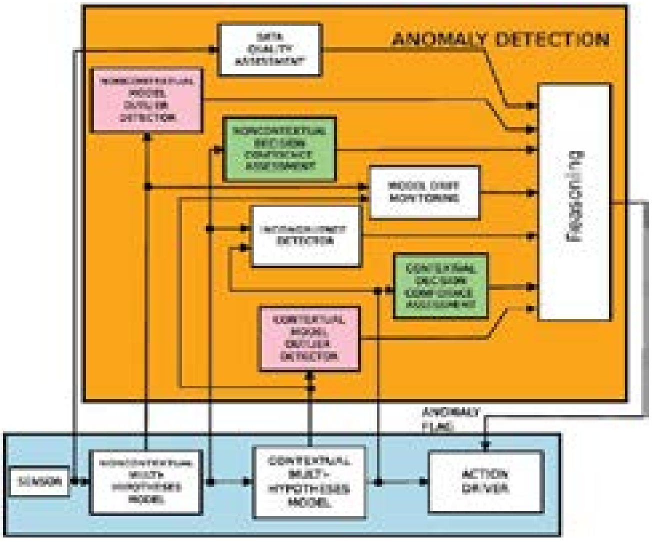
University Defence Research Collaboration in Signal Processing

LSSC Consortium White Paper

Statistical Anomaly Detection in Communication Networks

Introduction

Cyber-security is something that affects Internet users every day. Providing strong and reliable security mechanisms has become imperative in all areas, but it becomes especially critical in the context of networked national security, as parts of its core infrastructure are constantly targeted by cyber-attacks. The implementation of monitoring tools, such as Network Intrusion Detection Systems (NIDSs), is fundamental in security infrastructures in order to provide an extra level of assurance. The use of data mining and data fusion techniques has contributed to increase the efficiency of the NIDSs. However, as the complexity of cyber-attacks keeps increasing, new and more robust detection mechanisms need to be developed.


ANOMALY DETECTION
DATA QUALITY ASSESSMENT
NONCONTEXTUAL MODEL OUTLIER DETECTION
NONCONTEXTUAL DECISION CONFIDENCE ASSESSMENT
MODEL DRIFT MONITORING
INCONGRUENCY DETECTION
CONTEXTUAL DECISION CONFIDENCE ASSESSMENT
CONTEXTUAL MODEL OUTLIER DETECTION
Reasoning
ANOMALY FLAG
SENSOR
NONCONTEXTUAL MULTI-HYPOTHESES MODEL
CONTEXTUAL MULTI-HYPOTHESES MODEL
ACTION DRIVER

Current NIDSs utilise only measurable network traffic information from the protected system or signatures of known attacks during the intrusion detection process, but these systems do not take into account available high-level contextual information (i.e. above the network operation) regarding the protected system to improve their effectiveness. The next generation of NIDSs should be designed incorporating reasoning engines supported by modules that could assess the quality of the analysed datasets, manage contextual and non-contextual information about the network, or deal with incongruent decisions between different NIDSs. We have developed at Loughborough University [1] a novel methodology that allows incorporating contextual information into the detection process of our NIDS.

Method

Our starting point is an unsupervised anomaly-based NIDS developed at Loughborough University [2] tailored to detect different types of injection attacks in IEEE 802.11 wireless networks, and able to operate in real-time. This system makes use of metrics from multiple layers of the TCP/IP stack to produce a collective decision on the presence of attacks. The Dempster-Shafer Theory of Evidence, which is used as the data fusion technique, is provided with a novel Basic Probability Assignment (BPA) methodology able to automatically adapt the assignment of its evidences to the current characteristics of the network traffic, without intervention from a NIDS administrator.

EPSRC
Engineering and Physical Science Research Council

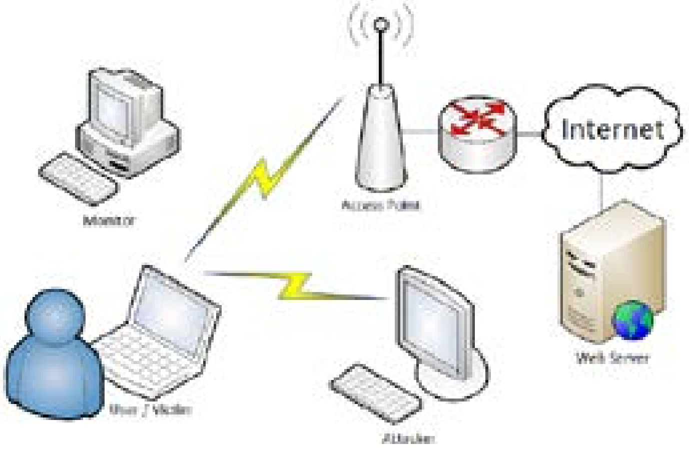
[dstl]

UDRC

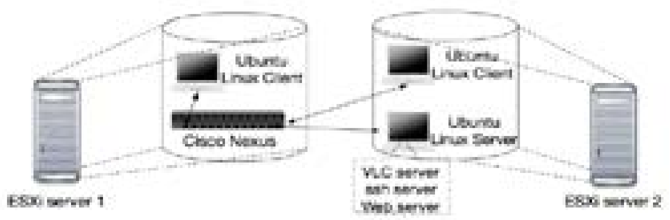
We have developed a novel approach [3] to automatically generate labelled network traffic datasets. This approach is based on the statistical characteristics of the outcome of our anomaly-based NIDS. The resulting labelled datasets are subsets of original unlabelled datasets. The labelled datasets can then be used:

- To create new rules to train supervised NIDSs
- To evaluate the efficiency of NIDSs
- To aid in Feature Selection tasks

We processed the labelled dataset, using a Genetic Algorithm based approach, to automatically provide a set of input metrics that generate the most appropriate intrusion detection results for the evaluated scenario.



Current efforts have focused on incorporating available high-level information into the intrusion detection process to improve their detection results:



- Contextual information
- Situational awareness
- Cognitive information

We have proposed different approaches [1] by which the network administrator and users would provide this high-level information by the use of Fuzzy Cognitive Maps (FCMs). A FCM provides a useful framework for network users to contribute their knowledge, to model new and unseen situations, and to represent unknown behaviours. Also, a FCM allows calculating the influence that each individual event may have in the whole system and in other events. The experimental results empirically confirm that by considering the contextual information through the use of a FCM, the efficiency of our NIDS can be improved.

As for future work, we wish to contribute with new techniques and methods that could increase the efficiency of the NIDSs. For instance, we will investigate new methods to include high-level information into the intrusion detection process (e.g. Ontologies), and investigate new methods to handle uncertainty.

References:

[1] K.G. Kyriakopoulos, F.J. Aparicio-Navarro, and D.J. Parish, “Manual and automatic assigned thresholds in multi-layer data fusion intrusion detection system for 802.11 attacks,” in IET Information Security, vol.8, no.1. 2014. pp. 42-50.

[2] F.J. Aparicio-Navarro, K.G. Kyriakopoulos, and D.J. Parish, “Automatic dataset labelling and feature selection for intrusion detection systems,” in Proc. of the Military Communications Conference (MILCOM), 2014, pp. 46-51.

[3] F.J. Aparicio-Navarro, K.G. Kyriakopoulos, D.J. Parish, and J.A. Chambers, “Adding contextual information to intrusion detection systems using fuzzy cognitive maps,” submitted to IEEE Int. Conf. on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016.