Lessons Learned from Robotics Applied to Cyber Security

Teresa Escrig
Cognitive Robots
ESPAITEC University Jaume I,
12071, Castellon, Spain

Sam Chung
Institute of Technology,
University of Washington,
Tacoma, WA 98402

ABSTRACT
An extensive research and development activity of almost twenty years in two fields of Artificial Intelligence - Robotics and Cognitive Vision, can bring new perspectives to Cyber Security field. At the beginning, there was a knowledge gap between the different fields that we needed to bridge. This paper is about the lessons learnt from Robotics that can be transferred into Cyber Security as wisdom to provide the basis for a holistic strategy to mitigate the severe and increasing Cyber Security problems.

General Terms
Cyber Security, Artificial Intelligence, Qualitative Models, Ontologies.

Keywords
Cyber Security, Common Sense, Qualitative Models, Data Visualization, Graph Databases, Ontologies.

1. INTRODUCTION
The Internet's takeover over the global communication landscape has been almost instant in historical terms (slightly over a decade): the Internet was commercialized in 1995, in 2000 it already communicated 51% of the information flowing through two-way telecommunications networks, and in 2007 more than 97% [1]. This fast growth has also created a huge problem of cyber security. Due to its urgency, the cyber security landscape consists of an ad hoc patchwork of solutions with no global satisfactory result. The current solutions have failed to prevent cybercrime or fraud losses, which amount to $100 billions of dollars each year. Computer attacks against the Pentagon currently average 5,000 each day. "Cyber-threat is one of the most serious economic and security challenges we face as a nation", declared by President Obama [2]. Existing security tools provide marginal protection "at best", i.e. if they are correctly used. Security management is in a state of profound change.

Cyber security is a very hard multifaceted problem for several reasons [3]:

- *It deals with complexity at all levels*: the Internet and the information infrastructure is a complex system of systems of hardware, software, operating systems, data, networks, and people. Failure in such an infrastructure can be so complex that no one can determine the cause or the cure.
- *It transfers immense amounts of data*: an estimated of 72 Giga Bytes a year for each person on Earth.
- *There are problems converting data to knowledge*: cyber security decisions require converting data into information and hence into knowledge. Current systems cannot create knowledge. They rely on decisions by humans who cannot respond at computer speeds of milliseconds or less.
- *There are many practical constraints, such as* protection of private information; appropriate handling of imperfect data (errors, incompleteness, inconsistency, and noise); usability and cost effectiveness; facilitation of open source software use, parallelism, debugging, and software quality assurance; and enabling of multilanguage development.
- *The perimeter defenses are* inadequate: traditional cyber security approaches focus on a layered defense, which is ineffective against malicious insiders.
- *More and smarter attacks* are happening every day.

Because of those reasons, a grand-challenge-class of R&D is necessary to address these long-standing and increasingly severe issues in cyber security [4]. There is an extraordinary need for a holistic solution to the cyber security problem, which includes more intelligence. Artificial Intelligence (AI) seems to be the research field that can provide such a holistic solution [6, 7]. However, AI has extensively been used for cyber security for over 20 years [7].

An Intrusion Detection System (IDS) monitors the events that take place in a computer system or computer network, and analyzes them for signs of attempts to compromise information security, or to bypass the security mechanisms of a computer or network [5, 7]. AI has been used for both approaches to IDS - Anomaly Detection (AD) and Misuse Detection (MD) [7]. For AD, several AI methods have been used: statistical models [8, 9], expert systems [10], and neural nets [11], among others. For MD, other AI methods have been used: rule-based languages [12], Petri automata [13], and genetic algorithms [14]. The main drawbacks of the AI techniques used in IDS are that, although they provide good results for some aspects of the problem, they are not scalable, they do not focus on the problem as a whole, and some of them act as "black boxes," in the sense that they provide solutions with no explanation that can help to justify decisions or report results. Moreover, IDS are passive techniques, which do not do anything to stop attacks.

With the intent of overcoming some of the IDS drawbacks, the emerging technology of Intrusion Prevention Systems (IPS) is appearing. IPS is proactive and functions as radar to monitor the stream of network traffic, detecting, identifying and recognizing patterns of security violation, preventing the attack before it happens [15].

To be effective, cyber security solutions need to:

- **Obtain automatic knowledge from data**. Converting raw data into information (data in the context of other data) and hence into knowledge (information in the context of other information) is critical to support automatic decision

processes and predictions. Knowledge-based decisions cannot process arbitrary instructions and therefore are not hackable [3].

