Every node in the WSN can be either stationary or mobile. The nodes, aside from processing the information locally (if tasked to do so), can also serve as intermediary hops which relay the information in the network. Due to this routing capability, the information gathered by sensing nodes eventually reaches the base station, which does not have the same resource constraints on computational and communication resources. The integration of automated UAS to form a wireless sensor network is straightforward, where the drones carry sensor equipments as well as communication facilities via which they can exchange information with each other. This can be achieved by equipping an UA with a wireless mesh node [14]. A large number of drones can then form a swarm and carry out the mission in a collaborative manner.

Faults, including those originating from hardware and software, are inevitable. The probability of failure becomes much higher when a UA operates in a hostile environment. Moreover, wireless communications are through radio waves in open air and adversaries may intercept the signals and deduce sensitive information. Interference from the adversaries is another threat during the operation of UAS. Therefore, the communication and information dissemination systems utilized in UAS swarms shall be hardened to not only achieve high-level fault tolerance but also withstand adversarial attacks.

### *B. An Overview of the UAS Collaboration Wireless Network*

In this paper, we propose a conceptual design of secure UAS Collaboration Wireless Networks (UAS-CWNs). Figure 1 shows an overview of a UAS-CWN system. In a UAS-CWN, each drone is considered as a node in the collaboration network. When a piece of intelligence is acquired by a drone, the information will be split into $n$ slices using an Information Dispersal Algorithm (IDA) [15]. These $n$ slices of the gathered information will then be delivered to $n$ nearest neighbors. These data segments can be further propagated (depending on the required security-level parameter set) in the network by their receivers (other drones in the network). In other words, the UAS-CWN exhibits mesh networking topology, where each node not only captures and disseminates its own data, but also serves as a relay for other nodes. The $n$ value and the level of propagation (security-level) shall be set based on redundancy and security needed for the mission. When the drones return the base station, an operator can easily reconstruct the gathered data using the

corresponding IDA decoder. Due to various reasons (e.g., some drones may be lost during the mission, or communication device failure, etc.), not all $n$ data slices may be available. However, IDA ensures that the original data can be restored as long as there are $k$ ($k << n$) complete data slices. In order to secure the data, i.e., the gathered intelligence/information, we use one-way hash key-chain. In UAS-CWN, a pair of private ($x_i$) and public ($g^{x_i}$) keys is generated and deployed onto each drone before the mission. The private key is known to the operator and the specific drone on which it resides. The public key for a drone is known to all other drones. When a piece of intelligence is gathered, the drone first encrypts the data using symmetric encryption algorithm with $h(x_i)$ as the encryption key. The drone then applies the IDA encoding to split the encrypted data into $n$ slices. Before sending each data slice to nearby UAS, the data packet is signed digitally with the drone's private key to ensure integrity and authenticity. In addition to these message slices, the drone will also send the next-level encryption key $h(h(x_i))$ to the relay nodes (also drones). The same process will repeat on the receiving nodes before the message is propagated further. These, first-step nodes will use $h(h(x_i))$ as a key for encrypting the received message slices. The encryption key $h(h(x_i))$ was obtained from the sender at the time the message slice was received. The properties of one-way cryptographic hash function ensures us that: 1) no two message slices will have the same hash value; and 2) it is impractical to deduce $x_i$ from $h(x_i)$. Using one-way hash key-chain, we separate the data from its encryption key and ensure that only the originator will be able to decrypt the data stored in the mesh network formed by the drones.

