Design, Development and Implementation of a Network Intrusion Detection Tool for Air Traffic Management Systems

Nicolas Larrieu, Theobald de Riberolles, Guthemberg Silvestre

Design, Development and Implementation of a Network Intrusion Detection Tool for Air Traffic Management Systems

Nicolas Larrieu
ENAC
Toulouse, France

Theobald de Riberolles
Activus Services
Toulouse, France
theobald.deriberolles@activus-services.fr

Guthemberg Da Silva Silvestre
ENAC
Toulouse, France

***Abstract*—An Air Traffic Management (ATM) relies on a set of critical systems composed of control centers, sensors, communication means and radio navigation systems. These critical systems may be subject to different attacks and thus compromise their security. Indeed as there is a desire to open this system more and more outward and there is a gap between this world and the interconnected world, threats are increasing. The ATM system have particular characteristics as the fact that it is a very distributed system with a lot of real-time applications using proprietary and/or legacy protocols. Thus, the need to have an efficient Intrusion Detection System (IDS) is primordial in terms of reliability (a false negative rate as low as possible) and relevance (a lowest possible false-positive rate). The development of an IDS combining misuse detection (i.e., defining attack scenarios and finding traces of these scenarios in the traffic.) and anomaly detection (i.e., the construction of a reference model of the behavior of the supervised entity to which we will be able to compare the observed behavior) based on wavelet theory is a promising approach as they are already shown for this type of systems. The detection capability for such complex system could be enhanced using the specific characteristics of its exchanges, use them to enrich its normal signature and reduce the probability of false positive and false negatives.**

This paper describes the context and the state of the art of the current research direction of the authors with the aim to present the challenges and the future works that the student aims to perform in the next years.

***Index Terms*—Anomaly detection, intrusion, IDS, ATM**

I. Introduction

Areas such as the military, health or civil aviation are deploying more and more critical applications in their communication network. The security of these systems is therefore an essential issue. The objectives of this security are confidentiality, integrity and availability. As defined in [1]: An intrusion is a violation of one of these three objectives, and therefore exhibits a different behavior than the normal behavior of a system. An attack is an attempt to violate the system's security policy. The purpose of intrusion detection and prevention is to report intrusions or attacks to the security administrator so that the security administrator can take appropriate action.

DSNA (Direction des Services de la Navigation aérienne), the French ANSP (Air Navigation Service Provider), relies on a set of control centers (en-route, approaches, control tower), sensors (radars, multilateration systems, etc.), communication means (centers, air traffic control and management) and radionavigation systems, distributed throughout the territory (metropolitan and ultra-marine) to ensure its missions of control and management of air traffic. A private computer network connects the centers to each other and allows the exchange of large amount of data in a non-centralized way between the different elements constituting the monitoring and control system. These critical systems are increasingly open to the outside world to facilitate the exchange of data and information retrieval. Thus there is a need for secure these informations exchanges from intrusions and attacks in the most efficient way.

The work of this thesis focuses on the definition of an intrusion detection method specifically design for air traffic management (ATM) systems.

The paper is organized as follows. Section II presents the background and related work, Section III presents the stakeholders of the work, while in section IV we describe the problematic of the thesis.Finally, Section V summarizes some key aspects and defines the future works.

II. Related works

In intrusion detection, according to Chandola et al. [2] there exist two main approaches: the signature approach (misuse detection) and the behavioral approach (anomaly detection).

The signature approach consists of defining attack scenarios and looking for signatures of these attacks in data exchanges. This approach is ineffective when dealing with new attacks because their signatures are unknown.

The behavioral approach is the capability to build a reference model, called normal, of the monitored system and to compare it with the observed behavior. The differences between the two raise an alert to report an anomaly and a potential intrusion. It is not easy, however, to define what

may be representative of the normal behavior of a system, and thus these methods often generate a large number of false positives or false negatives as the approach is under-fitting.

