EasyChair Preprint

№ 3788

Context-Aware Operation for Unmanned Systems with HAMSTER

Mariana Rodrigues, Daniel Fernando Pigatto and
Kalinka Regina Lucas Jaquie Castelo Branco

July 8, 2020

Context-Aware Operation for Unmanned Systems with HAMSTER

1st Mariana Rodrigues
Instituto de Ciências Matemáticas e de Computação (ICMC)
Universidade de São Paulo (USP)
São Carlos, Brazil
rodrigues.mariana@gmail.com

2nd Daniel F. Pigatto
Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Universidade Tecnológica Federal do Paraná (UTFPR)
Curitiba, Brazil
pigatto@utfpr.edu.br

3rd Kalinka R. L. J. C. Branco
Instituto de Ciências Matemáticas e de Computação (ICMC)
Universidade de São Paulo (USP)
São Carlos, Brazil
kalinka@icmc.usp.br

***Abstract*—Unmanned Vehicles can benefit from contextual information to improve their operation and security. In fact, a node in any network might assume different levels of criticality depending on several factors, such as their inner components' states, data relevance, provided services, and contextual information. Being aware of a criticality level for an individual node helps determining more consistent approaches to communication and security/safety implementations. In this paper, the integration of security contextual information in a UV communication architecture is demonstrated, in order to increase its safety, overall security and survivability.**

***Index Terms*—context-aware, security, safety, unmanned systems**

I. Introduction

Unmanned Systems (USs) can be defined as systems containing powered vehicles that do not carry a human operator. They may have different autonomy levels and vehicle types such as Unmanned Aerial Vehicles (UAVs), Unmanned Ground Vehicles (UGVs), Unmanned Surface Vehicles (USVs), Unmanned Underwater Vehicles (UUVs), and other designations. Network communications become a fundamental component as those systems get more distributed and ubiquitous, making them more vulnerable to attacks [1].

Context-Aware Security enables UVs to adapt to different kinds of environments, increasing safety, overall security and survivability. In a benign environment, security mechanisms can be less robust and more efficient, while in malicious environment strong security solutions are needed [2]. It is possible then to keep communication safe more efficiently, a highly desirable property in UV systems.

In this paper, it is demonstrated how context is incorporated in HAMSTER architecture for unmanned systems. HAMSTER (HeAlthy, Mobility and Security based data communication archiTEctuRe) is a communication architecture for unmanned vehicles designed for improving mobility, security and safety of the system [3]. Assuming contextual knowledge, HAMSTER can improve communication security, vehicle safety and service provision, making UV applications more reliable, robust and compatible to the new IoT systems.

This paper is organized as follows. Section II presents some related work in context-aware security for unmanned vehicles. Section III discusses how context is fed and dealt by the architecture. Section IV details how contextual information is evaluated, with a case study for UAVs being demonstrated in Section V. Finally, Section VI concludes the paper.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. Research was also sponsored by the Army Research Office and was accomplished under Grant Number W911NF-18-1-0012. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

II. Related Work

Context can help UV operation in many aspects, such as user interface, path planning, task optimization and, as discussed, to adapt to different threat levels in the network. This is of great value for critical systems.

Authors from [2] propose a security framework which aims at providing necessary security services through all network layers while minimizing the potential security redundancy and resource consumption. For this, the selection is made in two steps: an offline selection model and an online self-adaptive control module. In order to select the protocol set, all protocols are classified with two indexes: a security index (higher SI means more resistant protocols) and a performance index (higher PI means lower performance cost). On deployment, the MANET nodes can perceive if the threat level increases or decreases, triggering a negotiation for a new set of protocols. SI and PI values were estimated for 6 different protocol sets.

The work in [4] presents an adaptive security framework for battleground UAV-assisted networks. The authors discuss two different operation modes: in the infrastructure mode, UAVs act as a central authority for certificate issuing and authorization, while in the infrastructureless mode the functions are distributed among all network nodes. It is possible to switch between operation modes seamlessly by means of backup CA keys and employing e-voting systems in a distributed manner.

The work in [5] presents a health management model based on Bayesian Networks for adapting UAVs to failures during operation, making its firmware adaptable to context.

