ISCRAM 2019

LETSCROWD: Dynamic Risk Assessment for Mass Gatherings

C. Dambra (ZenaByte), J. Arias Martí (ETRA)

letsCROWD

Introduction

This work proposes an innovative approach to dynamically assess the risks for the crowd during mass gathering events.

Dynamic Risk Assessment (DRA) is necessary to update the risk for the crowd in the critical time frame from the event planning to the event execution.

Methods

DRA bases its reasoning on the receipt and processing of **Weak Signals** (WS) inspired by network Intrusion Detection Systems (IDS) approaches.

Each received WS has a **unique ID** and has associated a **time signature**, **location** and a **significance** value.

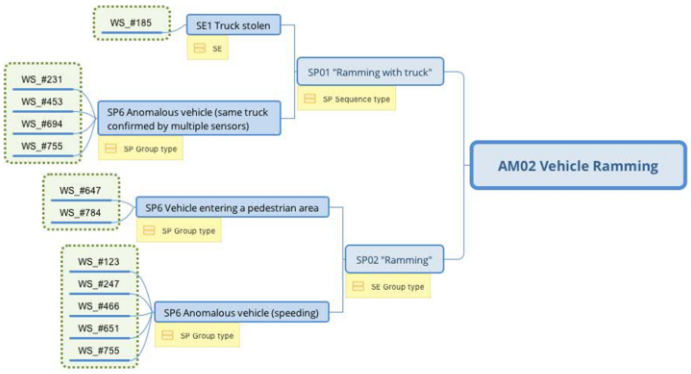
WSs are correlated to generate **Suspicious Patterns** (SP) and brought to the operator's attention to increase its **situational awareness**.

Results

The Suspicious Patterns can be generated using:

- **rules** defined using the LEAs' knowledge combining different WSs;
- an **automatic grouping** of WSs simultaneously happening in space or time;
- **data analytics**.

The DRA is fully integrated in the **Letscrowd Server(LS)** developed by ETRA. This platform use the trending Web Technologies as DRA and it also receives information from other external modules (web crawling , crowd information of the Venue and multimedia detection of suspicious behaviour) using REST technology.



Future Work

The proposed approach is going to be tested and verified during mass gatherings events in Spain by **Ertzaintza** and the **Madrid Police** and in Germany by the **University of Applied Sciences for Public Service in Bavaria**.

Conclusions

DRA methodology has the following advantages over more traditional approaches:

- Searches for **out-of-the-ordinary behaviours** and unseen threats;
- Allows **memory of hypotheses** and data rejected by security analysts;
- Notices what **analysts are watching and asking**.

Acknowledgements

This work has received funding from EU H2020 project LETSCROWD (GA no. 740466)

LETSCROWD: Dynamic Risk Assessment for Mass Gatherings

Carlo Dambra
ZenaByte s.r.l.
carlo.dambra@zenabyte.com

Alex Gralewski
PROPRS Ltd.
alex.gralewski@proprs.com

Jordi Arias
ETRA I+D S.A.
jarias.etraid@grupoetra.com

INTRODUCTION

Risks for crowd in mass gathering events are "High Impact Low Probability Risks" (e.g. terrorism, lone wolfs, domestic extremisms) and therefore managed accordingly and therefore "*rather than seek an optimal method for estimating risk, we seek a method that leads us to make the least egregious errors in decision-making across the range of possible scenarios that might develop in the future*" (Willis, et al., 2005).

This work proposes an innovative **Dynamic Risk Assessment** (DRA) approach to dynamically assess the risks for the crowd during mass gathering on the basis of dynamically collected information to minimise errors in decision-making across the range of possible scenarios that might develop in the critical time frame from the event

planning to the event execution.

METHODOLOGY

The proposed methodology is inspired by the network Intrusion Detection Systems (IDS) approaches as those proposed by (Chakir, et al., 2017) based on the analysis of Weak Signals (WS). A WS can be defined (Schoemaker & Day, 2009) as *a* disconnected piece of information that at first appears to be background noise but can be recognized as part of a significant pattern by connecting it with other pieces of information.

WSs can be detected by different sensors detecting threat precursors: from humans as sensors (e.g. policemen in crowd or a 112 calls) to CCTV-based systems, from Cyber-Threat Intelligence systems to physical sensors (e.g. explosive detectors).

Each Weak Signal has a **Significance** (**S**) value assigned to it that is a combination of the **Credibility** (**C**) of the Sensor (assigned a priori by LEAs experts) in detecting the considered precursor, the **Reliability** (**R**) of the detection and the **Time Distance** (TD) from the event (a speeding car can be considered differently if it is happening 3 days before the event or during the event), where $S(WS) \in [0, 1]$.