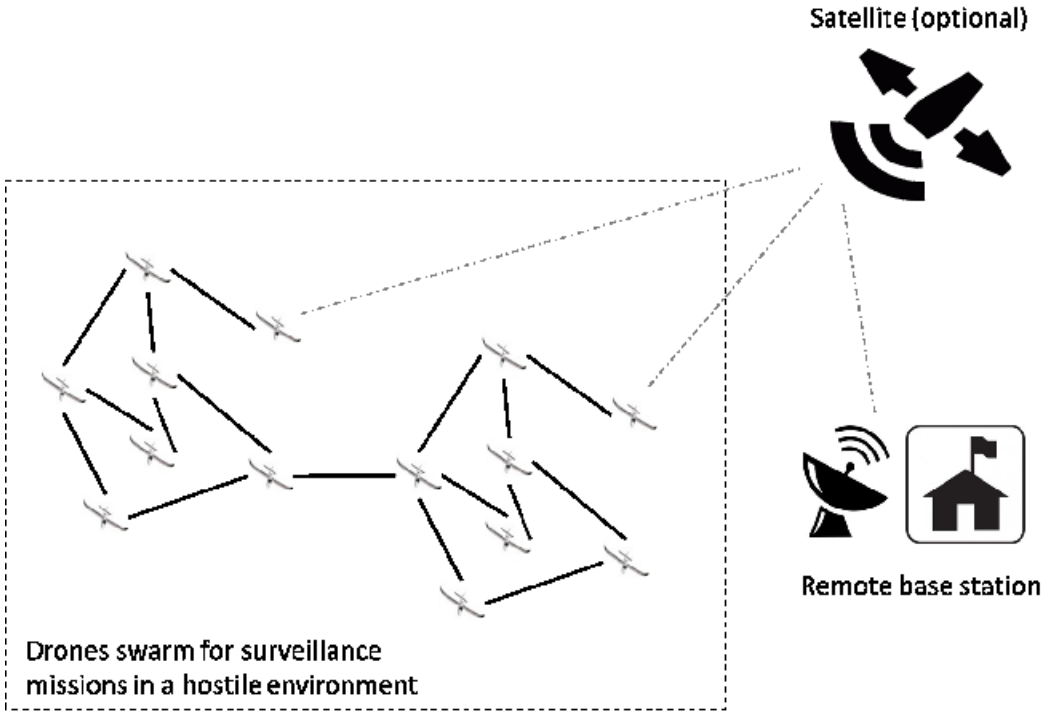


**Figure 1. Overall Architecture of UAS-CWN**

Wireless signals are also prone to jamming. The UAS-CWN has an Active Status Polling (ASP) mechanism to address the scenario where the communications are disrupted. Each drone in the UAS-CWN will actively query its neighbors' security status and if no response or a false response is received, the querying node will report an abnormal event for the queried drone and set a flag for the operator. This flag will warn the operator that the information stored on the potentially compromised UA needs to be treated with caution. Authentication in ASP communications is crucial in order to prevent man-in-the-middle attacks. Section 4 discusses the ASP and man-in-the-middle attacks in details.

### *C. Operational Assumptions and System Design Goals*

The main goals of UAS-CWNs are to provide a certain level of fault tolerance for recovering the gathered information and to protect the data collected by UAS during the mission. Each UA is assumed to be equipped with necessary sensors (e.g., camera), a radio transceiver for communicating with other drones, an energy source (e.g., a battery or an embedded form of energy harvesting device like solar panels), and may or may not have a satellite communication module. Even if a UA is capable of communicating with the base station through a satellite link, such communication channel may not be available, as the mission may be carried out in an environment where satellite communication is not feasible. Therefore, UAS still need to have a mechanism of securely storing and disseminating the collected data before the data can be transferred to the base station. Because of the unique characteristics of UAS-CWNs and the hostile deployment environment, design considerations need to include a variety of factors including the wireless coverage area, battery life, ability to cope with node failures, ability to withstand harsh environmental conditions, and communication failures.

As the focus of this paper is the design of a cooperative communication and information dissemination network, the design issues related to the hardware on UAS, such as power and storage capacity, wireless communication range, etc., are out of the scope of this paper. However, the ability to cope with node and/or communication failures, due to either software or hardware faults, is addressed in the UAS-CWN design, since the availability of the system is a key aspect of its security assurance.

The availability of a satellite communication channel on each UA is not critical to the design of a UAS-CWN. Due to the nature of surveillance missions, we shall assume that satellite communication may only be available periodically. The design of the UAS-CWN with satellite-enabled UAS is straightforward. When the satellite connection is available, the UAS will send the collected information to the base station, and offload its storage burden. However, the communications between UAS as well as those between a UA and the base station shall still be protected and fault-tolerant since the adversaries can capture these communications and the satellite communication channels can fail. Therefore, our design of the UAS-CWN shall be self-sustainable without presence of any real-time external communication link.

The UAS-CWN utilizes the mesh networking topology. The mesh connectivity established among sensor nodes is flexible for deployment and robust to network faults and link failures. Blind spots in communication can be eliminated by adding or adjusting power levels of the mesh nodes/routers (UAS). We assume that the implementation of the mesh networking is sufficient in propagating data among nodes in the network. There is a large body of research on routing protocols that can efficiently disseminate data within a mesh network. Surveys of recent advancements on this topic can be found in [16, 17]. Hence, we do not consider the failures of low-level transmission of individual data packets. However, we do consider communication failure at a higher abstraction level, where not all $n$ data segments produced by the IDA can be successfully transmitted to other nodes.

## III. Security Assumptions and Threat Models

To develop the threat models, the threats the system may be subjected to are first identified and then ranked with respect to the associated risk. The threats that are identified to be viable are then addressed with specific elimination or alleviation measures in the system design. Threat modeling should also specify the assumptions made regarding the system under consideration. We make a set of assumptions for the UAS-CWN considering the nature of its applications. We assume that modifications to the internal settings of the sensing equipments and to the information processing components within each UA during the mission cannot go undetected. Therefore, it is reasonable to assume that if a UA is captured, the adversaries may be able to tamper with it. However, the adversaries may not recover the encryption key stored on the UA (e.g., self-destruction of the encryption key in response to tampering). Since all UAS are launched from a remote base station, a security check of the components inside each UA can be performed such that any compromised UAS shall be detected and removed from the UAS-CWN before departure. Thus, pre-planned insider attack is not

possible (e.g., an attacker may not learn any of the encryption keys used by UAS in the network).