III. Contex-Aware Security in HAMSTER

The Node Criticality Index (NCI) is a key feature provided with HAMSTER architecture [3] which consists on a rich index to help determining single and global priorities for nodes within a network. Considering the HAMSTER architecture domain, NCI is applied to several communications: machine-to-machine (M2M), machine-to-infrastructure (M2I) and internal machine communications (IMC). The main goal is to provide a measurable level of criticality associated with individual nodes, allowing better decision making on Quality of Service (QoS), security, safety and prioritization approaches for modules, clusters of modules and entities. NCI is flexible enough to encompass different sets of goals based also on mission information.

NCI was designed to work in three different situations within an Unmanned System: i) the network connecting basic and mission-specific internal modules individually, ii) the network connecting internal clusters of modules, and iii) the external network among unmanned vehicles and eventual infrastructure entities.

To deal with context for UVs, HAMSTER deals with three different types of contextual information, based on the work presented in [6] for an autonomous underwater vehicle and later in [7] for an autonomous ground vehicle. In these works, contextual information is composed by three elements: environmental or *external context*, task-related or *mission context*, and operation-related or *internal context* information.

External context relates to environmental information. It does not depend on the vehicles' actions, but allows the UV to perceive its surroundings and adapt itself accordingly. Mission context is dependent on mission specifications, and therefore is different for every assigned mission. Finally, internal context refers to the UV's internal state, and interferes directly on the information reliability and UV safety.

HAMSTER gathers all context information and translates it to a *Perceived Security Index* or PSI used to make decisions regarding security mechanisms, service provision and consumption and for UV safety and self-preservation. The PSI is estimated given the three types of context being considered.

A. External Security Context

External Security Context relates to threats that are not a direct consequence of UV operation, but rather caused by external agents. This is translated mainly in any cyber-threat the UV is vulnerable to and also, specially on UAVs or small UGVs, hijacking.

Fig. 1 brings a taxonomy of attacks for autonomous vehicles provided by [8] and later expanded for UAVs by [9]. The taxonomy classifies the attacks according to physical or remote access to the UV, and in invasive or non-invasive attacks. Fig. 1 also brings possible targets of each attack, as in Electronic Control Units (ECU), Sensors and GPS and the communication links (Internal Vehicle Communication — IVC, Vehicle-to-Vehicle — V2V and Vehicle-to-Infrastructure — V2I). Moreover, there is an indication of which element of the CIA triad (Confidentiality, Integrity, Availability) could be compromised for each attack, based on UAV attack taxonomy presented in [10].

An initial estimation of PSI for external context can be obtained by performing a risk evaluation for those attacks, taking into account their likelihood and impact. Available security mechanisms also have to be considered, as well as any indicator that the UV is suffering an attack.

HAMSTER has some in-built security mechanisms and policies that help mitigate some of the attacks presented.

1) Authentication of UV internal modules: In *Cloud*–SPHERE (Security and safety Platform for HEteRogeneous systEms connected to the Cloud [11], which is a platform responsible for communication security and safety management in HAMSTER), all internal modules are identified and authenticated in an "Almost Deny All" approach, meaning that the vehicle is unable to operate unless all critical components are properly authenticated. This makes attacks of code modification and code injection more difficult on those modules.

2) Use of Cryptography: HAMSTER supports the use of cryptography in all types of communication (HAMSTER-specific or user-defined messages). This greatly decreases the risk to confidentiality, provided that the key-distribution scheme is successfully executed with no disclosures.

3) Support to different types of network topology: NIMBLE (NatIve MoBiLity platform for unmanned systEms [12]) has specific modules to deal with both ad hoc and infrastructure communication, making it possible for the UV to change communication strategy if a specific link is being jammed or spoofed. The use of cognitive radio hardware also helps to avoid these types of attacks.

B. Mission Security Context

Mission Security Context relates to the tasks the UV has to perform in the application it is being used, and the risks associated with them. There are many aspects that can be considered, such as the mission target and its path from initial location, sensitiveness of data and component usage.

Regarding information security, data sensitiveness is a very important aspect to be considered. Depending on the application, stored data need to be encrypted, and self-destruction policies may be necessary if the environment becomes hostile.

An initial estimation of PSI for mission context can be obtained by evaluating the localization of the UV (for instance, a rural or populated area), risk of collision with other vehicles or people, and mission data sensitiveness.

