Advanced Cyber and Physical Situation Awareness in Urban Smart Spaces

Zoheir Sabeur[1], Constantinos Marios Angelopoulos[1], Liam Collick[1], Natalia Chechina[1], Deniz Cetinkaya[1] and Alessandro Bruno[1]

[1] Bournemouth University, Department of Computing and Informatics, Talbot Campus, Fern Barros, BH12 5BB, Dorset, England, United Kingdom
{zsabeur, mangelopoulos, lcollick, nchechina, dcetinkaya, abruno}@bournemouth.ac.uk

Abstract. The ever-growing adoption of big data technologies, smart sensing, data science and artificial intelligence is enabling the development of new intelligent urban spaces with real-time monitoring and advanced cyber-physical situational awareness capabilities. In the S4AllCities international research project, the advancement of cyber-physical situational awareness will be experimented for achieving safer smart city spaces in Europe and beyond. The deployment of digital twins will lead to understanding real-time situation awareness and risks of potential physical and/or cyber-attacks on urban critical infrastructure specifically. The critical extraction of knowledge using digital twins, which ingest, process and fuse observation data and information, prior to machine reasoning is performed in S4AllCities. In this paper, a cyber behavior detection module, which identifies unusualness in cyber traffic networks is described. Also, a physical behaviour detection module is introduced. The two modules function within the so-called *Malicious Attacks Information Detection System* (MAIDS) digital twin.

Keywords: Internet of Things · Artificial Intelligence · Edge Computing · Crowd Behavior · Digital Twins

1 Introduction

Current urban environments do require 24/7 guaranteed safety and security of citizens for using smart spaces, operational systems and services. These constitute smart cities main infrastructures such as transport networks and their multi-modalities (motorways, rails, airports or maritime ports), energy and water supply networks; hospitals as well as spaces with public character or the so called “soft targets” such as malls, open markets, pedestrian precincts, city squares, sports venues, tourist sites and more. The provision of guaranteed 24/7 safety and security in the smart city spaces is of paramount importance for all citizens to confidently participate, cooperate and effectively contribute to the sustainable progress of the city socio-economic activities. Nevertheless, and with the ever advancement of smart city technologies, together with the mass deployment of IoT technologies, cities operations and services are being transformed at

unprecedented rates and scales. Hundreds of thousands of connected systems are being embedded in many cities critical infrastructures, for urban planners and security practitioners improve their operations to assure safety of citizens. Nevertheless, while these emerging technologies are bringing increased operational efficiencies, smart city infrastructure have become vulnerable to new threats and attacks on soft targets such as crowded city open spaces. On July 14th 2016, a 19-tonne cargo truck was deliberately driven into crowds of people in Nice, France, which resulted in 86 fatalities: An attack considered as a "*physical attack"* at a city open public space [1]. While on May 13th, 2017, the German transport system, specifically the electronic travel announcement boards at train stations, which started in Berlin, were completely crippled by a ransomware: An attack that is indeed a "*cyber-attack"* to a city public transport [2]. These types of cyber-physical attacks, have also occurred in other locations in the world in recent years. They present a threat to safety and security while they raise the concern of high vulnerability and risks of attacks to which urban spaces and infrastructure may be exposed.

2 S4AllCities project

The S4AllCities project [3] was launched in September 2020, as a large consortium of 27 partner organizations from academia and industry in Europe. One of the main goals of the project is to deploy automated, scalable and performing captures of real-time intelligence for safety and security in urban smart spaces environments. Three European pilot cities with respective urban smart spaces were selected for demonstrating our S4AllCities technology by the fall of year 2022. These include: The City of Bilbao, Spain; Trikala Municipality, Greece; and the City of Pilsen, Czech Republic.