A WS alone could be insignificant, but when put in combination with other WS could become important. Therefore, the WS could be grouped into a **Suspicious Pattern** (**SP**). To build a Suspicious Pattern at least two WS are necessary. The Suspicious Pattern can be generated:

1. Before the event takes place, using the LEAs' knowledge that defines the rules for building the patterns that is specific to each LEA.
2. Dynamically using an automatic grouping of WSs using logic similar to those currently used, for example, at some airport security checks: 3 or more credible WSs "**simultaneously**" from different sources of information can be considered as SP. The minimum number of credible WS can be adapted to the specific local conditions.
3. Dynamically, using **data analytics** that works on all received WS and generates suspicious pattern. Recently, researchers started to publish deep learning techniques to automatically learn high-level representations, and then avoid the requirement of domain experts in designing features (Vu, 2017) (Hasan, et al., 2016).

Significance values for an SP with 2 WSs contributing to it with significance S_1 and S_2 respectively, is derived from Certainty Factors theory (Lucas, 2001) using the following formula

$$S(S_1 \; and \; S_2) = S_1 + (1 - S_1) * S_2$$

Having more than 2 WSs contributing to the same SP, it is possible to iteratively apply the proposed formula as follows (in case of 3 WSs with Significance S_1, S_2 and S_3, respectively):

$$S_{1 \; and \; 2} = S(S_1 \; and \; S_2) = S_1 + (1 - S_1) * S_2$$

$$S_{1 \; and \; 2 \; and \; 3} = S(S_{1 \; and \; 2} \; and \; S_3) = S_{1 \; and \; 2} + (1 - S_{1 \; and \; 2}) * S_3$$

RESULTS

DRA is integrated in the LETSCROWD Server (LS) developed by ETRA that incorporates also a policy making toolkit and crowd evacuation modelling tools. LS uses the trending Web technologies and receives info from external modules (web crawling, crowd info and multimedia suspicious behaviour detection) using REST technology. SPs above a selected threshold of Significance are brought to the attention of the operator together with the attached multimedia information (e.g. a snapshot of the scene, a picture of the suspicious person) and related metadata to allow a risk-aware decision-making process.

CONCLUSIONS AND FURTHER WORK

The proposed approach is going to be tested and verified during mass gatherings events in Spain by Ertzaintza and the Madrid Police and in Germany by the University of Applied Sciences for Public Service in Bavaria.

DRA methodology has the following advantages over more traditional approaches:

- Searches for **out-of-the-ordinary behaviours** and unseen threats;
- Allows **memory of hypotheses** and data rejected by security analysts;
- Notices what **analysts are watching and asking**.

Finally, the proposed DRA approach is fully in line with the European Security Model (Council of the European

Union, 2010) has defined a that prescribes, amongst other guidelines, the following:

- *"… stronger focus on the **prevention of criminal acts** and terrorist attacks before they take place can help reduce the consequent human or psychological damage, which is often irreparable.*"
- "*This allows us to deepen our **understanding of the different types of threats and their probability** and to anticipate what might happen …*"
- "***Guidelines for hazard and risk-mapping methods, assessments and analyses** should be developed as well as an overview of the natural and man-made risks that the EU may face in the future.*"

ACKNOWLEDGMENTS

This work has received funding from the EU H2020 project LETSCROWD "Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings" (GA no. 740466) https://letscrowd.eu.

REFERENCES

Chakir, E., Moughit, M. & Khamlichi, Y., 2017. *A Real-Time Risk Assessment Model for Intrusion Detection Systems.* s.l., International Conference on Information Technology and Communication Systems.

Council of the European Union, 2010. *Internal security strategy for the European Union - Towards a European Security Model.* s.l.:General Secretariat of the European Council.

Hasan, M. et al., 2016. *Learning temporal regularity in video sequences.* Las Vegas, 29th IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

Lucas, P. J. F., 2001. Certainty-factor-like structures in Bayesian belief networs. *Knowledge-Based Systems*, Volume 14.

Schoemaker, P. J. H. & Day, G. S., 2009. How to Make Sense of Weak Signals. *MIT Sloan Management Review*, 50(3).

UK Government Office for Science, 2011. *Blackett Review of High Impact Low Probability Risks,* s.l.: s.n.

Vu, H., 2017. *Deep Abnormality Detection in Video Data.* Melbourne, Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17).

Willis, H., Morral, A., Kelly, T. K. & Medby, J., 2005. *Estimating Terrorism Risk,* s.l.: RAND Corporation - Center for Terrorism Risk Management Policy.

Xu, D. et al., 2015. *Learning deep representations of appearance and motion for anomalous event detection.* s.l., BMVC.