American Journal of Engineering Research (AJER) 2015
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-4, Issue-8, pp-186-190
www.ajer.org
Research Paper Open Access

Secured UAV based on multi-agent systems and embedded Intrusion Detection and Prevention Systems

K.Boukhdir[1], F.Marzouk[1], H.Medromi[1], S.Tallal[1], S.Benhadou[1]
[1](Systems Architecture's Team, ENSEM)

ABSTRACT : *Unmanned aerial vehicles, or drones, are a relatively recent area of research and in full effervescence with more and more amateur and academic projects. Initially associated to the military, these vehicles are way to be used in many other areas. In effect, demand is growing for various applications within of this type of technology. Inspection of buildings, search and rescue of missing or in distress people are some examples. This research paper highlights a lightweight intrusion detection system with the objective to secure UAVs. Our IDP(Intrusion and Prevention System) uses real-time architecture, based on the multi-agent systems so it can be autonomous and distributed between the ground control station(GCS) and the UAV is more suited to be embedded in low computation resources devices in general and especially UAVs.*

Keywords *-UAV security, Intrusion and Prevention systems, multi-agent systems.*

I. INTRODUCTION

The main goal of the project is to create a secure UAV (Unmanned Aerial Vehicle), stable and efficient, operating in several modes: full autonomy (Autopilot), partial autonomy (planning instant flight) or instant driving.The UAV includes a set of features and equipment, enabling it to undertake different kind of tasks like flying in tactical or strategic objective, recognition, monitoring objectives or inspection. Furthermore, our drone must be secured against all types of attacks that may arise. However, some security techniques do not translate well to embedded systems, where constraints such as low-power, low-memory, and real-time operations may impact the computational capability of the system. The need to secure systems that express complex logic is well understood and presents many challenges –strict timing requirement, computational and storage limitation, adaptability and ubiquitous presence. Our security model is characterized by its board and lightweight nature insofar as it helps to ensure a level of security - confidentiality, integrity and availability- without soliciting too many computational resources.Existing intrusion detection and prevention systems undergo the following problems: intrusion detection system cannot detect and block all the malicious traffic; signature database are not updated on a regular basis; different intrusion detection and prevention systems are not interoperable; and most of all they are not suitable to protect embedded systems because due to structural problems, in other aspects of the architectures can not meet the strict timing and restriction in resources. In this paper, we present a modular and extensible approach to building a system helps solve the complex problems in an embedded intrusion and detection system. It divides the problem into the aspects of information gathering, pre-processing and classification, analysing and configuration. Lightweight agents have been developed to retrieve information from the ground control station, classify and analyse the data and prevents threats, and stores the logs into a database. We also demonstrate how dynamic agents provides a convenient mechanism for extending existing objects and allows us to quickly add new features to the system.

II. BACKGROUND

The extensive use of information and communication technologies (ICT) to solve complex, significant-applied problems has profoundly affected critical infrastructures and systems conception. Such evolutions implicate the exposition to new kinds of security threats. Moreover, the dependence to those technologies has become critical due to the evolution and development of networks in terms of users and provided services. However the need to secure systems that express complex logic is well understood and presents many challenges [1] –strict timing requirement, computational and storage limitation, adaptability and ubiquitous presence for data analysis and monitoring- that have nothing new for security experts. Afterwards, the traditional intrusion detection paradigm based on a hypervisor to create a safe environment from which a analyze entity can operate is impractical to secure critical infrastructures

However, some security techniques do not translate well to embedded systems, where constraints such as low-power, low-memory, and real-time operation may impact the computational capability of the system [5].

A. State Of The Art.

While many work have been done to secure various kinds of wireless based communication like sensor networks (WSN) [6]-[7]-[15] and mobile ad-hoc networks [8], these models cannot be useful to secure usual UAVs. Modeling of UAVs communication is harder and distinctive from other networks for its wider complexities and vast discrepancy in various properties. The use of different channels of different type, the various range of communications (short/long), different power requirements for different components, different types of traffic flows involving commands, video, audio, image and more, the disponibility and integrity and confidentiality requirements, are roughly the features which make security requirements of a UAV dissimilar from other state of the art systems.