Wireless communications among the UAS in the UAS-CWN face a broad spectrum of threats, including eavesdropping, spoofing, impersonation, and denial-of-service (DOS) attacks [18-20]. The UAS-CWN system is designed to protect the gathered information and shield it from unauthorized access or modification as well as blockage. Any of these attacks may be attempted by adversaries. A thorough understanding of the potential threats to the UAS-CWN system will help us develop corresponding threat mitigation strategies. The presented threat model is developed using the STRIDE (i.e. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) method described in [21-23]. Table 1 lists potential threats discovered during the initial design and implementation of the UAS-CWN system.

**Table 1. Threat Models and General Countermeasures**

| # | Threat | Categories | Countermeasures |
|---|---|---|---|
| 1) | Without proper protection, an attacker can impersonate a compromised UA node to eavesdrop on the communications passing through the node, send false response messages to other UAS queries. | *spoofing* | strong *authentication* and/or *digital signatures* applied to the data |
| 2) | An attacker may have the ability to capture a number of UAS and gather information (e.g., segments of intelligence and other nodes' status updates) from these nodes. | *spoofing* + *information disclosure* | strong *authentication* and *encryption* of the data |
| 3) | An attacker may have the ability to intercept the communications among sensor nodes and the information in transit may be altered, spoofed, replayed again, or vanished. | *information disclosure* + *tampering* | cryptographic *hash functions* for integrity checks and/or *encryption* of the data |
| 4) | An attacker may have the ability to gain necessary privilege to modify the data stored on compromised UAS (e.g., change the status from "compromised" to "normal"). | *elevation of privilege* + *tampering* | *encryption* of the data |
| 5) | An attacker may use a drone to promptly report bogus intrusion events as false alerts to cause distraction, while denying having made such reporting. | *spoofing* + *repudiation* | strong *authentication* and identification of traffic |
| 6) | An attacker can jam wireless signals or perform other types of denial-of-service (DoS) attacks against the system. | *denial-of-service* | strong *authentication* and incident detection and reporting mechanisms |
| 7) | An attacker can be an insider and perform a sybil attack, where a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of the fault-tolerant scheme. | *spoofing* + *denial-of-service* | strong authentication |

### *A. Implementing Security Services in Wireless Sensor Networks*

Along with the identified threats, Table 1 also lists the general countermeasures, which can be employed to address these security threats. The countermeasures include use of authentication to thwart adversaries' attempts of joining the network, use of encryption algorithms to ensure the confidentiality of the communications and gathered data, use of digital signatures for the authenticity of the information, and use of cryptographic hash functions to ensure the integrity of transmitted data packets.

The sensor nodes in traditional WSNs are resource limited. The resource limitation poses challenges for using strong encryption and authentication at each individual sensor node. However, secure peer-to-peer communication is necessary for many applications. Traditional public-key algorithms and pairwise key agreement strategies are considered computationally intensive for embedded systems [24]. However, recent

developments in the field of WSNs suggest use of public-key infrastructure as a viable option for dynamic key generation and distribution [25]. Some implementations of public-key infrastructure for sensor networks rely on pre-distribution of keys [26, 27]. For example, SPINS [28] contains two sets of protocols: SNEP for data confidentiality, two-way data authentication, and data freshness; and $\mu$TESLA for providing efficient broadcast authentication. However, the SPINS system assumes existence of a base station to act as a gateway for all the other sensor nodes. This gateway is also the single point of failure for the whole system. Some other key management related research in WSN include [29] and [30]. The UAS-CWN design adopts the idea of key pre-distribution due to the fact that all UAS are launched from a base station, where the pre-generated key pairs can be distributed to each UA during a maintenance phase prior to launch for the mission.

Symmetric encryption algorithms and cryptographic hash functions are relatively computationally cheaper and faster [24] compared to the public key infrastructure-based solutions. In [31] and [32], a one-way hash key chain is used to ensure the authenticity of the packets broadcast from the base station. First, the base station uses a one-way function $h()$ to generate a sequence of keys $k_0$, $k_1$,...,$k_n$, such that $k_i = h(k_{i+1})$. $k_0$ and hash function $h()$ are pre-distributed to every node. In the first broadcast round, the base station use $k_1$ to sign its packet, and the child nodes can verify the signature by comparing $h(k_1)$ with the known $k_0$. Since $h()$ is a one-way hash function, it is impracticable for an adversary to compute $k_{i+1}$ from $k_i$. This way the authenticity is ensured, since the base station is the only entity who knows $k_{i+1}$ at the $i$th round of communication. Moreover, even if a node is compromised by an attacker, $k_i$ is not used in the next round of communication and hence, it is useless. The challenge in this scheme is that the base station may need to compute a long sequence of keys for pre-distribution. For missions that are of long durations and/or many rounds of communication are needed, the computation of the key chain will increase the setup time. Our UAS-CWN design takes a different perspective: the goal of using the one-way hash key chain is to separate the data from the encryption key, rather than authenticating the communications between nodes.