The S4AllCities technology adopts a distributed and interoperable System of System (SoS) architecture which is driven by three major Digital Twins; each of which specialises in levels of situation awareness and uses computer machine intelligence. Together, they revolutionise the way cities enhance strategic protection, preparedness and resilience against cyber-physical threats and potential attacks on urban smart spaces and critical infrastructure networks. The three Digital Twins are:

a) Distributed Edge Computing IoT Platform: *DEC_IoT*
b) Malicious Actions Information Detection System: *MAIDS*
c) Augmented Context Management System: *ACMS*

They function intelligently on the following levels of situation awareness in context of the smart spaces environment respectively:

a) *DEC_IoT* → Processing of observed events in the urban smart spaces
b) *MAIDS*→ Intelligent detection and understanding of unusual behavior
c) *ACMS* → Augmented realization of intelligence for threat alerts

2.1 System of Systems architecture (SoS)

Real-time intelligent detection and understanding of observed processes in urban smart spaces are being experimented in the S4AllCities project. As shown in Figure 1, below, the SoS connects to the urban smart spaces physical IoT with all the relevant

sensing networks; operational legacy systems and critical infrastructure information and communication networks. The generated data streams are ingested by the DEC_IoT twin and aggregated intelligently on the edge for further diagnosis by MAIDS twin through a message broker middleware. The DEC_IoT is event-driven while it dynamically emulates a problem environment which is representative of the smart environment of interest and to which one subscribes. The subscription of the MAIDS to it leads it to enacts further processing for unusualness detection and understanding of physical motions of objects, individuals, clusters of individuals and overall crowd in the smart environment. It assesses cyber traffic unusualness in communication networks which function within the same smart environment too. The overall states of unusualness of both cyber and physical detections may also require high data fusion and knowledge modelling and reasoning in order to obtain an accurate context understanding of the nature of unusualness as potential threat and/or attack on the smart space.

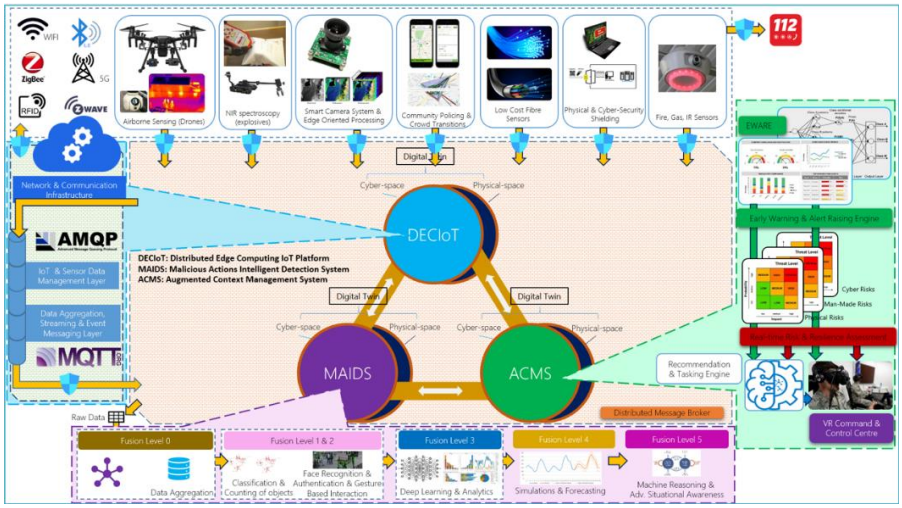

Figure 1 S4AllCities SoS High Level Architecture with its three Digital Twins

The This results into stream messaging such information from the MAIDS to the ACMS twin for realizing a real-time augmented contextual understanding of the smart environment. This is what is called the Common Operational Picture (COP).