Very little research to date has been done to secure UAVs and their communication with the GCS (Ground Control Station) and this resulted in many attacks to those systems. In the next chapter we have reported some of the knows attacks against UAVS

B. Known attacks

Till 1997 there were reports about cyber-attacks targeting UAV systems throughout the world. This is due to the relatively recent of use of those systems in the developed nations. Israeli experts [10] recently determined that the Hezbollah leader Hassan Nasrallah and claims taken over - by an IDF (Israel Defense Forces) drone in the scene of Squadron 13 Banzriih night between 4 and 5 September 1997 are authentic. Nasrallah explained that his organization had intercepted the filming at the time, and that it allowed its fighters to ambush the soldiers [11]. In 2009, the arrest of a terrorist group leads to the detection of the recording of UAV video. The unencrypted video footage was assembled by the terrorists using software called SkyGrabber, which is used to capture satellite data using a satellite antenna [9].

In December 2011 members of Iran's elite Revolutionary Guards put on show a US unmanned aerial vehicle they claimed to have brought down electronically. US officials later confirmed the aircraft was captured in Iran but insisted it malfunctioned and was not hijacked. [12].

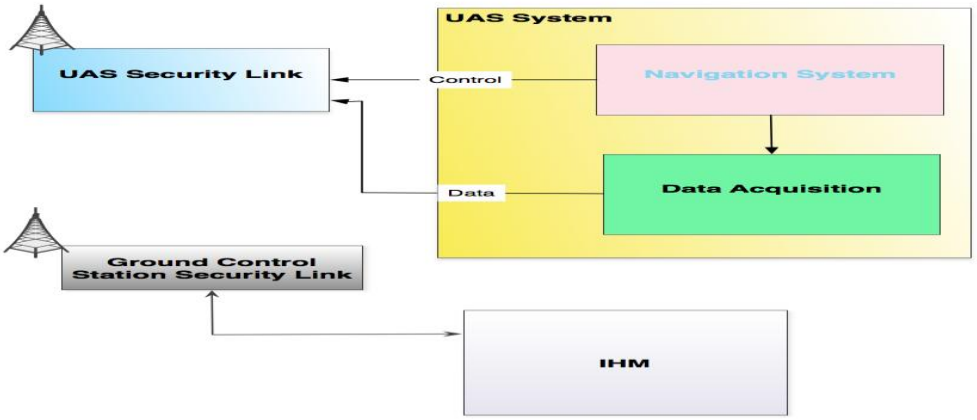

Figure 1 UAV Architecture with security links

III. SYSTEM DESIGN

The system is designed to deliver highmanoeuvrability – vertical Take Off and Landing (can land on very small areas) and able to perform stationary/slow flight (useful to perform long time tasks in the same position) and can easily fly in small and cluttered environment by performing hovering and slow motion.

The hexacopter can be flown in different modes using manual/autonomous control. In the standard mode, hexacopter attitude (roll and pitch), yaw rate and thrust is manipulated with a standard flight radio RC Transmitter, whilist in the autonomous mode, the attitude and thrust are being calculated using the autopilot module wich use a set of data fusion using sequences of PID and some extended filters (figure 2).

To ensure that our security solution won't affect the control system, which needs finely grained timing like controlling the throttle, we plugged it as an expansion board that runs real time Linux. We separated the low-level control loops (PIDs) and all the sensing and filtering that are considered time critical stuff to the autopilot hardware and then run highlevelintrusion detection on the embedded linuxon the Raspberry Pi Card.

III.2. Agents and multi-agent sytems

Agents can push further the level of abstraction and the flexibility of component coupling, notably through self-organization abilities.

An agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through its effectors to maximize progress towards its goals [2][3].

Multi-agent Systems have emerged as one of the most promising solution to cater for the complex, robust[16], and reliable security processes. (Ferber, 1999; Stone &Veloso, 2000; Sycara, 1998; Weiss, 1999) have suggested that MASs are well suited for applications that are distributed, complex, modular, scalable and flexible, where problems in the security fields exhibit these characteristics [3].