- **Process network traffic Big Data in real-time.**
- **Include intelligence** to automatically identify not only known attacks but also suspicious activity, which might correspond to new attacks.
- **Provide evidence or explanation on the decision** that a suspicious Internet activity corresponds to a new unknown attack. A solution based on a black box is not acceptable.
- **Scalable**, meaning that the solution provided for a part of the Internet system should be straightforwardly extended to provide a solution for the whole system.

Experts at CMU such as Dr. Morel [6] argue that cyber security calls for new and specific AI techniques developed with the cyber security application in mind. He advocates for the use of Knowledge Based Systems *(representation)*, Probabilistic *(reasoning)*, and Bayesian *(learning)*. Representation, reasoning, and learning are indeed the basic principles of human intelligence, and therefore necessary to provide a holistic solution to cyber security. However, probabilistic and Bayesian models have extensively been used in other AI areas, such as Robotics and Computer Vision, with very good initial results, that have not been scalable.

The problems detected in the probabilistic approaches have been twofold: 1) it is a brute force method with high computational cost. And 2) no common sense, or any other cognitive approach, is being used to make sense of the numbers. Therefore after the first initial promising results, further improvements are limited.

In the same way that happened in the Robotics field, the type of knowledge that the cyber space needs to obtain is **common sense knowledge**, the one used by people in their daily life. Contra intuitively, common sense knowledge is more difficult to model than expert knowledge, which can be quite easily modeled by expert systems. The concept of common sense knowledge is introduced in Section 2.

Qualitative Models have been demonstrated to be the best approach to model common sense knowledge [16, 17, 18, 19, 20], by transforming incomplete and uncertain data from the environment into knowledge. The key concepts of qualitative representation and reasoning are introduced in Section 3.

Highly promising results have been obtained in the application of qualitative representation and reasoning models to provide the intelligence needed for Service Robots to be completely autonomous in non-structured unknown environments for autonomous map building, auto-localization, navigation, and high-level decision-making [21, 22]. A spin-off private corporation, Cognitive Robots (www.c-robots.com), has been created to exploit these pending-patent research results [23]. Section 4 includes a summary of the key components for the success of qualitative representation and reasoning to solve the main problems of robotics.

How can the wisdom learned in almost 20 years of research on the area of computing common sense reasoning for Robotics be transferred to the Cyber Security area? The first approach in this direction is introduced in Section 5.

2. WHAT IS COMMON SENSE KNOWLEDGE?

According to [24], AI is a field of science and engineering concerning the computational understanding of what is commonly called intelligent behavior, and with the creation of artifacts that exhibit such behavior. The artifacts can be physical (such as robots or other autonomous vehicles which show intelligence in the physical 3D world) and non-physical (such as software robots or other software "vehicles" which show an intelligent behavior in cyberspace).

There is a clear analogy between the physical space and the cyberspace: In the physical space people or intelligent vehicles can move, behave, interact, etc. In the cyberspace, people and software robots surf the web (visit places), interact with other people (chats), perform actions (buy books, rent movies, make bank transactions), etc.

A significant part of common sense knowledge encodes our experience with the physical world we live in [17, 24, 25, 26]. Common sense is defined both for human and computers as "the common knowledge that is possessed by every schoolchild and the methods for making obvious inferences from this knowledge" [26]. Commonsense reasoning relaxes the strongly mathematical formulation of physical laws.

The aquarium metaphor [18] illustrates the essence of the commonsense reasoning: two people situated close together are looking at an aquarium and they try to speak about how wonderful the fish are; they need to identify the fish by their relative position (Figure 1).

Fig 1: The aquarium metaphor: two people situated close together are looking at an aquarium and they try to speak about how wonderful the fish are.

Various resource limitations are found in formalizing common sense knowledge [19]:

- The amount of time for observation and object identification is limited: The fish are in motion.
- Perceptual resolution is limited (coarse knowledge).
- The perceivable features are limited (incomplete knowledge).
- The movement and muddiness of the water may prevent the observers from clearly recognizing the boundaries of the objects and relations (fuzzy knowledge).
- The observers are located at different positions, thus they may observe different spatial relations for the same situation (subjective knowledge).
- One observer can easily model how the observation of the other observer may deviate from the own observation (conceptual neighborhood of relations).
- The object description and identification task is strongly simplified since identification must be possible only in relation to this context (context-aided communication).