2.2 IoT and edge computing

Over the past years research and technological advancements have enabled the paradigm of Internet of Things (IoT) to transition towards higher technological readiness levels by addressing key underlying issues. With respect to hardware components, the reduced cost of sensor, compute and communication components enables the development of low-power, highly embedded and affordable IoT devices with small physical form factor that can be deployed *en masse*. This underpins the development of cyber-physical systems, that are well-integrated in the physical environment and seamlessly interconnected with other digital systems. In this context, the emergence and high adoption rates of Single Board Computers (e.g. Arduino's and Raspberry Pi's) allow the

deployment of embedded devices with considerable compute resources at the fringe of the IoT network, able to support sophisticated services, such as localized data processing and decision making. Advances in the area of Low Power Wide Area Networks (LPWANs) have fine-tuned the trade-off between energy consumption and long-range wireless communication of IoT devices, thus facilitating the deployment of IoT systems over wide areas, spanning across urban regions. The variety of available solutions accommodates diverse requirements not only from a technical perspective but from an operational one as well. For instance, LPWANs operating in the unlicenced spectrum (e.g. LoRaWAN and Sigfox) allow the deployment of private standalone IoT systems with low operational costs. On the other hand, LPWANs operating in the licenced spectrum (e.g. NB-IoT) allow quick and scalable deployment of IoT systems over the existing cellular infrastructure. In the context of 5G networks, the interconnection of such IoT systems with backhaul networks and backend systems underpins the interplay with next Generation Networks (e.g. Software Defined Networks and Network Function Virtualisation), other technological enablers (e.g. Edge Computing, Big Data Analytics and Machine Learning) as well as more agile development tools and methods, such as the use of micro-services and containers.

The aforementioned advances shape a technological ecosystem for cyber-physical systems that not only are able to collect sensory data from the physical environment but can process this data and take decisions locally. This is highly relevant since IoT data are typically characterized by timeliness and their value is highly localized[4], [5].

S4AllCities introduces the DECIoT Digital Twin which builds upon a collection of open source micro-services that span from the edge of the physical plane. The use of the EdgeXFoundry Platform disassociates the physical IoT devices from the generated IoT data by obfuscating implementation complexities and dependencies via standardised south-bound and north-bound interfaces. This modular architecture supports data and event-driven decision-making at the Edge as specialized services (e.g. machine learning models) that typically reside on the Cloud can now be deployed closer to the data sources for intelligent pre-processing.

2.3 Data fusion, modelling and reasoning

Multi-level data fusion which adopts the *De-Facto* Joint Director of Laboratory (JDL) data fusion framework has revolutionized the way we intelligently advance situation awareness [6]. While, the Endsley model is well-known for advancing situational awareness in context of critical decision support on cyber or physical security it can be mapped onto the JDL model, for equivalence, as illustrated in Figure 2. The JDL framework offers a more adaptive approach to intelligent data processing, i.e multi-level fusion, and interpretation of progressively advanced situational awareness which can be applied to cyber-physical security [7]. [8]. With the recent advancement in IoT, large streams of big data can be generated and from which critical knowledge can be extracted in real-time using machines reasoning in order to understand threats and/or attacks on urban spaces with high context awareness [9], [10]. The MAIDS twin of S4AllCities SoS, adopts the JDL data fusion framework, for big data processing and analytics while it can efficiently organize them at various fusion levels, which themselves are levels of cyber-physical

situational awareness. These include: *Level 0: Pre-processing; Level 1: Object Assessment; Level 2: Situation Assessment; Level 3: Impact Assessment; Level 4: Context Refinement and Level 5: User Refinement.* These respectively cover equivalent levels situational awareness that concern*:* 1- Perception; 2- Comprehension; 3- Projection; 4: Decision; and 5- Performance feedback.