# IV. Design of the UAS Collaboration Wireless Network and Threat-Mitigation

## *A. Information Dispersal Algorithm in UAS-CWN*

This section details how the Information Dispersal Algorithm (IDA), introduced by Michael O. Rabin [15], is utilized in the proposed UAS-CWN system. When a piece of information is acquired by a UA, the information $m$ is first encrypted by a key ($k_x$) derived from the UA's private key ($x$, and see Section 4.2 for the distribution of private key) using a one-way cryptographic hash function ($h()$) (i.e., $k_x = h(x)$). This operation produces the encrypted message $c = enc_{h(x)}(m)$, which is then split into $n$ (this parameter is set prior to the mission) slices using an IDA and delivered to the $n$ nearest neighbors along with the Message Identifier (MID), and Node Identifier (NID). The receiving nodes can choose to propagate the segment further depending on the required confidentiality level or store the data segment locally [2]. In case a UA is required to propagate the received data segment ($c = enc_{h(x)}(m)$) further, it will first encrypt $c$ using the key $h(y)$ received from its private key ($y$), and generate a new encrypted data segment ($c = enc_{h(y)}(enc_{h(x)}(m))$). Then this node will apply the IDA again and deliver the new slices to its $n$ nearest neighbors. The more encryption layers and IDA processes, the more resources (i.e., computing units, storage, and time) a UA will require. However, the assumption here is that the more important a mission (e.g. a critical military surveillance mission), the stronger encryption will be needed. The actual implementation of such layered encryption and recursive IDA approach has been demonstrated in [6]. For the sake of simplicity and clarity, we continue our discussion based on a 1-layer example.

When the drones return to the base station, an investigator can easily reconstruct the information gathered by them using the corresponding IDA decoder. Since the message slices are transmitted through wireless communications, some of the message slices may be corrupted due to various reasons. For instance, a receiving UA may have experienced a device failure during transmission; the transmitted data packets may be lost due to weak

wireless signal, etc. In addition, some message slices may be missing simply because some drones were lost during the mission. However, the original message can still be restored as long as there are $k$ (based on the setting of the IDA) UAS still holding the message slices. For example, as illustrated in Figure 2, let us assume that $n$ is 10 and $k$ is $three$. The probability that all 10 nearby UAS have failed to receive a message or all of them have been compromised by an attacker at the same time is negligible. As long as at least $three$ UAS survive the failure or attack they underwent during the mission, we can reconstruct the original information (i.e., gathered intelligence).

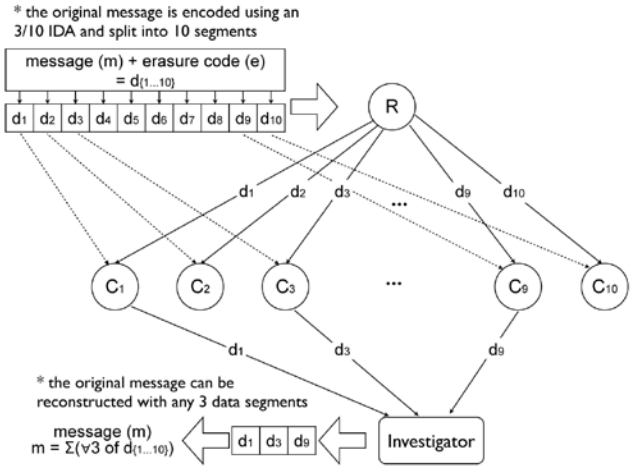


**Figure 2. Split and Reconstruct a Message in the UAS-CWN Using an Information Dispersal Algorithm**

The IDA [15] was introduced to design fault-tolerant and transmission efficient information storage systems. The IDA is a special deployment of *erasure codes*, which are also referred to as *forward error correction* (FEC) codes. The most commonly known erasure code is the one employed in the implementation of RAID level-5 systems. The basic idea of erasure codes is to generate and deploy redundant data for error correction, in addition to the original data before transmission or storage. This extra information allows the receiver or reader to detect and correct data errors without having to ask the sender to resend the message.

It is legitimate to raise the question of sending out the original messages $n$ times to $n$ different nodes instead of employing the IDA. This would eliminate the reconstruction phase associated with use of IDA. It also may be the case that one can add more resources into a UA node. However, it is necessary for communication messages among the UAS to be short in order to increase the probability of successful delivery of messages. According to the IDA encoding, splitting the original message into $n$ segments and adding the redundancy bits result in messages that are smaller than the original. With message sizes being small, the chance of successful delivery of messages increases when the communication channel is unstable or under attack. If we assume that a large number of UAS will be launched for the mission and hence be part of the UAS-CWN, smaller message sizes will improve the overall efficiency of operation of the UAS-CWN. Employing the IDA in the UAS-CWN also serves the purpose of obfuscating the operation of the individual UAS as part of the system. Since the communications in the UAS-CWN are carried through wireless signals, the communications can easily be intercepted or interfered by the adversaries. Open radio waves are suitable for an adversary to perform man-in-the-middle attacks when preventative measures such as encryption and authentication are not utilized. If the messages are in plain text, an attacker may block warning messages, which are issued when there is something wrong in the system and replace the warning messages with a message that indicates normal operation. An attacker may also choose to alter the content of messages to provide the system with wrong intelligence. However, when an IDA is employed, the resulting message slices are not necessarily meaningful to an attacker and any modification made to message slices during their transmission will be detected by the IDA decoder as these modified slices would fail in the validation test performed by the IDA decoder.