C. Internal Security Context

Internal Security Context relates to the UV internal state and is strongly connected to its safety. Any component malfunction or failure impacts on PSI for internal context.

In HAMSTER, *Cloud*–SPHERE manages connection status and safety supervision of all UV components. The component

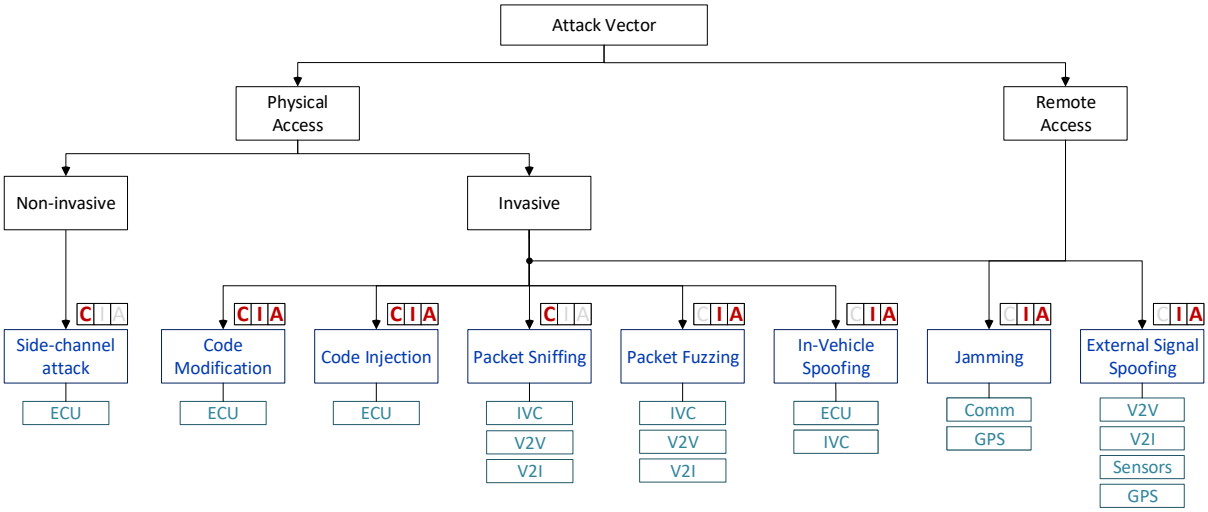

Fig. 1. Taxonomy of UV attacks (adapted from [8]).

state contributes to its criticality index, measured by NCI. NCI value depends on data sensitiveness, module importance and safety state.

IV. HAMSTER Contextual Evaluation

As discussed before, estimated PSI value impacts HAMSTER security mechanisms, service provision and consumption and for UV safety and self-preservation.

Since the architecture leans heavily on abstractions, different strategies for security mechanisms like cryptography, identification or authentication can be made available to the application. Every strategy has an impact on the perceived security and has to be considered in PSI calculation, which determines the UV actions. For example, a UAV performing a mission on a lower populated area may use a symmetric cryptography algorithm, which is usually lighter and has a lower security index. If a threat is identified, the UV could switch to an asymmetric algorithm to improve PSI or decide to abort the mission for UV self-preservation.

Service provision and consumption handled by SEMU (Service Exchange Management Unit [13]) is also affected. Unauthorized or defective components are not eligible for providing reliable services. A malfunction or disconnection results in services being discontinued. Also, a UV can decide on a minimal PSI level for service exchange with other UVs.

A. PSI evaluation

For each UAV in the scenario, PSI value is given by the combination of every contextual component:

$$\Psi = \sqrt{\frac{\psi_{ex}^2 + \psi_{mi}^2 + \psi_{in}^2}{3}}$$

where Ψ is the Perceived Security Index, PSI and ψ_c is a partial security index related to context c.

PSI values are discretized to five levels (TABLE I). $\Psi = 0$ means that the environment is hostile and there is none or insufficient security measures for UV operation; $\Psi = 5$ means a benign environment with more than sufficient security measures in place.

HAMSTER platforms and user application can refer to these values when making decisions and assuring UV security and safety. HAMSTER Units have a minimum PSI requisite to operate normally. If the PSI value falls below this security threshold, the UAV initiates an emergency protocol, in which modules can be turned off by Navigation Phases and all but critical operations be stopped by Cloud–SPHERE and SEMU.