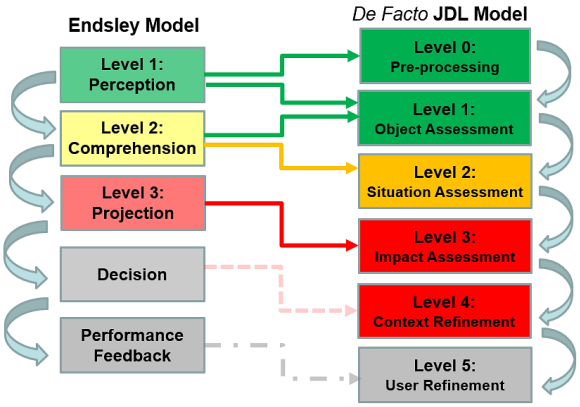

Figure 2. Endsley model equivalence with the JDL for advanced situational awareness

Howwever, the most important element for the successful deployment of framework, for the detecting and understanding unusualness in the cyber and physical environments is the acquisition of quality observation data. Such quality data is expected to uniquely manifest key features of physical and cyber behaviour in context of urban smart spaces in order to achieve performing machine learning algorithms. Without which we will not be able to select the correct optimised features and generalise the algorithms into per-great Correct Classification Rates (i.e. CCR > ~ 90%) of unusual behaviours.

3 Cyber behaviour detection

The growth of smart spaces brings with it a massive increase in the adoption of IoT and ICT technologies. Coupled with an ever-growing issue of cybercrime there is an inevitable exposure to a vast number of cyber-attacks within smart spaces due to their large surface area for attack. With smart spaces being at the forefront of today's technology it is only natural for cybercrime targeting these spaces to become more sophisticated too. To protect the smart space, its critical infrastructure and communication networks equal sophistication is required, basic defences would not be suitable. A scalable incident detection solution will be implemented for S4AllCities, it will be able to detect unusualness in the network using machine learning. It will also be able to grow and adapt to handle ever-increasing amounts of data.

3.1 High-level architecture

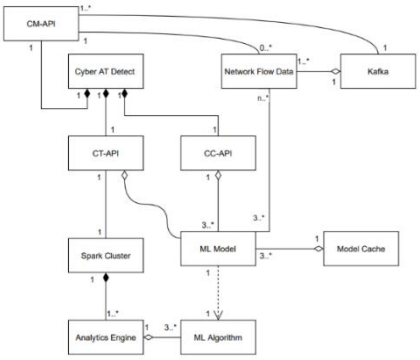

Figure 3. High-Level Class Diagram of the CyberATDetect

A cyber incident detection module, CyberATDetect, will be developed as a component of MAIDS. The component will consist of multiple APIs (See Figure 3.) with the data flow being based on the state of the system. A management API will consume data from an Apache Kafka broker. There will then be a training and classifying API both of which will utilise a Spark cluster for machine learning. Spark was selected due to its high performance as a distributed stream processing system. It has high throughput when dealing with network data and compared to a similar performing competitor Samza it is less strict on its data requirements [11]. The combination of Spark and Kafka will allow for real-time classification of network flow data with high volumes of data and will enable the possibility of scaling the system up as required. The spark cluster will be running on the Hadoop platform and the system will utilise the benefits of the Hadoop File System (HDFS).

As aforementioned the data flow will be dependent on the state of the module (See Figure 4.). The module itself will be in one of two major states: harvesting and classifying. During the harvesting state, data will be ingested pre-processed and then stored within the HDFS. Once the component has harvested enough data the models can be trained, the details of which will be discussed in section 3.2. The models will be based on three main ML algorithms, identified as strong performers on network traffic data from previous research.