The UAS-CWN system proposed in this paper particularly targets UAS with constrained resources. As the software implementation of IDA is often computationally expensive, the software implementation of IDA may not be suitable for the UAS-CWN. However, there are many cost-effective hardware IDA implementations and these solutions can easily be adopted for the UAS in the UAS-CWN.

### *B. Active Status Polling*

Let us consider a scenario in which a UA has been isolated by an attacker from rest of the UAS-CWN system. The proposed system must be resilient enough to detect absence of activity from the isolated UA. Therefore, in the proposed UAS-CWN

system, UAS not only disseminate the intelligence they gather, but also actively query/update each other on their status. If a UA does not respond to the status polling message issued by another UA in the UAS-CWN, it is highly likely that the polled UA is either captured or facing some technical difficulties. The polling UA will raise a warning event associated with the polled UA and report the event. This technique makes sure that the potential intrusions can be quickly identified and do not go undetected, even if the attacker is able to block the communications of a victim UA.

The UAS-CWN is designed to employ threat mitigation measures in order to minimize the chance of the attacks against the system. However, in case an attack is successful, the messages reporting such an attack needs to be delivered with a high probability of success. For the sake of simplicity, the response from the polled node does not use the IDA encoding as the response is only for the polling node. Using the techniques typically employed in peer-to-peer communications while utilizing appropriate encryption and authentication would be sufficient. In general, public key-based crypto-systems are not suitable for use in resource-constrained devices due to the fact that such algorithms are compute intensive. However, Watro et al. have developed a lightweight public key-based security system called TinyPK [34] to be used in wireless sensor networks. The UAS-CWN proposed in this paper uses TinyPK. In UAS-CWN, for each UA, a public/private key pair is generated. The private key is known to the operator and specific UA on which it will reside. The public key, on the other hand, is known to all other nodes in the UAS-CWN. The encryption keys will be deployed to the UAS at the base station before the launch for the mission.

A digital signature is necessary to ensure the integrity and authenticity of the data. The digital signature for a UA is computed using the same private key deployed on it. Let us assume that UA $C_i$ is going to send a message $m^{i\rightarrow j}$ to UA $C_{j\neq i}$. Let $x_i$ and $g^{x_i}$ be the private and public keys of $C_i$, respectively. Let $sign()$ denote the signing function, $enc()$ the encryption function, and $h()$ a cryptographic hash function. Before sending the message $m_{(i\rightarrow\cdot)}$, UA $C_i$ uses $h()$ to compute the hash value for $m_{(i\rightarrow\cdot)}$. UA $C_i$ then signs the message by encrypting the computed hash value with its private key $x_i$ using the signing function $S()$:

$$S_{m_{i\rightarrow\cdot}} = sign(h(m_{i\rightarrow\cdot})).$$

Then, UA $C_i$ sends the whole packet $P_{(i\rightarrow j)}$ to UA $C_{j\neq i}$. The packet $P_{(i\rightarrow j)}$ contains the message $m_{(i\rightarrow j)}$ as well as the signature $S_{(i\rightarrow j)}$ associated with the message. The packet has the following format:

$$P_{(i\rightarrow j)} = [m_{(i\rightarrow j)}, S_{(i\rightarrow j)}].$$

When UA $C_j$ receives $P_{(i\rightarrow j)}$, it can check the integrity and authenticity of the message by verifying the attached signature $S_{(i\rightarrow j)}$, as UA $C_j$ knows UA $C_i$'s public key $g^{x_i}$.

If an attacker tries to respond to a status poll by impersonating another UA, the attacker's response will not be valid as the private key for the UA being impersonated is not known to the attacker. Applying a digital signature to messages ensures the integrity of the messages.

# V. Evaluation

As robust data dissemination and fault tolerance is one of the main goals of UAS-CWN, in this section, we focus on evaluating UAS-CWN in terms of data recovery rate through simulations. Since the interactions of the UAS within a UAS-CWN are highly dynamic, the underlying mesh networking topology is highly mobile and difficult to define. Therefore, we adopt the generative Erdös-Rényi random graph model [12] to simulate the possible communication channels (links) among UAS (nodes) within a UAS-CWN. In the Erdös-Rényi model ( $G = (m, p)$ ), a graph ( $G$ ) with $m$ nodes is constructed by linking nodes at random with independent probability ( $p$ ). Figure 3 shows an example of the simulated interaction network within a UAS-CWN.