As discussed, initial PSI values are likely to be dependent on the vehicle type and application, assuming subjective values depending on the specialist doing the security analysis. In the next section, a case study for initial PSI estimation for a typical UAV application in precision agriculture is detailed.

TABLE I
Perceived security levels in HAMSTER.

5	High security
4	Medium to high security
3	Medium security
2	Medium to low security
1	Low security
0	No security

V. Case Study with UAVs

In this section, a demonstration on PSI estimation in HAMSTER is provided for an application with UAVs. In this scenario, three small ($< 1m$ size) UAVs are used to capture images of a crop. They communicate in an ad hoc manner and each one has an IMU (Inertial Measurement Unit) and a GPS to identify its location, a camera to capture the images, an autopilot that also activates the camera, a propeller and servomotors. All UAVs know the identity of

TABLE II
DIFFICULTY CRITERIA PROPOSED BY [14].

Required Hardware (H)	1	No extra hardware required
	2	Basic hardware other than PC/Laptop
	4	Advance hardware requirement
Required Skills (S)	1	No expert knowledge required
	2	Tools are available in the public domain
	4	Advanced skills needed
Physical Access (PA)	1	Physical access not required
	4	Physical access required

their communication peers and perform (1) internal module authentication before (2) mutual UAV authentication so the mission can be started. The UAVs communicate with each other using asymmetric cryptography and take-off/landing and mission location is the same controlled area.

A. External Context Initial Evaluation

In order to evaluate the external context security index (ψ_{ex}), threats and available security measures need to be analyzed. The perceived security will be at its maximum when the risk coming from the external environment is minimum. In this case, the risk is analyzed based on attack difficulty, impact and countermeasure.

For determining attack difficulty, threats shown in Fig. 1 are classified based on a criteria proposed by [14]:

$$D = \frac{H + S + PA}{12}$$

where H represents the type of hardware required for the attack, S the level of skill and PA if physical access is needed. The difficulty D results in a value from 0.25 (Easy) to 1 (Hard). The criteria proposed in [14] are reproduced in TABLE II. The likelihood of an attack to happen will be inversely proportional to its difficulty.

The threat impact (TI) on the system is also classified according to the criteria used by [10], with values Low (Very limited systems outages), Medium (Limited systems outages) and High (Long time systems outages).

Finally, the countermeasure impact (CI) for this study case (asymmetric cryptography and component/UAV mutual authentication) also needs to be assessed. Countermeasure impact can vary from 0 (none) to 3 (high).

Once those values are made, the threat risk r is given by

$$r = \frac{D * (1 - TI)}{2.25 * CI},$$

whose values are classified according to TABLE III. The 2.25 value in denominator is used to normalize the risk values to the interval $[0, 1]$.

The results for this assessment are shown in TABLE IV, which shows that the most dangerous situations for these UAVs will be when a Jamming or External Spoofing attacks happens. In this case, security countermeasures have very low impact, and the UAVs need to take drastic measures if a critical sensor is being spoofed or if communication is jammed.

TABLE III
RISK CLASSIFICATION OF THREATS.

$r < 0.20$	Very low risk
$0.2 \leq r < 0.4$	Low risk
$0.4 \leq r < 0.6$	Medium risk
$0.6 \leq r < 0.8$	High risk
$r > 0.8$	Very high risk

Once the evaluation is made, it is possible to estimate the PSI external component ψ_{ex}, which is given by:

$$\psi_{ex} = 5 * (1 - \overline{r}),$$

which in this case will evaluate to $\psi_{ex} = 2.99$.

B. Mission Context Initial Evaluation

The mission context security index (ψ_{mi}) is evaluated analyzing the steps the UAV needs to perform in order to finish its mission. UAVs are specially critical since they present a risk of collision to other aircraft, manned or unmanned, called *air risk* and a risk of failure that can result in a free fall and bring injury to people of infrastructure, called *ground risk*. Therefore, mission location and the path planned for its execution can be quite critical.