This limit can nevertheless be circumvented when the data flows are from specific networks for which we have a very good knowledge of the characteristics of the traffic exchanged on the latter is possible. This is particularly the case for industrial networks for which all the data flows exchanged are mapped accurately and explicitly, and where the data exchanges should be invariant over time (or with identifiable patterns, for example over a day or a week. Network traffic within DSNA systems falls into this category. As such, it is conceivable to propose intrusion detection techniques based on behavioral tools. These should help to detect attacks on the specific traffic that is exchanged in and between the various en-route control centers of air navigation (CRNA) and the control centers present in each French airport.

The specificities of the DSNA traffic (statistical determinism in particular) make it possible to use intrusion detection methods based on statistical analysis which gives very good results on deterministic and invariant traffic.

Several research studies have been conducted for traffic characterization using spectral analysis. We can highlight, signature-based detection techniques based on statistical methods such as wavelets [3], Kalman filters [4], hashing projection [5], [6], principal component analysis (PCA) [7] [8] or pattern recognition [9]. Several of these earlier works deal with the classification of anomalies using events detected with a limited set of signatures (less than 10) [10], [11] . The method presented in [12] seems promising because adapted to any type of network traffic and seems to bring very interesting results for the rest of this thesis work. The authors demonstrated how Long Range Dependence (LRD) can be an efficient parameter to quantify the level of variability of Internet traffic. They used wavelet analysis, via a toolbox, to process data traffic. Thanks to this method, they obtain the variability level of any data series for different time scales and different moments of analysis.
In our work, we will use a version of the method introduced in [13] developed by H. Wendt more recently called Wavelet Leader Multi-fractal (WLM) analysis wich already show efficient results in terms of false positives/false negatives with a system with a similar characteristic, a drone fleet. [14].

III. Stakeholders

This part presents the roles and responsibilities of each stakeholders in the work.

A. Activus Services

ACTIVUS-Service is a digital service company operating in the information systems consulting sector in several IT domains. It is developing an internal project called Connect'it with the aims to design and develop, among others, a network monitoring solution. Part of ACTIVUS-Services' research and development work revolves around the centralization of network data as well as the detection of anomalies in these networks.

With its experience in the application of behavioral methods, the work with ACTIVUS-Services is to test and implement these methods by focusing on network data in order to generate relevant alerts for the user. This is done in a Big Data context that is to say using technologies allowing the real time processing of a large volume of data. ACTIVUS-Services software solution expertise will integrate work into a Connect'it industrial systems and networks monitoring module.

B. DSNA

For air transport management, the International Civil Aviation Organization (ICAO) and Air Navigation Service Providers (ANSP) have put in place dynamic air traffic management which is the space based on highly interconnected systems. In France, the DSNA (Direction des Services de la Navigation Aérienne) has the role of ANSP. It is one of the components of the DGAC (Direction Générale de l'Aviation Civile).
The DSNA provides the network traffic records from the air traffic control and management systems as well as the contextual elements for analyzing these records.

C. ENAC

ENAC (Ecole Nationale de l'Aviation Civile), a french engineering school, has a teaching program for the security of information systems and a privileged link with the aeronautical field. The ReSCo (networks and systems communicating) research team has expertise in the field of network security applied to aeronautical networks but also civil aviation. In addition, the ReSCo team is working on various research problems with security problems during exchanges between aircraft in flight. It has solid expertise in the field of onboard aeronautical networks and in the various traffics that can be exchanged between an aircraft and the various ground communication systems of French and European air navigation.

IV. Problem Formulation

The presence of exchanges between old and/or proprietary protocols with newer protocols, and the large amount of data to be processed in real time in an ATM network means that intrusion detection for this type of network raises new challenges. Indeed, according to the DSNA, classical methods do not show sufficiently satisfactory results for the criteria of civil aviation. This part, express the difficulties related to anomalies detection and the particularities of the aeronautical environment for this subject.

1) Anomaly Detection: The methods to detect anomalies are based on the observation of numerous of events and on the analysis of these. We need to collect data and to analyze them to find traces of intrusions and / or anomalies. This analysis can be done in several ways: after the facts, almost real-time or in real time. One goal of our work is to get an intrusion detection system that responds to criteria express by the DSNA:

- A criterion of reliability of the system: any intrusion must rise an alert which corresponds to a false negative rate as low as possible.
- A criterion of relevance of the alerts: any alert must correspond to an effective intrusion which corresponds to a false-positive rate as low as possible.