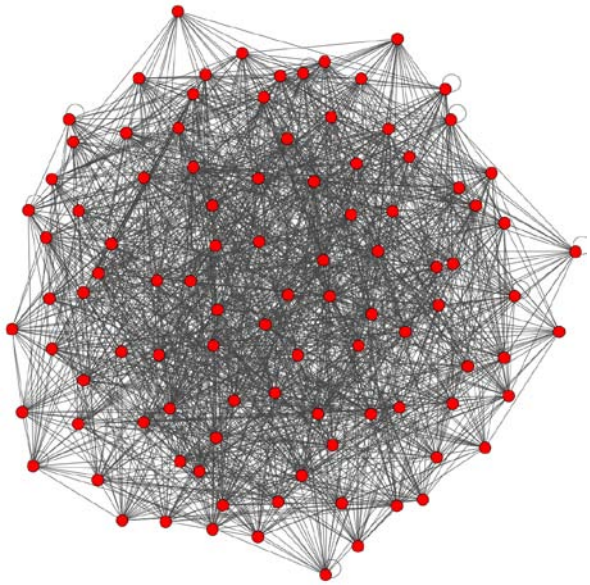

**Figure 3. A Simulated Interaction Network of a UAS-CWN (i.e., $100$ UAS)**

To evaluate the data recovery rate, in each simulation experiment, we consider a number of failure points in the data dissemination process. The communication failure is modeled as the data segments fail to transfer between UAS with probability $p_c$. The loss of drones (i.e., either being captured by an adversary or hardware failures that cause the stored data segments irretrievable) is modeled with a destroy rate ($d$). The general steps for our simulation setup are described as follows:

1) Set the size of the modeled UAS network as ($m$), simulate the interactions using the Erdös-Rényi model ($G = (m, p)$), and set the following initial variables:

- Communication failure rate: $fc$
- Required security-level: $sl$
- IDA parameters: $k/n$

2) Consider $t$ time steps where at each time step $m \times e$ ($e$ is the data emission rate) UAS will emit the collected intelligence to its neighbors;

(a) For each UA that emits a data segment, it will randomly choose $n$ (i.e., using an $k/n$ IDA encoder, and if the node has less than $n$ neighbors, it will evenly distribute the $n$ slices to all its neighbors) neighbors defined by the interaction network ($G$), and send data slices to these neighbors with a failure rate of $fc$;

(b) The receiver nodes will further propagate the received data segment to its $n$ neighbors until reaches the required security-level ($sl$).

3) After the data dissemination process, we reconstruct the original data assuming that only $1 - d$ percent of drones (i.e., randomly choose $n \times (1 - d)$ nodes in the network) have survived the mission.

4) We compute the data recovery rate ($r$) as the fraction of the number of recovered data sets over the total number of data sets that were originally emitted during the dissemination process.

We have evaluated a number of scenarios through varying different parameters of the system. Here, we present a few key findings. As can be seen in Figure 4, the performance of the proposed UAS-CWN design does not vary with the number of UAS deployed in the network. The data recovery rate is almost constant with small UA failure rates and only decreases slightly (but still $r > 0.94$) when the failure rate exceeds $0.2$.

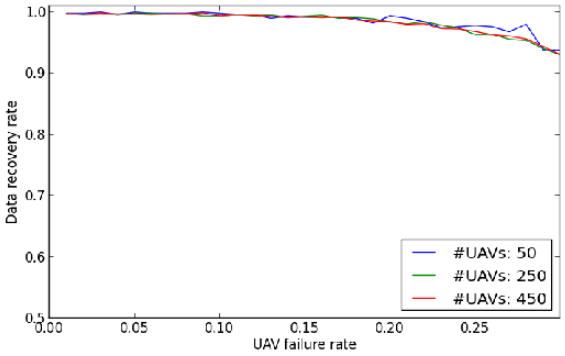


**Figure 4. The Relation Between the Data Recovery Rate ($r$) and the UA Failure Rate ($d$) with Different Network Sizes (Parameter Setting: $k/n = 3/5, sl = 2, fc = 0.1, t = 100, and e = 0.05$).**

We also observe that a UAS-CWN system with a higher security-level ($sl$) configuration outperforms the systems with low $sl$ values, as shown in Figure 5. Moreover, when the UA failure rate increases, a UAS-CWN with $sl = 3$ still has stable performance with $r > 0.96$, while its performance with $sl = 1$ deteriorates and drops below $0.85$ quickly.

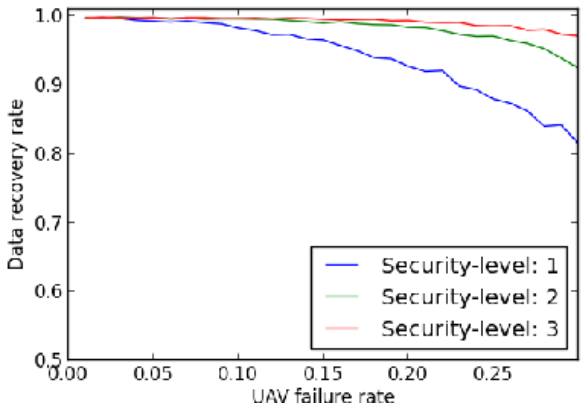


**Figure 5. The Relation Between the Data Recovery Rate ($r$) and the UA Failure Rate ($d$) with Different Security-Level Settings (Parameter Setting: $n = 500, k/n = 3/5, fc = 0.1, t = 100, ande = 0.05$).**

We have also compared the data recovery rate of the UAS-CWN design using different IDA settings (i.e., $k/n$), and compared the use of IDA with a simple mirroring scheme for data redundancy. As shown in Figure 6, the $2/5$ and $3/7$ IDA settings provide reasonable performance compared with other IDA configurations and the simple mirroring scheme. The $3/5$ IDA scheme has only $0.67$ redundancy and a relatively low data recovery rate when the UA failure rate increases even compared to the simple mirroring scheme. However, on the other hand, the $3/5$ IDA scheme only has $67\%$ storage overhead, while the mirroring has $100\%$ overhead. Furthermore, the $3/5$ IDA scheme still outperforms the mirroring scheme when the UA failure rate is below $0.14$. Last but not least, a $3/5$ IDA distributes the storage load onto $5$ different nodes, while in the mirroring scheme, two nodes bear a heavy burden of the required redundancy.