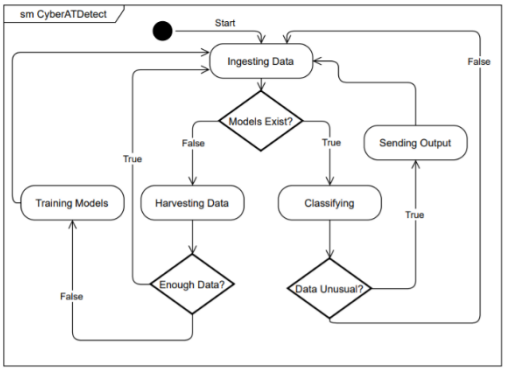

Figure 4. State Transition Diagram of CyberATDetect

3.2 Cyber detection with machine learning

Machine learning has become a necessity to secure modern networks. With the growing number of cyber threats and attack profiles, it is not possible to simply have a list of known attacks and their signatures. It has become a requirement to implement intelligent intrusion detection to fortify systems and their users. In S4AllCities this cyber incident detection module, within the MAIDS twin, will focus on identifying unusual traffic within the S4AllCities network. As specified in the architecture section three main algorithms will be selected for the CyberATDetect module itself, this will be based on research on their performance on various synthetic network traffic data. These will be strong performing algorithms that, when combined, should be able to identify a large variety of unusualness within the network traffic data, with a high degree of accuracy.

Network flow data has many features resulting in noise within the dataset and which limits the effectiveness of the machine learning algorithms and increases the time it takes them to be trained and classified [12]. Therefore, unimportant features must be removed in the pre-processing stage. These will be identified using feature-set selection. Once these are identified, the module should be able to preprocess this before storage to reduce training and classifying times.

When identifying strong performing algorithms there is not a single metric that will be looked at to rank these. A combination will be used, this is due to the various requirements of the CyberATDetect module itself and the balance of the datasets used for research. In the investigation many metrics were recorded, including area under the receiver operating characteristic (ROC) curve and Matthews Correlation Coefficient (MCC). The curve itself was also plotted giving a visual representation of the algorithm's performance.

The algorithms have been tested on multiple sources of data to ensure reliability. These are open datasets of synthetic network traffic data. The approach being used is to train using labelled data and to test the developed model on an unseen hold-out set, this was appropriate since all the datasets had many instances.

3.3 Discussion

The research will be expanded to investigate the classification of various attack types. This is not an area being focused on for the initial implementation due to the added complexity it may reduce the effectiveness of the system, hence it will be an additional feature on top of identifying unusualness. Overall cyber-security of the S4AllCities SoS is the priority, therefore it will be important to limit false negatives for readings as much as possible. In the event of a cyber-attack, it should be raised on the maximum number of occasions, although false positives can be disruptive if kept at a manageable rate it would be more tolerable than a high false-negative rate. Clustering will also be researched to aid with the classification of attack types, clustering may be useful to identify prominent features within the different types of attack. Clustering will also be useful if labelled data is not available, with the combining of multiple algorithms being a useful method of improving accuracy [13]. It will be important to identify algorithms with strengths in different areas to cover as many attack types as possible. With S4Allcities running pilots within multiple European cities: Trikala, Bilbao, and Pilsen, real network traffic quality data will become available. In this case, CyberATDetect CCRs will be scrutinised using such data. This data will also challenge the effectiveness of the S4AllCities SoS, as it will then be important to improve it in future versions, by the fall of 2022.

4 Physical behavior detection

The Physical behaviour detection module lays out within the MAIDS twin and approaches the detection of unusual behaviours in crowds using image analysis and computer vision techniques. Even though much progress has been made over the last decades, the task mentioned above remains a challenge due to several varying factors [14], such as camera field-of-view, crowd scale in video sequences, and cameras spatial resolution. As highlighted in the scientific literature, there are some analogies and similarities drawn between crowd behaviour, classical fluid dynamics and statistical mechanics of molecular gases [15].

Some crowd behaviour models are also inspired by cellular automata [16], which allow achieving good results in detecting macro-dynamics of crowds (macroscopic scale). Another popular model is the Social Force [17] that relies on a simple concept by which individuals in crowds move accordingly to certain constraints (environmental) and goals. Crowd Collectiveness was introduced to measure how individuals act as a group in motion [18]. Different from models inspired by hypothetical structures to understand crowd behaviour, some techniques learn patterns detecting semantic regions within crowded scenes[19]. Physical analogies using statistical mechanics principles have been successfully implemented to measure the crowd system's flow, energy and collectiveness using smart sensor observations and measurements for detecting crowd behaviour in context of urban spaces. In a way, the module of physical behaviour detection in S4AllCities represents an extension of an existing scientific method, which we set up in the last few years [20], [21].