Then, the goal is to detect intrusions properly in DSNA networks for air traffic control. These networks are critics and as a result, they are eager to detect intrusions as early as possible to prevent further damage. However, the amount of network traffic generated by ATM can be a large amount of bytes per day, requiring extremely efficient methods of analysis to maintain a reasonable detection time and the use of centralized IDS to obtain efficient results. In this context, we conduct research in models to detect intrusions in real time. Several modeling methods and attributes are explored and combined to obtain relevant data processing. Based on the work of statistical models [2], [15], [16], [17], neural networks [15], immunological approach [18], basic graph [19], unsupervised approach [15], [19], we are working on the development of a better anomaly detection model to respond to the criteria express by the DSNA.

2) Aeronautical: One of the particularities of data exchange in the DSNA ATM system is the use of many proprietary and/or old protocols, but also the statistical determinism of these exchanges. Indeed, they exhibit characteristics relatively stable and have cyclic dynamics. This determinism is induced by the repetitive nature of the various aeronautical movements, which is reflected in the information from the sensors (radars) as well as in the processing subsystems of the flight plans. Thus, there will be recognizable and regular variations in air traffic that will have an impact on the data traffic. This repetitive nature present in the network makes it possible to envisage the use of algorithms based on behavioral approach to detect events that would be abnormal. This unsupervised methodology is different to the more traditional method, since it does not require upstream definition of attack signatures. By using the reproducibility of events in time, we will define a nominal behavior. This nominal signature will then be a basis to which we will compara collected data to highlighting abnormal behavior and therefore intrusion attempts.

The aim of this thesis work is to establish a link between the spectral characterization works (based on wavelet analysis) and the behavioral intrusion detection algorithms being developed for Connect'it. In particular, we are considering the development of a new detection module that would rely on the analytics methods presented in the previous paragraph and use these as inputs for the wavelet analysis. This method should answer to the requests for efficiency, stability and adaptability from the DSNA

V. Work in progress

In our future work, we intend to identify several research perspectives. First of all, we plan to propose an evolution of the WLM model adapted to our system to have a better characterization of the traffic analyzed. Moreover, we plan to analyze different types of traffic: first only radar data caracteristics of ATM system then also other traffic present in ATM system to enrich our bank of knowledges. To address these last objectives, we would like to consider experiments with real traffics from DSNA.

A. Intrusion Detection Methodology

This first step is dedicated to traffic characterization. The objective is to get a specific signature of the traffic we want to analyse. It is possible with the Wavelet Leader Multi-fractal (WLM) analysis.

The WLM analysis is used to quantify the variability of any time series, as a series of networks, that we want to characterize. With this method, we are able to capture the complexity of the traffic for different time scales and analysis times. The result of this analysis is a graph (called spectral signature) that allows us to visually see the difference between legitimate traffic and traffic that contains an attack. Using this WLM methodology, we are able to quantify the variability of any time series from two complementary parameters: the time scale and the time of the analysis. The time scale allows us to see any repetition in the process over time, while the analysis time allows us to analyze the traffic data in different spectral representations. This second metric quantifies the traffic variation according to, for example, q = 1 (mean), q = 2 (variance) and so on.

With this method, we are able to highlights differences between different analyzed traffics and these differences are useful for traffic characterization.

B. Characterization of data radar

As a first step to our IDS for ATM, we decide to work with data radar provided by DSNA. These data are considered as characteristic of an ATM system. They are the most stable data, but also those they represent perfectly the cyclic determinism of network data caused by the repetitive nature of the different aeronautical movements. Moreover, they are part of the essential data for the proper functioning of the ATM system, which makes them very critical. They are also intended to be increasingly exchanged with partners and the outside world to share information as air routes, flight tracking. It is therefore interesting at first to focus on the characterization and profiling of this type of network data.