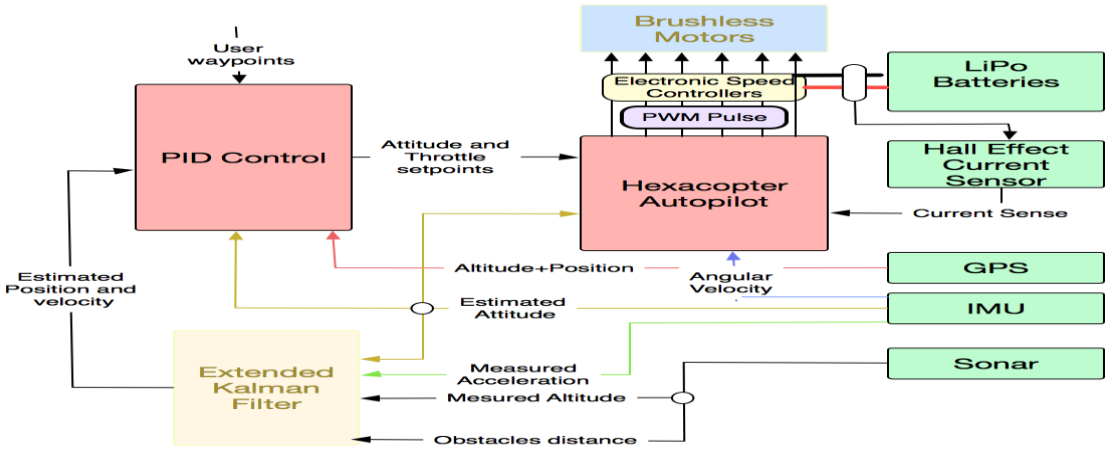

Figure 2 Autopilot design

III.2. UAV IDPS Engine agents Architecture

To overcome the deficits of traditional IDPS systems, the software design use an effective lightweight detection technology witch is the pre-filtering combined with full analysis. The overall structure of the agents composing the IDPS Engine is shown in Figure 3.

Listener Agent is purely a reactive agent with the charge of capturing traffic data. The continuous traffic flows between the GCS and the drone is captured in order to be sent to the preprocessor Agent for processing.

Preprocessor Agent: after receiving traffic data from the listener, it's pre-processed in order to be analyzed. Once the data has been pre-processed, it's sent to the analyzer agent. The task of a preprocessor is to segment the traffic, remove excessive information, defragmentation, checksum validation, connection tracking, and stream re-assembly. And convert into a form that can be feasibly processed by the Analyzer Agent.