Spatial crowd density allows to measure and represent crowd seeds. A set of key features can be defined for the crowd at various scales (micro, meso and macro). These

features are chosen on purpose to characterize the state of crowd's dynamics being monitored and clustered, including for Individuals (micro-scale), Groups (meso-scale) and Whole Crowd (macro-scale). The method relies on entropy as a crowd analysis descriptor, and a crowd-space based on three features of Structure, Energy and Translation. In the next subsection, more details are given about the overall computer vision techniques to accomplish the task.

4.1 Physical detection with computer vision

In this subsection, a more detailed description of the Physical Detection module is given. As briefly mentioned in the previous sections, Physical Behaviour Detection builds on the computation of some image features' entropy and works in a crowd -space defined on features of Energy, Structure and Translation as proposed in [21]. It is worth to spend some more words about the three features concerning different stages of crowds.

Structure represents the connection strength among individuals in crowd; Energy represent the level of excitation of crowd as a whole; Translation shows the motion of crowd.

The diagram in Figure 5 shows some stages in crowd space. Point 1, represents a crowd state with zero connection strength, zero motion and no energy (it is not a likely state of crowd). To mention some more intuitive crowd states, point 5 coordinates have low energy, high translation and high structure such as a group of people on an elevator. Point 2, may represent the state of a group of bored spectators in a stadium (zero translation and energy and high structure). Point 7 may show the state of a sparse panicked crowd moving towards a direction (high Energy and Translation but zero Structure).

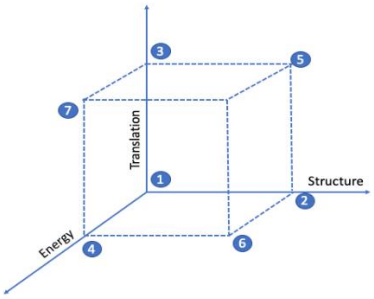

Figure 5 Crowd space representations with Energy, Structure, Translation.

Structure, Energy and Translation are used as crowd density descriptors, which are mapped onto the statistical mechanics principles of entropy. An important assumption is that the crowd or the groups whose crowd is made of are considered homogeneous systems.

From the Information theory, the joint entropy of two ensembles X and Y is defined as in equation (1)

$$H(X, Y) = \sum_{xy \in \mathcal{A}_X \mathcal{A}_Y} P(x, y) \log \frac{1}{P(x, y)} \quad (1)$$

X and Y are triples. $X = (x, A_x, \zeta_x)$ where x is a random variable from possible values in $A_x = \{a_1, a_2, \ldots, a_l\}$ with probabilities $\zeta_x = \{p_1, p_2, \ldots, p_l\}$. Y is a triple (y, Ay, ζ_y).

The entropy of a crowd [2] is defined as the joint entropy of N_p individuals who are scattered in N_l locations with a probability mass function f_{Y_i} on a discrete random variable, Y_i , defined at each spatial bin, l_i.

$$H\left(X_1, \ldots, X_{N_p}\right) = -\sum_{x_1 \in \zeta_x} \ldots \sum_{x_{N_p} \in \zeta_x} P\left(x_1, \ldots, x_{N_p}\right) \log P\left(x_1, \ldots, x_{N_p}\right) \quad (2)$$

Where X_k is a triple $(x_k, \zeta_X, \mathrm{P}_{X_k})$. x_k assume values out of the set $\zeta_X = \{l_1, l_2, \ldots, l_{N_l}\}$, having probabilities $\mathrm{P}_{X_k} = \{p_{k,1}, p_{k,2}, \ldots, p_{k,N_l}\}$, with $P(x_k = l_i) = p_{k,i}$.