There are many ground risk models for UAVs, as surveyed by [15]. Also, the Joint Authorities for Rulemaking of Unmanned Systems (JARUS[1]) is a worldwide organization that aims at providing a unique set of technical, safety and operational requirements for Remotely Piloted Aerial Systems (RPAS). They have produced a guideline for Specific Operations Risk Assessment (SORA) that has been used to assess risk in some works in the literature.

For this demonstration, the context security index is initially estimated by using a much simpler approach, which can be considered a simplification of SORA. UAV size, path, mission target and airspace operation are taken into account, as shown by TABLE V.

Similarly, the PSI mission component is given by the multiplicative inverse of the normalized risk, proportionally to the maximum PSI level:

$$\psi_{mi} = 5 * (1 - \hat{r}),$$

which in this case will evaluate to $\psi_{mi} = 5 * (1 - (1/3)) = 3.33$.

C. Internal Context Initial Evaluation

As described, Internal Context is dealt by HAMSTER' NCI platform.

The scenario is analyzed by defining the each module's $NCIm$ and then the $NCIe$ for the UAV. According to the formulae and definitions of $NCIm$, for each module in normal functioning are assumed as shown in Table VI.

Considering that sensors (GPS and IMU), actuators (motor and servomotors) and the radio transmitter/receiver do not

[1] www.jarus-rpas.org/

TABLE IV
EXTERNAL CONTEXT SECURITY INDEX INITIAL ASSESSMENT.

Threat	Difficulty (D)	Threat Impact (TI)	Countermeasure Impact (CI)	Risk
Side-channel attack	Hard (0.83)	High (3)	None (0)	Low (0.22)
Code Modification	Hard (0.83)	High (3)	Low (1)	Low (0.22)
Code Injection	Hard (1)	High (3)	Low (1)	Very low (0)
Packet Sniffing	Easy (0.33)	Medium (2)	High (3)	Very low (0.19)
Packet Fuzzing	Medium (0.58)	High (3)	Medium (2)	Low (0.28)
External Signal Spoofing	Easy (0.25)	High (3)	Low (1)	High (1)
Jamming	Easy (0.33)	High (3)	Low (1)	Very High (0.89)

TABLE V
PROPOSED GROUND AND AIR RISK ASSESSMENT BASED ON SORA.

LOCATION GROUND RISK

Operation Scenario	UAV size			
	$< 1m$	$1-3m$	$3-8m$	$> 8m$
Controlled area	Low	Low	Low	Medium
VLOS/underpopulated	Low	Low	Medium	Medium
BVLOS/underpopulated	Low	Medium	Medium	High
VLOS/populated	Medium	Medium	High	High
BVLOS/populated	Medium	High	High	High

AIR RISK FOR ATYPICAL AIRSPACE

Operation Scenario	Risk
Controlled area	Low (1)
VLOS, underpopulated	Low (1)
BVLOS, underpopulated	Medium (2)
VLOS, populated	Medium (2)
BVLOS, populated	High (3)

TABLE VI
$NCIm$ FOR EACH MODULE OF A UAV.

Module	$NCIm^{sec}$			$NCIm^{saf}$			$NCIm$
	$storedData$	$temporaryData$	total	$health$	$priority$	total	
GPS	0	0.3	0.3	0	0.5	0.25	0.275
IMU	0	0.3	0.3	0	1	0.5	0.4
Camera	0.5	0	0.5	0	0	0	0.25
Autopilot	0.3	0.3	0.3	0	1	0.5	0.4
Motor	0	0	0	0	0.5	0.25	0.125
Servomotor1	0	0	0	0	1	0.5	0.25
Servomotor2	0	0	0	0	1	0.5	0.25
Radio transmitter/receiver	0	0.3	0.3	0	0.3	0.15	0.225

store data, $storedData$ is set to 0. The camera stores images of the overflown region to identify assets and vulnerable areas, which leads to a score of 0.5 for $storedData$. The autopilot stores information about the positioning of the aircraft when pictures are taken. This module's $storedData$ is set to 0.3 due to the importance of stored information. The GPS log is not as important as acquired images for the mission, which justifies the difference in scores between these modules.

GPS, IMU, autopilot and radio transmitter/receiver manipulate data related to the aircraft positioning, thus $temporaryData$ is set to 0.3. Remaining modules deal with no data that could be considered risky for the UAV, being set to 0 on $temporaryData$. In a normal operation, all modules are properly working, thus $health$ is set to 0.