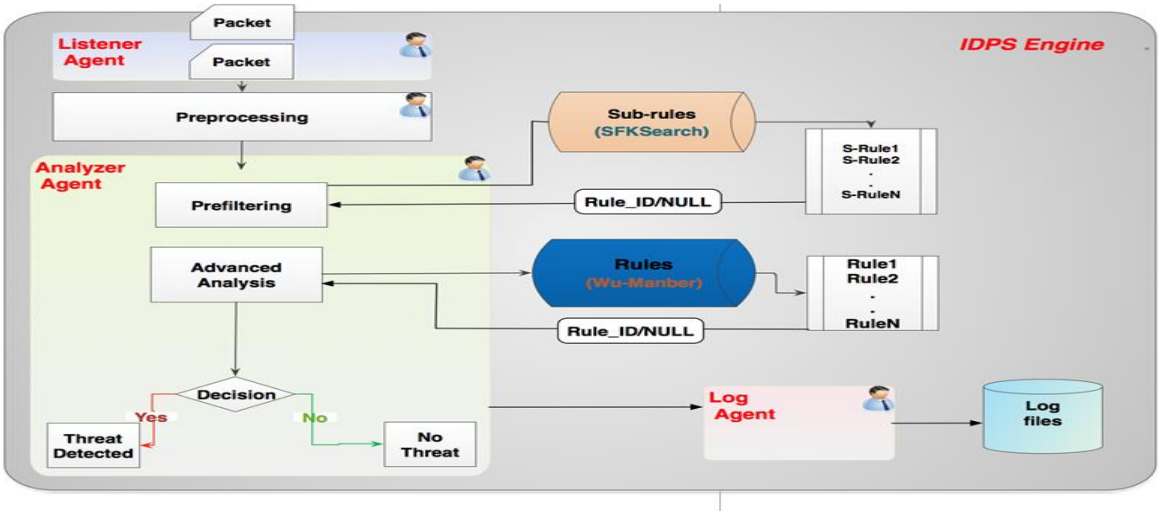

Figure 3 IDPS Engine Architecture

AnalyzerAgent: This intelligent agent is embedded in the analyze stage in order to investigate the pre-processed traffic data. Preprocessed incoming data arrive to the pre-filtering sub-module, which reveals the probably activated rule in a set of sub-rules using the algorithm SFKSearch[13][14]. This algorithm builds a tree and each level in the tree is a sequential list of sibling nodes that contain a pointer to matching rules, a character that must be matched to traverse to their child node, and a pointer to the (next) sibling node. The algorithm uses a bad character shift table to advance through search text until it encounters a possible start of a match string, at which point it traverses the tree looking for matches. If there is a match between the character in the current node and the current character in the packet, the algorithm follows the child pointer and increments the character packet pointer. Otherwise, it follows the sibling pointer until it reaches the end of the list, at which point it recognizes that no further matches are possible. In the case that matching fails, the algorithm backtracks to the point at which the match started, and now considers matches starting from the next character in the packet.

In the worst case, the SFKSearch algorithm can make L · P memory references where L is the length of the longest pattern string and P is the length of the packet examined.

If in the pre-filtering stage a rule has already been activated, the information's about the rule are reported to the advanced analysis sub-module. This sub-module is responsible for content matching and deep analyzing by using the Wu-Manber[13][14]algorithm. This algorithm starts by pre-computing two tables, a bad character shift table, and a hash table. When the bad character shift fails, the first two characters of the string are indexed into a hash table to find a list of pointers to possible matching patterns. These patterns are compared in order to find any matches and then the input is shifted ahead by one character and the process repeats.

An interface between the pre-filtering and the advanced analysis sub-module should be used to feed the advanced analysis sub-module with the identification (ID) of the matched sub-rules and their exact position in the rule database.

Log Agent: This agent is responsible for storing and maintaining the log data in order to be used to generate detailed reports about the communication and the threats detected. This log is also needed to check the performance of the IDPS Engine by studying it.

The IDPS Engine assures near real-time analyses by analyzing information sources gathered by the listener agent on a real-time basis. Thus, it is important to provide responses before an attacker significantly damages the systems.

III.3. Summary

The proposed architecture ensures that the IDPS is using the minimal resource in the systems when monitoring. In fact, the minimal resource could avoid the shortage of the systems resource and prevent the system from possible crash caused by overloading. In order to respect real time constraint and to use the minimal possible resources in the system, the pre-filtering agent witch uses a set of sub-rules extracted from full rules and a very efficient matching algorithm (SFKSearch). The most complicated task of the pre-filtering is to figure out an effective way to generate a tiny rule (sub-rule) of the each original intrusion detection rule-set and that the sub-rule must be representative of the full rule so that the amount of activated rules in the Pre-filtering phase would be as significant as possible.

IV. EXPERIMENTAL RESULTS

To test our architecture, we used a Raspberry Pi computer (ARM1176JZF-S CPU and 512 MB SDRAM) embedded in our UAV. The performance of the Raspberry Pi computer is far too low compared to a usual computer with high computational power, but the fact that it weights less than 45 g (1.6 oz) and its battery very low battery consumption makes it more suitable to be embedded in a UAV in order to host our lightweight IDPS.