The aquarium metaphor emphasizes a few issues, which are present in all spatial perception, representation, and identification situations [19]:

- The perceptual knowledge is necessarily limited with regard to resolution, features, completeness, and certainty;
- There is a more or less well-defined context;
- Perceptions are finite;

- The neighborhood of objects and conceptual neighborhood of relations between objects provide very useful information for spatial reasoning.

Representation, reasoning and learning are the basic principles of human intelligence. The Concise Oxford dictionary defines the word "reason" as the intellectual faculty by which conclusions are drawn from premises. The human reasoning mechanism is efficient, robust and trustworthy enough to solve important problems and humans seem to just "pick it up without any effort" [25]. Complex situations are handled and the behavior of physical objects are predicted without having to solve the kind of differential equations that physicists would use to formally describe a physical situation [16]. Moreover, this type of adaptability and flexibility of the human reasoning process for incomplete knowledge has been defined formally and logically. The kind of reasoning that human beings rely on, based on commonsense knowledge in everyday situations, as well as in very specialized domains, is called commonsense reasoning [17]. Commonsense reasoning has, therefore, a certain degree of uncertainty.

3. WHAT IS QUALITATIVE REPRESENTATION AND REASONING?

The method most widely used to model commonsense reasoning in the spatial and temporal domains is qualitative models [16, 17, 18, 19, 20]. Qualitative models help to express poorly defined problem situations, support the solution process and lead to a better interpretation of the final results [19]. A qualitative representation can be defined [16] as that representation which makes only as many distinctions as necessary to identify objects, events, situations, etc. in a given context. i.e. **provides relevant information from the environment**.

Qualitative models are defined with three aspects [26]:

1) REPRESENTATION: What particular aspect of the world are we representing? For instance, the orientation of an object, c, with respect to (wrt) the reference system defined by two points, a and b, that is, c wrt ab. Orientation representation implies three objects, i.e. it is tertiary relationship. Representation also describes all the points of view in which we can perceive the information by using representation operations [27].
2) DOMAIN THEORY: Qualitative models express the kind of partial knowledge available in that context. A few examples of partial knowledge include comparison of size (smaller, bigger, equal), orientation (right, left-back, right-front, north, south, etc.), distance (close, closer, far, etc.), topological relations (contains, overlaps, etc.), and shape of objects (round, square, rectangular, triangular, etc.).
3) INFERENCE TECHNIQUES: Each qualitative model has a complete inference mechanism. Inference in AI refers to various processes by which programs, as opposed to people, draw conclusions from facts and suppositions [24]. The most common types of inference methodologies in AI are logical: classical (in which resolution forms a basis for logic programming of which PROLOG is an example) or non-classical. In Spatial Reasoning, the basic step of the inference process is usually implemented by tables [ESC98]. For example, for the concept of size, the inference process provides, given the relations "a is smaller than b" and "b is smaller than c", the relation "a is smaller than c". That is, the logical property of transitivity is used.

Qualitative representations are better on recognition tasks than on reconstruction tasks. Qualitative representations do not structure domains homogeneously (i.e. with uniform granularity of physical entities) as quantitative representations do; rather they focus on the boundaries of concepts: the representation may be viewed as having low resolution for different values corresponding to the same quality and high resolution near the concept boundaries [19]. Thus, qualitative representations may be viewed as regions from the viewpoint of quantitative representations.

Qualitative methods allow us to reason with partial information, and they have the following **advantages**:

- It might be expensive, time-consuming, or impossible to get complete information [26], thus a reduction of data without loss of information remains an important goal [18].
- Computing with exact information may be too complex [26].
- High-precision quantitative measurements are not as universally useful for the analysis of complex systems as was believed at the beginning of the computer age [18].
- Qualitative knowledge is robust under transformations [19].
- Reasoning with partial information allows the inference of general rules that apply across a wide range of cases [26]. Therefore, qualitative methods possess a higher power of abstraction [16], which can be viewed as that aspect of knowledge, which critically influences decisions [28].
- Qualitative representations handle vague knowledge by using coarse granularity levels, which avoid having to be committed to specific values in a given dimension. Only a refinement of what is already known is needed [16].
- Qualitative representations are independent of specific values and granularities of representation. In this way, qualitative representations allow for top-down approach to characterizing situations, in comparison to bottom-up approaches suggested by quantitative representation [19].
- The expressive power of qualitative constraints results from their interaction [19]. For example, the assertions "a is smaller than b" and "b is smaller than c", restrict the value of b to the values of the interval [a, c]. In the domain of real values, there are still an infinite number of quantities in this interval; however, if we further constrain the assertions to refer to a domain of discrete entities, the qualitative constraint may have the power of selecting small sets of quantities without directly addressing their value.
- While in the qualitative approach only a refinement of what is already known is needed, in conventional default reasoning approaches the false assumption has to be retracted and a potentially costly revision has to be carried out to take back facts derived from it.