The most critical modules for a proper functioning are IMU, autopilot and the servomotors. These modules are set to the highest value for $priority$, 1. GPS and motor's $priority$ score are set to 0.5, because it is still possible to land the UAV even if any of these modules fails. The radio transmitter/receiver is not necessary to the accomplishment of the task. However, if the UAV is forced to land, it is necessary to establish a communication via radio in order to locate and rescue the UAV, which justifies its value of 0.3 for $priority$. Finally, regarding camera's $priority$, it is set to 0 because if it fails, the UAV can safely go back home.

The definition of entities' $worth$ measure is dependent on its cost. In this case, $worth$ is considered as 1. The variable $field$ is set to 0 due to the fact that the covered area is a crop and presents no risk to the environment or people in case of an accident. The $accomplishment$ is set to 0 since the mission can be restarted at any time and a deadline was not specified. Indeed, the $NCIe$ is 0.345.

Similarly, the PSI internal component is given by the multiplicative inverse of the normalized risk, proportionally to the maximum PSI level:

$$\psi_{in} = 5 * (1 - NCIe),$$

which in this case will evaluate to $\psi_{in} = 5*(1-0.345) = 3.27$.

D. PSI Initial Evaluation

Given the three estimations, the initial Perceived Security Index value is given by

$$\Psi = \left\lfloor \sqrt{\frac{\psi_{ex}^2 + \psi_{mi}^2 + \psi_{in}^2}{3}} \right\rceil =$$

$$= \left\lfloor \sqrt{\frac{2.99^2 + 3.33^2 + 3.27^2}{3}} \right\rceil = \lfloor 3.2 \rceil$$

which is classified as 3 – Medium security risk according to Table I.

E. Context changes impact on PSI

In this section, it is discussed how HAMSTER deals with security context changes. For that, two situations are discussed: a GPS failure due to malfunction and the same failure caused by a spoofing attack.

First of all, HAMSTER SMU platform inside Cloud–SPHERE detects a non-expected change in GPS reading.

This detection is informed to NCI, which updates the $health$ component from GPS' $NCIm^{saf}$ index from 0 (normal) to 1 (experiencing issues). The GPS NCI then changes from 0.275 to 0.442. This results in a UAV NCI of 0.426.

As a consequence, the NCI modification impacts the PSI's internal context component, which evaluates to

$$\psi'_{in} = 5 * (1 - NCIe) = 2.79,$$

which in turn will impact global PSI with a new value of Ψ'=3.04, which is still evaluated as Medium Security.

The change in NCIm value results in the module being considered unreliable, as are all SEMU services related to it. As discussed in the beginning of Section IV, those related services have their provision and advertisement interrupted. If another module inside the UAV or an external client is using those services, they will have to query new providers.

Besides the GPS malfunction, if the SMU or another IDS-enabled component detects a spoofing attack, not only will the internal context change, but also the external context. In this case, the external risk is overruled to the normalized value of threat impact (TI in TABLE III), if this value is higher than the current risk evaluation.

In this case, the TI normalized value for external spoofing attack is 1, and therefore the new value for PSI external component will be given by:

$$\psi'_{ex} = 5 * (1 - 1) = 0$$

The new PSI value in case of spoofing attack considers the value changes from both external and internal context, being evaluated to:

$$\Psi' = \left\lfloor \sqrt{\frac{{\psi'_{ex}}^2 + \psi_{mi}^2 + {\psi'_{in}}^2}{3}} \right\rceil =$$

$$= \left\lfloor \sqrt{\frac{0^2 + 3.33^2 + 2.79^2}{3}} \right\rceil = \lfloor 2.5 \rceil ,$$

which is conservatively evaluated to 2 - Low Security.

In HAMSTER applications, as previously discussed on Section IV-A, there is a minimum PSI level for the UAV to operate. In this case, if the PSI level was set to Medium Security, the detection of the spoofing attack would trigger the execution of an emergency protocol defined by the UAV application and not HAMSTER itself. In this situation, the UAV can be commanded to turn off all non-critical modules, interrupt services which have low security mechanisms applied to them, or return to base immediately.