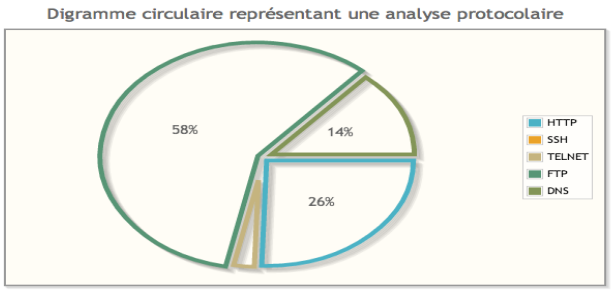

Figure 4 : Report Chart

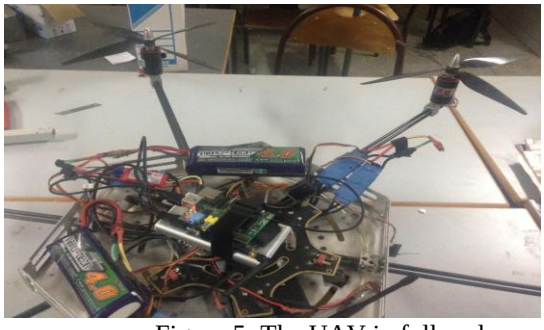

Figure 5: The UAV in full scale

We tested our IDPS against several threats techniques. Most of the threats tested are samples that help demonstrate the capabilities and the efficacy of the detection and prevention approach. Those threats code were written with the only purpose to test the platform and the test was conducted mainly while embedding the system in the UAV (Fig.4). Fig.5 shows screenshots of the result after testing the IDPS with a set covering a large scope of attacks (badTraffic, evasionTechniques, shellCodes, DOS/DDOS) and a ruleSet which are basic rules testing. These attacks are supposed to be detected by the rules sets shipped with the IDPS.

V. CONCLUSION

Intrusion detection and prevention systems are a good solution to mitigate threats but the state of the art IDPSs are not suitable to protect embedded systems because due to structural problems, like strict timing and restriction in resources.In this paper, we presented a modular and extensible approach to building a system helps solve the complex problems in an embedded intrusion and detection system that divides the problem into the aspects of information gathering, pre-processing and classification, analysing and configuration. The use of lightweight agents helped modularizing the platform in order to make it more suitable for embedded devices.

However an overall security threat analysis of the UAVs system must be conducted to mitigate other threats like GPS spoofing and signal jamming and also expand the platform to help secure the ground control station (GCS).

REFERENCES

[1] J. Reeves, AshwinRamaswamy, Michael Locasto, Sergey Bratus, Sean Smith "Intrusion detection for resource-constrained embedded control systems in the power grid Original Research Article" International Journal of Critical Infrastructure Protection, Volume 5, Issue 2, July 2012, Pages 74-83

[2] Book Chapter in the book "Multi-AgentSystems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9, InTech, April4, 2011

[3] CHAIB-DRAA : « Systèmesmultiagents : Versuneapprocheformellebaséesurl'action et l'interaction » Décembre 2009.

[4] A. Sayouti and H. Medromi. "Autonomous and Intelligent Mobile Systems based on Multi-Agent Systems".

[5] P. Kocher, et al., Security as a new dimension in embedded system design, in: 41st Design Automation Conference, 2004.

[6] Bo Sun; Osborne, L.; Yang Xiao; Guizani, S., "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications, IEEE , vol.14, no.5, pp.56,63, October 2007

[7] Esfandi, A., "Efficient anomaly intrusion detection system in adhoc networks by mobile agents," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on , vol.7, no., pp.73,77, 9-11 July 2010.

[8] Patrick Traynor, Kevin Butler, William Enck, Patrick McDaniel, Kevin Borders, "malnets: large-scale malicious networks via compromised wireless access points", Journal of Security and Communication Networks, Special Issue on Security in Mobile Wireless Networks, Vol. 3, Issue 2-3, June 2010.

[9] AvielMagnezi, "The Naval Disaster Report", ynet 01/07/14 http://www.ynet.co.il/articles/0,7340,L-3980739,00.html.

[10] YAAKOV KATZ 06/12/2012 "IDF encrypting more drones amid hacking concerns" http://www.jpost.com/Defense/IDF-encrypting-more-drones-amid-hacking-concerns.

[11] SIOBHAN GORMAN, YOCHI J. DREAZEN and AUGUST COLE Dec. 17, 2009 "Insurgents Hack U.S. Drones" http://online.wsj.com/news/articles/SB126102247889095011

[12] CNN Wire Staff, "Obama says U.S. has asked Iran to return drone aircraft", http://www.cnn.com/2011/12/12/world/meast/iran-us-drone

[13] BenfanoSoewito et al. / International Journal of Engineering Science and Technology (IJEST)

[14] Nathan Tuck et al. "Deterministic Memory-Efficient String Matching Algorithms for Intrusion Detection",

[15] O. Kachirski, R.K. Guha, Effective intrusion detection using multiple sensors in wireless ad hoc networks, in: Proceedings of HICSS, 2003, 57 pp.

[16] M. Fisk, G. Varghese, Fast content-based packet handling for intrusion detection, Tech. Rep. CS2001-0670, Department of Computer Science, University of California, San Diego, May 2001.