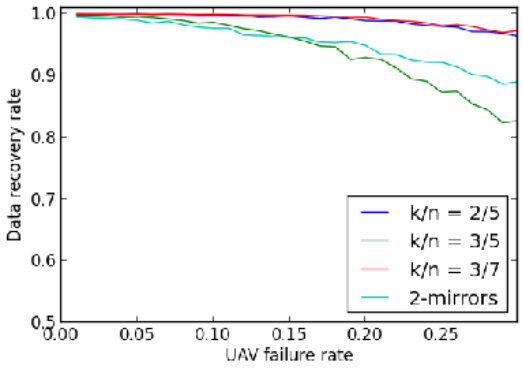


**Figure 6. The Data Recovery Rate ($r$) under Different IDA Settings and Its Comparison to a Simple Mirroring Scheme with Respect to the UA Failure Rate ($d$) (Parameter Setting: $n = 500, sl = 1, fc = 0.1, t = 100, ande = 0.05$).**

## VI. Conclusion

This paper presented the UAS-CWN, a secure, fault tolerant, and collaborative network of UAS. The system is fault tolerant and addresses the threats identified through the STRIDE threat modeling methodology. The simulations conducted for evaluating the UAS-CWN design provides promising results. Especially, a UAS-CWN configured with a higher security-level can perform reliably above $0.95$ even with significant UA failure rates (e.g., $0.3$). Moreover, the high performance of the proposed UAS-CWN design is consistent across different sizes of the network. Such properties make the UAS-CWN well suited for carrying out large-scale missions in adverse environments.

## References

[1] Abolhasan, M. and Hagelstein, B. and Wang, J. C -P. Real-World Performance of Current Proactive Multi-Hop Mesh Protocols. *Communications, 2009. APCC 2009. 15th Asia-Pacific Conference on*, pages 44-47, 2009.

[2] Agogino, Adrian and HolmesParker, Chris and Tumer, Kagan. Evolving Large Scale UAV Communication System. *Proceedings of the Fourteenth International Conference on Genetic and Evolutionary Computation Conference* in GECCO '12, pages 1023–1030, New York, NY, USA, 2012. ACM.

[3] I. F. Akyildiz and W. Su and Y. Sankarasubramaniam and E. Cayirci. Wireless

Sensor Networks: a Survey. *Comput. Netw.*, 38(4):393–422, 2002.

[4] Bian, J. and Seker, R. and Ramaswamy, S. JigDFS for Implementing Secure Container Communities. *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pages 3651-3656, 2009.

[5] Bian, J. and Seker, R. and Ramaswamy, S. and Yilmazer, N. Container Communities: Anti-Tampering Wireless Sensor Network for Global Cargo Security. *Control and Automation, 2009. MED '09. 17th Mediterranean Conference on*, pages 464-468, 2009.

[6] Bian, Jiang and Seker, Remzi. Jigdfs: a Secure Distributed File System. *Computational Intelligence in Cyber Security, 2009. CICS'09. IEEE Symposium on*, Pages 76–82, 2009. IEEE.

[7] Krishnendu Chakrabarty and S. Sitharama Iyengar and Hairong Qi and Eungchun Cho. Grid Coverage for Surveillance and Target Location in Distributed Sensor Networks. *IEEE Trans. Comput.*, 51(12):1448–1453, 2002.

[8] Hai Chen and Xin-Min Wang and Yan Li. a Survey of Autonomous Control for UAV. *Artificial Intelligence and Computational Intelligence, 2009. AICI '09. International Conference on*, Pages 267-271, 2009.

[9] Jing Deng and Richard Han and Shivakant Mishra. a Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. *in the 23rd IEEE International Conference on Distributed Computing Systems (IPSN 2003)*, Pages 349–364, 2003.

[10] Deng, Jing and Han, Richard and Mishra, Shivakant. INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks. *Computer Communications*, 29(2):216–230, 2006.

[11] Wenliang Du and Jing Deng and Yunghsiang S. Han and Pramod K. Varshney and Jonathan Katz and Aram Khalili. a Pairwise Key Predistribution Scheme for Wireless Sensor Networks. *ACM Trans. Inf. Syst. Secur.*, 8(2):228–258, 2005.

[12] Erd6s, Paul. on the Evolution of Random Graphs. *Publ. Math. Inst. Hungar. Acad. Sci*, 5:17–61, 1960.