VI. Conclusion

In this paper, it was shown how HAMSTER architecture considers the contextual information in security by defining a *Perceived Security Index* or PSI. Three different types of context were described (external, mission and internal context), as well as how HAMSTER deals with and is affected by contextual information. A case study for UAVs was conducted to demonstrate how PSI can be estimated initially and how context changes affect its value and, consequently, HAMSTER operation. Future work include context-aware protocol for operation configuration at different security levels, security mechanisms interchange and mission context configuration in the HAMSTER prototype being developed, as well as evaluations on how the adaptation of security mechanisms available impact on the environment, the communication links and UV survivability.

References

[1] E. Yuan, N. Esfahani, and S. Malek, "A Systematic Survey of Self-Protecting Software Systems," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 8, no. 4, p. 41, jan 2014.

[2] C. Chigan, Leiyuan Li, and Yinghua Ye, "Resource-aware Self-Adaptive Security Provisioning in Mobile Ad Hoc Networks," in *IEEE Wireless Communications and Networking Conference*, vol. 4. New Orleans, USA: IEEE, mar 2005, pp. 2118–2124.

[3] D. F. Pigatto, L. Gonçalves, G. F. Roberto, J. F. Rodrigues Filho, N. B. Floro da Silva, A. R. Pinto, and K. R. Lucas Jaquie Castelo Branco, "The HAMSTER Data Communication Architecture for Unmanned Aerial, Ground and Aquatic Systems," *Journal of Intelligent & Robotic Systems*, vol. 84, no. 1-4, pp. 705–723, dec 2016.

[4] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, "Adaptive security for multilevel ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 533–547, aug 2002.

[5] S. Zermani, C. Dezan, C. Hireche, R. Euler, and J.-P. Diguet, "Embedded context aware diagnosis for a UAV SoC platform," *Microprocessors and Microsystems*, vol. 51, pp. 185–197, jun 2017.

[6] R. M. Turner, "Context-mediated behavior for intelligent agents," *Int. J. of Human-Computer Studies*, vol. 48, no. 3, pp. 307–330, mar 1998.

[7] D. D. Bloisi, D. Nardi, F. Riccio, and F. Trapani, *Context-Enhanced Information Fusion*, ser. Advances in Computer Vision and Pattern Recognition, L. Snidaro, J. García, J. Llinas, and E. Blasch, Eds. Cham: Springer International Publishing, 2016.

[8] V. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. Chengdu, China: IEEE, dec 2016, pp. 164–170.

[9] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. Shanghai, China: IEEE, oct 2017, pp. 194–199.

[10] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System," in *IEEE Conference on Technologies for Homeland Security (HST)*. Waltham, USA: IEEE, nov 2012, pp. 585–590.

[11] M. Rodrigues and K. R. L. J. C. Branco, "Cloud–sphere: Towards secure uav service provision," *Journal of Intelligent & Robotic Systems*, Jun 2019. [Online]. Available: https://doi.org/10.1007/s10846-019-01046-6

[12] L. T. Munhoz, D. F. Pigatto, and K. R. L. J. C. Branco, "Performance Evaluation of Handoff in Mobile IPv6 Networks: The Case of Safety-Critical Systems with NIMBLE Platform for Mobility," in *Communication in Critical Embedded Systems. WoCCES 2014, WoCCES 2015, WoCCES 2013, WoCCES 2016.*, ser. Communications in Computer and Information Science, K. Branco, A. Pinto, and D. Pigatto, Eds. Cham: Springer International Publishing, 2017, vol. 702, ch. 2, pp. 23–44. [Online]. Available: http://doi.org/10.1007/978-3-319-61403-8_2

[13] M. Rodrigues and K. R. L. J. C. Branco, "UAVs at Your Service: Towards IoT Integration with HAMSTER," in *International Conference on Unmanned Aircraft Systems (ICUAS)*. Atlanta, USA: IEEE, jun 2019, p. to appear.

[14] K. Singh and A. K. Verma, "Threat modeling for multi-UAV Adhoc networks," in *IEEE Region 10 Conference (TENCON)*. Penang, Malaysia: IEEE, nov 2017, pp. 1544–1549.

[15] A. Washington, R. A. Clothier, and J. Silva, "A review of unmanned aircraft system ground risk models," *Progress in Aerospace Sciences*, vol. 95, pp. 24 – 44, 2017.