However, qualitative methods have at least one **drawback**: qualitative representations are non-deterministic in the sense that they might correspond to many "real" situations [16]. However, the context in which this representation is given should constraint the relative information enough to allow reasoning.

Qualitative approaches have been extensively used for modeling physical phenomena, and temporal and spatial reasoning. Qualitative Models can be used in many application areas from everyday life in which spatial knowledge plays a role, particularly in those that are characterized by uncertainty and incomplete knowledge [16]. A survey of the techniques and applications on Qualitative Reasoning can be found in [20]. Our claim in this paper is that Qualitative Models can also play an important role in providing a better landscape of solutions for cyber security.

4. ANALOGY IN ROBOTICS TO TRANSFORM DATA INTO KNOWLEDGE

Although in a much smaller scale compared with the Internet, robot distance sensors (perception) provide huge amounts of numbers per second as the robot moves through its environment. For instance, a laser sensor situated on top of a robot will provide a vector of distances (and the corresponding angles) from the robot to the obstacles in the robot's environment (Figure 2) every few milliseconds. The data needs to be processed in real time for the robot to take proper decisions about its behavior to solve the task in hand.

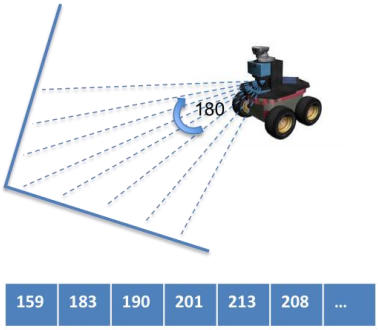

Fig 2: The laser sensor provides a vector of distances and angles every few milliseconds.

Using the qualitative approach of our analogy, instead of storing and handling all sensor data later, the relevant information is extracted in real time [21, 22, 23]. In this case, the relevant data corresponds to the point (distance and angle) where there exists a discontinuity. In our normal physical environments, the discontinuities correspond to concave and convex corners (Figure 3).

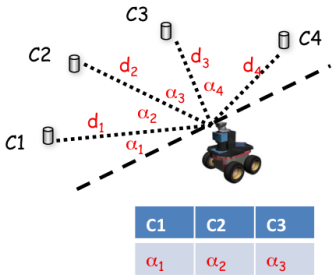

Fig 3: The quantitative representation of robot sensors is reduced into a qualitative representation of only the most relevant data of the environment, which normally corresponds to concave or convex corners (where Ci stands for the landmark name and α_i for its corresponding angle).

The qualitative representation uses a reference system (double cross with 15 spatial regions with their names or tags) to represent the spatial orientation of a landmark, i.e. *C1*, with respect to (wrt) the points *a* and *b* that forms the reference system, i.e. *C1 wrt ab*, as the region tagged as right-front (rf) (Figure 4).

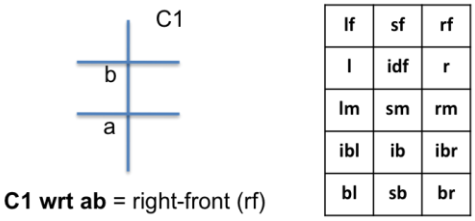

Fig 4: The qualitative representation of the landmark C1 wrt the reference system in doble cross formed by the points a and b on the robot, i.e. C1 wrt ab, is for example the region right-front (rf). Meaning of some of the regions: left (l), right (r), front (f), …

Qualitative Reasoning infers new knowledge from the knowledge already known, connecting the position of all the landmarks in the robot's environment (Figure 5).

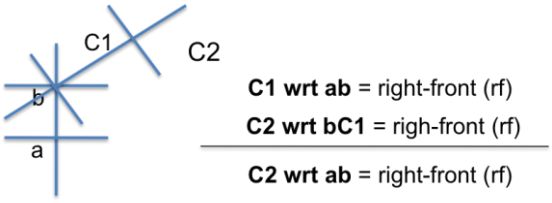

Fig 5: If we know the relationships *C1 wrt ab* and *C2 wrt bC1*, we can infer the relationship *C2 wrt ab*, using the qualitative reasoning proccess.