[13] Laurent Eschenauer and Virgil D. Gligor. a Key-Management Scheme for Distributed Sensor Networks. *CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security*, Pages 41–47, New York, NY, USA, 2002. ACM.

[14] Chao Gui and Prasant Mohapatra. Power Conservation and Quality of Surveillance in Target Tracking Sensor Networks. *Mobicom '04: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*, Pages 129–143, New York, NY, USA, 2004. ACM.

[15] Hill, Jason and Szewczyk, Robert and Woo, Alec and Hollar, Seth and Culler, David and Pister, Kristofer. System Architecture Directions for Networked Sensors. *ACM SIGOPS Operating Systems Review*, Number 5, Pages 93–104, 2000. ACM.

[16] Kalpana Sharma, M K Ghose. Article: Wireless Sensor Networks: an Overview on Its Security Threats. *IJCA Special Issue on Manets*, (1):42–45, 2010.

[17] Karlof, Chris and Sastry, Naveen and Wagner, David. Tinysec: a Link Layer Security Architecture for Wireless Sensor Networks. *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems* in Sensys '04, Pages 162–175, New York, NY, USA, 2004. ACM.

[18] Kumar, H. and Sarma, D. and Kar, a. Security Threats in Wireless Sensor Networks. *Aerospace and Electronic Systems Magazine, IEEE*, 23(6):39 -45, 2008.

[19] Malan, David J. and Welsh, Matt and Smith, Michael D. Implementing Public-Key Infrastructure for Sensor Networks. *ACM Trans. Sen. Netw.*, 4(4):22:1–22:23, 2008.

[20] Noth, Andre and Siegwart, R and Engel, W. *Design of Solar Powered Airplanes for Continuous Flight*. Phd Thesis, ETH, 2008.

[21] Taejoon Park and Kang G. Shin. Lisp: a Lightweight Security Protocol for Wireless Sensor Networks. *Trans. on Embedded Computing Sys.*, 3(3):634–660, 2004.

[22] Pathak, P.H. and Dutta, R. a Survey of Network Design Problems and Joint Design Approaches in

Wireless Mesh Networks. *Communications Surveys Tutorials, IEEE*, 13(3):396-428, 2011.

[23] Adrian Perrig and Robert Szewczyk and Victor Wen and David Culler and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. *Mobicom '01: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, Pages 189–199, New York, NY, USA, 2001. ACM.

[24] Roberto Di Pietro and Luigi V. Mancini and Alessandro Mei. Random Key-Assignment for Secure Wireless Sensor Networks. *SASN '03: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, Pages 62–71, New York, NY, USA, 2003. ACM.

[25] G. J. Pottie and W. J. Kaiser. Wireless Integrated Network Sensors. *Commun. ACM*, 43(5):51–58, 2000.

[26] Michael O. Rabin. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. *J. ACM*, 36(2):335–348, 1989.

[27] Romeo, Giulio and Frulla, Giacomo and Cestino, Enrico and Corsino, Guido. HELIPLAT: Design, Aerodynamic, Structural Analysis of Long-Endurance Solar-Powered Stratospheric Platform. *Journal of Aircraft*, 41(6):1505–1520, 2004.

[28] Santi, Paolo. Topology Control in Wireless Ad Hoc and Sensor Networks. *ACM Computing Surveys (CSUR)*, 37(2):164–194, 2005.

[29] Hiren Kumar Deva Sarma and Avijit Kar. Security Threats in Wireless Sensor Networks. *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, Pages 243 -251, 2006.

[30] Schaefer, Pete and Colgren, Richard D and Abbott, Richard J and Park, Han and Fijany, Amir and Fisher, Forest and James, Mark L and Chien, Steve and Mackey, Ryan and Zak, Michail and Others. Technologies for Reliable Autonomous Control (TRAC) of Uavs. *Digital Avionics Systems Conference, 2000. Proceedings. DASC. the 19th*, Pages 1E3–1, 2000. IEEE.

[31] Swiderski, F. and Snyder, W. *Threat Modeling* of Professional Series. Microsoft Press, 2004.

[32] Torr, Peter. Demystifying the Threat-Modeling Process. *IEEE Security and Privacy*, 3(5):66–70, 2005.

[33] Peter Torr. GUERRILLA THREAT MODELLING (or 'THREAT MODELING' IF YOU'RE AMERICAN). Peter Torr's Blog, 2005.

[34] Ronald Watro and Derrick Kong and Sue-Fen Cuti and Charles Gardiner and Charles Lynn and Peter Kruus. Tinypk: Securing Sensor Networks with Public Key Technology. *SASN '04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Pages 59–64, New York, NY, USA, 2004. ACM.

[35] Wise, Richard. *UAV Control and Guidance for Autonomous Cooperative Tracking Of A Moving Target*. Phd Thesis, University Of Washington, 2006.

## Email Addresses

Jiang Bian: jbian@uams.edu

Remzi Seker: sekerr@erau.edu

Mengjun Xie: mxxie@ualr.edu

*2013 Integrated Communications Navigation and Surveillance (ICNS) Conference*

*April 23-25, 2013*