Some assumptions are necessary to fully carry out all steps of the method [2]. The first one is to consider that a pattern is formed in the individuals in crowd. In this model, the locations of people are considered to be independent, and the individuals are considered to be identical.

The above-mentioned assumptions take to a more simplified computation of entropy as follows:

$$P(x = l_i) = \frac{n_i}{N_f N_p} \quad (3)$$

Where n_i is set as the sum of all density at bin l_i in N_f frames.

As briefly mentioned at the beginning of this section, some image features can be used to feed the Physical Behaviour Detection module. Corner features proposed in [22] well suit the purpose of the module because of their optimal performances on video tracking tasks. It is worth to notice that after detecting corners in frames, it is also necessary to remap them to locate the real-world locations and avoid the same side-effects previously discussed (distortions caused by projective transforms). More precisely, after remapping, the locations of corners are the internal positions of the features which are projected into the ground plane.

As noticeable in Figure 6, individual positions extracted at t_0 are marked with red dots, while those at t_1 frame are marked in yellow. Individual positions can reveal crowd states because of different structure, translation and energy. In figure 4a, small variations in individual positions are detected with the lower size bin while they cannot be identified with the larger size bin. In figure 4b, it is noticed greater crowd translation,

energy and low structure, having individuals moved faster and chaotically. Therefore, bin size needs to be fine-tuned over different real scenarios such as people on an escalator, spectator attending a concert or a football match. Some experiments are reported in [2]. In scenarios with crowds on escalators the best separation is achieved for bin sizes within the range [0.04 m, 0.2 m].

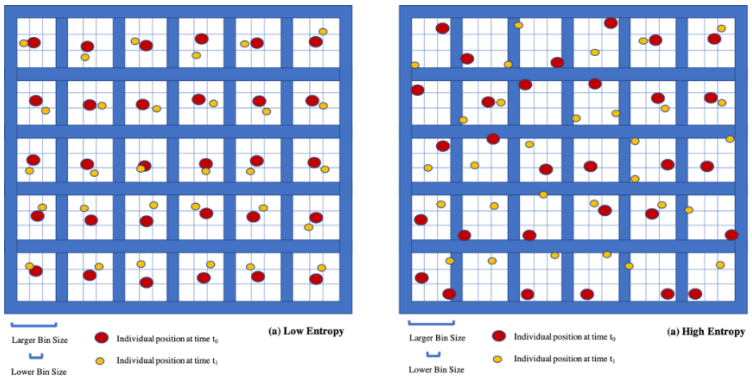

Figure 6 Graphical Representation of two different crowd states (low and high entropy) analysed with a larger and a smaller bin size.

Before using entropy to compare behaviours between groups having different number of people, it is necessary to go through a normalisation step. For this purpose, specific entropy is defined as the entropy per unit of mass [21]. Furthermore, prior to the computation of entropy, three pre-processing steps are run on each frame as depicted in Figure 7, below. The first pre-processing step deals with the distortion caused by the projective transform, which is due to the angle between the camera and scene plane. A head-height plane homography is applied to counterbalance the distortion side-effect. A calibration step is also considered for this purpose.

The second pre-processing step is the extraction of internal position density map. That is achieved by detecting each individual spatial coordinate within the crow. The computation of individual spatial coordinates is run over consecutive frames, which undergo a grid-based layout analysis defined by the bin size.

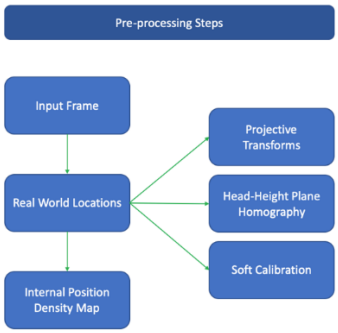

Figure 7 Pre-processing applied on each frame

Other descriptors such as Collectiveness and Kinetic Energy are also compared to analyse macro-dynamics of crowd behaviour. Collectiveness seeks collective manifolds wherein consistent motion is observed in neighbourhoods, while Kinetic Energy of a crowd as a thermodynamic system is used as a measure of how excited the crowd is. In Figure 8, below, Collectiveness and Kinetic Energy are employed and compared to run some tests over frames taken from a Stadium arena, at the Aneota Stadium, San Sebastian in Spain.