The above mentioned qualitative representation and reasoning processes have been used to generate reference systems, automatically create maps of unknown environments, localize the robot in them, navigate, etc. [23]. The level of abstraction of qualitative knowledge is so high that the robot can take decisions about the environment, which were not possible with the probabilistic approaches.

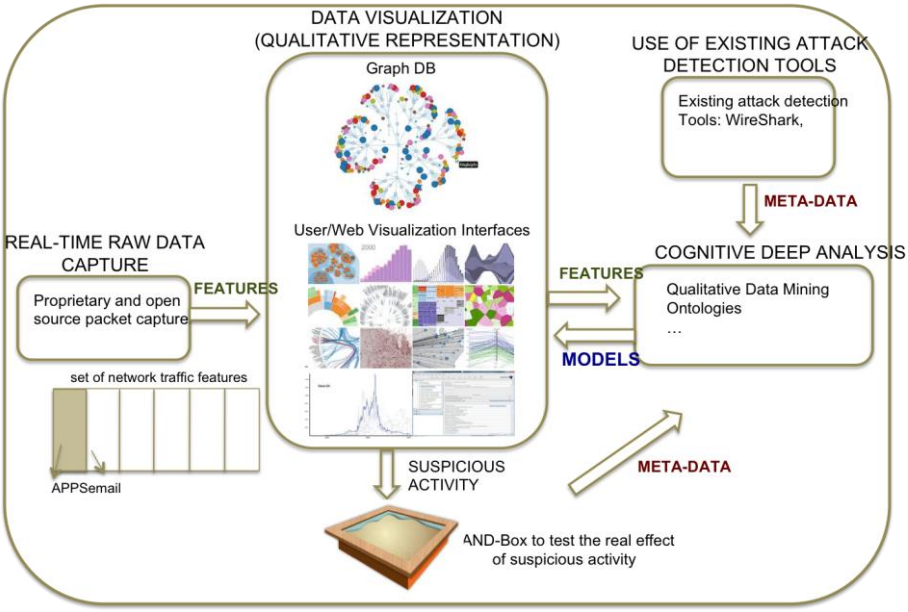

Fig 6: System architecture for Qualitative Smart Cyber Security

5. HOW TO TRANSFER THE WISDOM ACQUIRED IN ROBOTICS INTO CYBER SECURITY?

In the case of the robot, it is obvious that we cannot store the data and analyze it later to find out something important for the robot. However, this is the current approach for cyber security: storing the data (which of course becomes big data) to analyze it later. If something has happened, we will not know it on time!

In the approach we propose, first of all, we extract a qualitative representation of the raw network traffic data and obtain the relevant information in real time. The description of known attacks is used as a meta-data to help identifying general patterns of attacks, which automatically will generate general attack models (not signature based only). Traffic flow is constantly compared with those models in real time. Suspicious traffic might correspond to unknown attacks, which can affect critical aspects of infrastructure. They are tested in a sand box before they are executed in our real system to prevent attacks. Figure 6 shows the architecture of our approach.

Using an open source Internet traffic packet capture, the most relevant features related with different concepts like app, email, etc. are extracted. This feature selection is done manually and it will take several trials to tune. The qualitative representation is done in the Data Visualization module, which consists of representing the most relevant features with a graph database and visualize them with different web 3-D dynamic data visualization techniques. The result of this module is a particular representation of relevant features that feeds the module of Cognitive Deep Analysis together with the meta-data coming from the existing attack detection tools module. In the Cognitive Deep Analysis module, techniques of qualitative data mining [29, 30] and ontologies [31] are used to automatically create models of normal and abnormal behaviors corresponding to regular traffic data and cyber-attacks, respectively. The relevant features extracted in the Data Visualization module are constantly compared with the existing models of normal traffic and attacks. If there is a set of relevant features that doesn't correspond to any normal traffic or known attacks, it is classified as a suspicious activity. The traffic associated to a suspicious activity is tested in a sand box environment which reproduces the protected system without any dangerous consequence. The result of the test of the suspicious traffic data in the sand box (being an attack or normal traffic) corresponds to meta-data that feeds the Cognitive Deep Analysis module to automatically create new models of attacks or normal traffic data, respectively.

