BDA-CS: Big Data Analytics in Critical Systems

Special session at EMERGING 2016, October 9 - 13, 2016 - Venice, Italy
http://www.iaria.org/conferences2016/EMERGING16.html

Chair and Organizer
Dr. William Hurst, Liverpool John Moores University, UK, W.Hurst@ljmu.ac.uk

The technology being used in critical infrastructure systems has become more intelligent and adaptive to providing efficient services. A product, of this cumulative modern-day use of information technology, is the generation of significant volumes of data. As such, analysing behaviour within big data sets in order to detect security anomalies is becoming progressively problematic. Movements towards the use of technologies, which enable high computation power and storage, such as cloud computing, bring your own device (BYOD) and service automation has resulted in new challenges for security systems.

There is a need to process data by using increasingly complex techniques to detect security breaches. Adaptive systems must be employed, and existing methods built upon, to provide well-structured defence in depth. The increase and sophistication of malware is now a concern for companies and governments.

The task of developing effective protection methods remains a demanding one. There are significant weaknesses in the existing security currently in place. The use of wireless communication technologies within infrastructures facilitates interconnections and the exchange of information. However, in result, weaknesses are further aggravated. Additional access points are introduced into already complex critical infrastructure systems.

In light of this, research has taken a trend towards the use of big data analytics in recent years. Techniques, such as machine learning and graph analysis, are now being investigated in order to support critical system security and process the big datasets being generated. The main challenge is that data sets are often unstructured and reside in imaging systems or '*silos*'. Real-time analysis can also result in network traffic being slowed by having to pass through a bottleneck.

To-date, there have been many tools and techniques developed for open source intelligence gathering and big data analysis in forensic and security investigations. However, the analysis of massively increasing data sets, distributed within cross platforms, often goes beyond geopolitical borders. This remains a real challenge in forensic investigations. Yet, sophisticated methods, concerning big data analytics, are required to address the technical challenges facing the law enforcement community in particular.

In light of the challenges discussed above, this special session invited authors to submit high-quality research papers on emerging big data analytics in critical systems (BDA-CS), covering topics which include (but are not limited to) the following:

- Critical Infrastructure Data Analytics
- Cyber Security
- Forensics
- Intelligent gathering
- Big Data Analytics
- Simulation
- Machine Learning
- Intrusion Detection
- Control Systems
- Cloud Computing
- Data Fusion
- Web Services

The protection of critical systems a key issue for modern day security. As the volume of cyber-threats increase, security may lie away from conventional computer security techniques. An original approach to protection is required. Improving the level of support and increasing awareness through big data analytics is key to the well-being of people and the evolution of critical infrastructure security levels. As such, the contents of this section session include 4 papers which are organised as follows.

---

1. MICRO-CI: A Testbed for Cyber-Security Research

William Hurst[1], Nathan Shone[1], Qi Shi[1] & Behnam Bazli[2]
[1] Department of Computer Science, Liverpool John Moores University, UK
[2] School of Computing, Staffordshire University, UK

Abstract— A significant challenge for governments around the globe is the need to improve the level of awareness for citizens and businesses about the threats that exist in cyberspace. The arrival of new information technologies has resulted in different types of criminal activities, which previously did not exist, with the potential to cause extensive damage. Given the fact that the Internet is boundary-less, it makes it difficult to identify where attacks originate from and how to counter them. The only solution is to improve the level of support for security systems and evolve the defences against cyber-attacks. This project supports the development of critical infrastructure security research, in the fight against a growing threat from the digital domain. However, the real-world evaluation of emerging security systems for Supervisory Control and Data Acquisition (SCADA) systems is impractical. The research project furthers the knowledge and understanding of Information Systems; specifically acting as a facilitator for cyber-security research. In this paper, the construction of a testbed and datasets for cyber-security and critical infrastructure research are presented.

---

2. A Cyber-Support System for Distributed Infrastructures

Sahar Badri[1], Paul Fergus[1], William Hurst[1]
[1] Department of Computer Science, Liverpool John Moores University, UK

Abstract— The Internet is now heavily relied upon by the critical infrastructures (CI). This has led to different security threats facing interconnected security systems. By understanding the complexity of critical infrastructure interdependency, and how to take advantage of it in order to minimize the cascading problem, enables the prediction of potential problems before they happen. Our proposed system, detailed in this paper, is able to detect cyber-attacks and share the knowledge with interconnected partners to create an immune system network. In order to demonstrate our approach, a realistic simulation is used to construct data and evaluate the system put forward. This paper provides a summary of the work to-date, on the development of a system titled Critical Infrastructure Auto-Immune Response System (CIAIRS). It provides a view of the main CIAIRS segments which comprise the framework and illustrates the functioning of the system.

---

3. Smart Monitoring: An Intelligent System to Facilitate Health Care across an Ageing Population

Carl Chalmers[1], William Hurst[1], Michael Mackay[1] & Paul Fergus[1]
[1] Department of Computer Science, Liverpool John Moores University, UK

Abstract— In the UK, the number of people living with self-limiting conditions, such as Dementia, Parkinson's disease and depression, is increasing. The resulting strain on national healthcare resources means that providing 24-hour monitoring for patients is a challenge. As this problem escalates, caring for an ageing population will become more demanding over the next decade. Our research directly proposes an alternative and cost effective method for supporting independent living that offers enhancements for Early Intervention Practices (EIP). In the UK, a national roll out of smart meters is underway, which enable detailed around-the-clock monitoring of energy usage. This granular data captures detailed habits and routines through the users' interactions with electrical devices. Our approach utilises this valuable data to provide an innovative remote patient monitoring system. The system interfaces directly with a patient's smart meter, enabling it to distinguish reliably between subtle changes in energy usage in real-time. The data collected can be used to identify any behavioural anomalies in a patient's habit or

routine, using a machine learning approach. Our system utilises trained models, which are deployed as web services using cloud infrastructures, to provide a comprehensive monitoring service. The research outlined in this paper demonstrates that it is possible to classify successfully both normal and abnormal behaviours using the Bayes Point Machine binary classifier.

---

4. Impact of Topology on Service Availability in a Smart Grid Advanced Metering Infrastructure

Bashar Alohali[1], Kashif Kifayat[1], Qi Shi[1], William Hurst[1],
[1] Department of Computer Science, Liverpool John Moores University, UK

Abstract— Over the last decade, Wireless Sensor Networks (WSNs) have brought radical changes to the means and forms of communication for monitoring and control of a large number of applications including Smart Grid (SG). Traditional energy networks have been modernized to Smart Grids to boost the energy industry in the context of efficient and effective power management, performance, real-time control and information flow using two-way communication between utility provides and end-users. However, integrating two-way communication in smart grid comes at the cost of cyber security vulnerabilities and challenges. In the context of SG, node capture is a severe security threat due to the fact that a compromised node can significantly impact the operations and security of the SG network. In this paper, node compromise attack is explored on Advance Metering Infrastructure (AMI) with smart meters for Neighbor Area Networks (NANs) in star and mesh network topologies. Simulation of node compromise/failure for a SG network, using ZigBee nodes in simulation indicates that a partial mesh topology is more resilient to node capture attacks as compared to star topology. A larger number of nodes are reachable from the control center of the SG in a partial mesh topology compared to that in a star topology.