To realize this characterization, we conduct two types of analysis concerning these data:

- The first is an exploratory data analysis (EDA) of about two weeks of actual traffic data collected from different radars. The results of this first analysis will allow us to better understand the analyzed traffic. Then we can compare it with other types of traffic, and get an idea of the specificity / difficulty of using anomaly detection tools applied to this type of generic traffic.
- The second analysis, with the same data, is a traffic signature identification using a spectral analysis (with the WLM analysis methodology explained in the previous paragraph). It represents a normal signature to which other potentially corrupted data signatures can be compared.

With this characterization, we will be able to generate false or corrupted radar data and inject them into real traffic. With the comparison of the spectral analysis of the normal traffic and the corrupted one, we will can see visually the consequences of intrusions and thus see cases and conditions where we can raise alerts.

The results of these first works will be a first step towards designing a future and effective IDS for ATM. After the radar study, we will be able to use our methodology on other data, as flight plan data, flight information data or other critical data from ATM systems. Once, the characterization of these data will be done, one challenge will to analyze traffic with all these mixed data and be able to raise alerts when there are effective intrusions. The final challenge will be to use our module directly plug to ATM system and have effective results in real time.

REFERENCES

[1] M. AMAND and M. NSIRI, "Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire," *Rapport de projet LENAC*, 2011.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[3] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement*. ACM, 2002, pp. 71–82.

[4] A. Soule, K. Salamatian, and N. Taft, "Combining filtering and statistical methods for anomaly detection," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*. USENIX Association, 2005, pp. 31–31.

[5] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, "Sketch-based change detection: methods, evaluation, and applications," in *Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement*. ACM, 2003, pp. 234–247.

[6] D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K. Salamatian, "Anomaly extraction in backbone networks using association rules," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 6, pp. 1788–1799, 2012.

[7] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in *ACM SIGCOMM Computer Communication Review*, vol. 34. ACM, 2004, pp. 219–230.

[8] Y. Kanda, R. Fontugne, K. Fukuda, and T. Sugawara, "ADMIRE: Anomaly detection method using entropy-based PCA with three-step sketches," *Computer Communications*, vol. 36, no. 5, pp. 575–588, 2013.

[9] R. Fontugne and K. Fukuda, "A Hough-transform-based anomaly detector with an adaptive time interval," *ACM SIGAPP Applied Computing Review*, vol. 11, no. 3, pp. 41–51, 2011.

[10] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in *ACM SIGCOMM Computer Communication Review*, vol. 35. ACM, 2005, pp. 217–228.

[11] B. Tellenbach, M. Burkhart, D. Schatzmann, D. Gugelmann, and D. Sornette, "Accurate network anomaly classification with generalized entropy metrics," *Computer Networks*, vol. 55, no. 15, pp. 3485–3502, 2011.

[12] P. Borgnat, G. Dewaele, K. Fukuda, P. Abry, and K. Cho, "Seven years and one day: Sketching the evolution of internet traffic," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 711–719.

[13] P. Abry, D. Veitch, and P. Flandrin, "Long-range Dependence: Revisiting Aggregation with Wavelets," *Journal of Time Series Analysis*, vol. 19, no. 3, pp. 253–266, 1998.

[14] J.-P. Condomines, R. Chemali, and N. Larrieu, "Network intrusion detection system for drone fleet using both spectral analysis and robust controller/observer," in *AeroConf 2018, 39th IEEE Aerospace Conference*, 2018.

[15] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, "Outlier detection for temporal data: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2250–2267, 2014.

[16] A. Kejariwal, "Twitter Engineering: Introducing practical and robust anomaly detection in a time series [Online blog], 2015," *URL http://bit. ly/1xBbX0Z*.

[17] N. Laptev, S. Amizadeh, and I. Flint, "Generic and scalable framework for automated time-series anomaly detection," in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2015, pp. 1939–1947.

[18] S. Ahmad and S. Purdy, "Real-Time Anomaly Detection for Streaming Analytics," *arXiv preprint arXiv:1607.02480*, 2016.

[19] T. Pham and S. Lee, "Anomaly detection in bitcoin network using unsupervised learning methods," *arXiv preprint arXiv:1611.03941*, 2016.