The graph database will allow us to represent large volumes of network traffic. The graph database technology chosen for this research is Neo4j [32] due mainly to its fast growing community of users. The system offers high-speed processing, configurable data entry from multiple sources, and the management of networks with billions of nodes and connections from a desktop PC. Users can quickly and easily identify interrelated records by formulating queries based on simple values such as names and keywords. Until now, this was possible to a certain extent using database technology, but Neo4j extracts new information from interrelated data and improves the speed and the capacity to perform complex queries in large data networks. The data visualization technique chosen for this research project is Data Driven Document (D3) [33] because it allows us to visualize real time data in web applications.

Beside qualitative models, the human body's immune system metaphor, introduced by Hibeli et al. [3], which describes how the human body's management of complexity and nonlinearity in the biological immune response can be transferred into digital immunity, provides a key component to provide scalable trustworthy systems. From an information-processing perspective, several immunological principles make the analogy appealing [3]: distributing processing and decentralized control, pathogenic pattern recognition, multilayered protection, diversity, and signaling

Combining the basics of human intelligence (Representation, Reasoning, and Learning) with Qualitative Models, and the Human-Physiology-Immunity Metaphor seems to be an

effective strategy towards a holistic solution to the global problem of cyber security.

6. CONCLUSIONS

Currently a machine or a network is extremely easier to attack than it is to defend. The cyber security field is clearly not effective. The most urgent aspects to improve in the cyber security area are:

- Obtaining automatic knowledge from data,
- Processing network traffic big data in real-time,
- Having more intelligence in the automatic network traffic analysis,
- Providing evidence or explanation on the decisions taken,
- The solution that we provide needs to be scalable.

Although many AI techniques have been applied to cyber security, there is no evidence of an approach that includes all the previous mentioned aspects. In the area of Robotics, qualitative models have been successfully applied to automatically implement human common sense. We argue that this success can serve as a fruitful analogy to provide, still a rough first intent towards a more holistic solution of cyber security. We are currently implementing the approach to prove the concept.

7. ACKNOWLEDGMENTS

This research has been supported by the Endowed Chair of Information Systems and Information Security of the Institute of Technology at the University of Washington Tacoma.

8. REFERENCES

[1] Martin Hilbert and Priscila López, The World's Technological Capacity to Store, Communicate, and Compute Information, Science, 11 February 2011, pp. 692-693.

[2] National Security Council, Cybersecurity, www.whitehouse.gov/administration/eop/nsc/cybersecurity, accessed on June 6, 2013.

[3] L. Hively, F. Sheldo, A. Cinzia-Squicciarini, "Toward Scalable Trustworthy Computing Using the Human-Physiology-Immunity Metaphor", IEEE Security & Privacy, Vol. 9, Issue 4, July-Aug 2011, pp. 14-23.

[4] F.T. Sheldon and C.A. Vishik, "Moving toward Trustworthy Systems: R&D Essentials," IEEE Computer, vol. 43, no. 9, September 2010, pp. 31–40.

[5] K.R. Karthikeyan and A. Indra, "Intrusion Detection Tools and Techniques – A Survey," International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010, pp. 901-906.

[6] B. Morel, "Artificial Intelligence a Key to the Future of CyberSecurity", 4th ACM workshop on Artificial Intelligence and Security (AISEC2011), October 21, 2011, Chicago, IL, USA, pp. 93-97.

[7] M. Pradhan, S. K. Pradhan, and S. K. Sahu, "A Survey on Detection Methods in Intrusion Detection Systems," International Journal of Computer Application, Issue 2, Volume 3, June 2012. pp. 81-90.

[8] Javitz, H., Valdes, A., "The NIDES Statistical Component Description and Justification", SRI International Annual Report, March 7, 1994.

[9] Bace, R. "Intrusion Detection," ISBN 1-57870-185-6, 2001.

[10] Axelsson, S., "Research in Intrusion-Detection Systems: A Survey," TR 98-17. Goteborg, Sweden: Department of Computer Engineering, Chalmers University of Technology, 1999. http://www.cs.unc.edu/~jeffay/courses/nidsS05/surveys/Axelson99-ids-survey.pdf

[11] Fox, K.L., Henning, R.R., Reed, J.H., Simonian, R.P., "A Neural Network Approach Towards Intrusion Detection," in NIST (Ed.) Proceedings of the 13th National Computer Security Conference, October, 1990.

[12] Lindqvist, U., Porras, P.A., "Detecting computing and networking misuse through the production-based expert system toolset (P-BEST)," in L. Gong & M. Reiter (eds.) Proceeding of the IEEE symposium on security and privacy, IEEE Computer Society, pp. 146-161, Los Alamitos, CA, 1999.

[13] Kumar, S, Spafford, E.H., "A pattern-matching model for misuse intrusion detection," In NIST (Ed.), Proceeding of the 17th National Computer Security Conference, National Institute of Standards and Technology (NIST), pp. 11-21, Baltimore, 1994.

[14] Ludovic, M., "ASSATA: A Genetic algorithm as an Alternative Tool for Security Audit Trails Analysis," RAID, 1998.

[15] Stiawan, D. et al. "Intrusion Prevention System: a Survey," Journal of Theoretical and Applied Information Technology, Vol. 40, No. 1. June 2012. pp. 44-54

[16] Hernández, D., Qualitative Representation of Spatial Knowledge. Lecture Notes in Artificial Intelligence. Vol. 804, Ed. Springer-Verlag, 1994.

[17] Stèpánková, O., "An Introduction to Qualitative Reasoning," Advanced Topics in Artificial Intelligence, Lecture Notes in Artificial Intelligence, Vol. 617, 1992, pp. 404-418.

[18] Freksa, C., "Qualitative Spatial Reasoning," in Mark, D.M., Frank, A.U. (eds.), Cognitive and Linguistic Aspects of Geographic Space, pp. 361-372, Kluwer Academic Publishers, Dordrecht, 1991.

[19] Werthner, H. Qualitative Reasoning: Modeling and the Generation of Behavior, Springer-Verlag, 1994.

[20] Dague, P., "Qualitative Reasoning: A Survey of Techniques and Applications," Artificial Intelligence Communications, Vol. 8, No. 3-4, 1995, pp. 119-192.

[21] Escrig, M.T., Peris, J.C, "The use of a Reasoning process to solve the almost SLAM problem at the Robocup legged league", Catalonian Conference on Artificial Intelligence, CCIA'05, 2005.

[22] Peris, J.C, Escrig, M.T., "Cognitive Maps for Mobile Robot Navigation: A Hybrid Representation Using Reference Systems", 19th International Workshop on Qualitative Reasoning, Graz, Austria, pp. 179-185, ISBN 3-9502019-0-4, Graz, Austria, 2005.

[23] Escrig, M.T., Peris, J.C., USA pending patent: "SYSTEMS AND METHODS FOR ESTABLISHING AN ENVIRONMENTAL REPRESENTATION", Cognitive Robots S.L. (www.c-robots.com), October 2010.

[24] Shapiro, E., (editor). Encyclopedia of Artificial Intelligence, Wiley, 1987.

[25] Kuipers, B., "Commonsense Knowledge of Space: Learning from Experience," Proceedings of the 6th International Joint Conference on Artificial Intelligence, pp. 499-501. Los Altos, California. Morgan Kaufman, 1979.

[26] Davis, E., "Commonsense reasoning," in [16], pp. 1288-1294, 1987.

[27] Escrig, M.T., Toledo, F., "Qualitative Spatial Reasoning: Theory and Practice. Application to Robot Navigation," IOS Press, Frontiers in Artificial Intelligence and Applications, ISBN 90 5199 4125, Amsterdam, 1998.

[28] Freksa, C. & Röhrig, R., "Dimensions of Qualitative Spatial Reasoning," In Qualitative Reasoning in Decision Technologies, Proc. QUARDET '93, N. Piera Carreté & M.G. Singh, eds., CIMNE Barcelona 1993, pp. 483-492.

[29] Bratko, I., Suc, D., "Qualitative data mining and its applications," Proceedings of the 25th International Conference on Information Technology Interfaces 2003 (ITI 2003), pp. 3-8.

[30] Zabkar, J., Mozina, M., Bratko, I., Demsar, J., "Learning qualitative models form numerical data," Artificial Intelligence, vol. 175, No. 9-10, June 2011, pp. 1604-1619.

[31] Mattos-Rosa, Th., Olivo-Santin, A, Malucelli, A., "Mitigating XLM Injection Zero-Day Attack through Strategy-based Detection system", IEEE Security & Privacy, June 2012.

[32] Neo4j Documentation, http://docs.neo4j.org/, accessed on May 13, 2013.

[33] Data-Driven Documents, http://d3js.org/, accessed on May 13, 2013