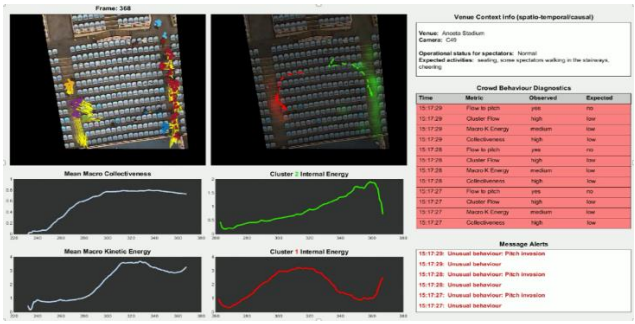

Figure 8 Unusual behaviour is detected in the frame above [21]

5 Conclusion and future recommendations

This early work in the S4AllCities project sets the primary foundations for the development of the MAIDS Twin system. It specializes in cyber-physical behaviour detection of unusualness and understanding in context of urban smart spaces safety and security enforcement. The cyber behaviour detection module relies on achieving performing machine learning algorithms which not only detect unusualness in cyber traffic network, but also classify the type of threat or attack a smart space environment may endure. The classification of threats or attacks will be researcherd through investigating on quality data from the S$AllCities pilot cities using clustering methods for

unsupervised learning. As for the physical behaviour detection module within MAIDS, we will exploit our described approach to investigate on the measurement and prediction of behaviour propagation in urban smart environment.

6 Acknowledgements

The authors are grateful to the European Commission for funding our research work in the S4AllCities project, under the H2020 Programme, Grant Agreement No. 883522

References

1. EUROPOL.: The European Union Terrorism Situation and Trend (TE-SAT) 2017. European Union Agency for Law Enforcement Cooperation. pp61. See weblink: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017. (2017)

2. The Daily Telegraph.: Cyber-attack hits German train stations as hackers target Deutsche Bahn. See weblink: https://www.telegraph.co.uk/news/2017/05/13/. (2017)

3. S4AllCities.: Smart Spaces Safety and Security in All Cities. See weblink: https://www.s4allcities.eu/project. (2020)

4. Angelopoulos, C. M., Filios, G., Nikoletseas, S., Patroumpa, D., Raptis, T., Veroutis, K. :A holistic IPv6 test-bed for smart, green buildings. ICC 2013: 6050-6054 https://doi.org/10.1109/ICC.2013.6655569. (2013)

5. Angelopoulos, C. M., Filios, G., Nikoletseas, S., Raptis, T. Theofanis.: Keeping data at the edge of smart irrigation networks: A case study in strawberry greenhouses. Comput. Net works 167 (2020). https://doi.org/10.1016/j.comnet.2019.107039.

6. K Lambert, D.A et al.: . A Blueprint for higher-level fusion systems. Information Fusion, Vol. 10, Issue 1. Pp 6-24. (2009)

7. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. The Journal of Human Factors and Ergonomics Society, 37(1), 32-64. (1995).

8. Sabeur. Z.: Lectures Series on Cyber Situational Awareness. Department of Computing and Informatics. Bournemouth University. UK. (2019)

9. Correndo, G., Arbab-Zavar, B., Zlatev, Z., Sabeur, Z.:. Context Ontology Modelling for improving Situation Awareness and Crowd Evacuation from Confined Spaces. IFIP Ad vances in Information and Communication Technology, Springer Publishing. (2015)

10 Sabeur, Z., Zlatev, Z., Melas, P., Veres, G., Arbab-Zavar, B., Middleton, L., Museux, N.: Large scale surveillance, detection and alerts information management system for critical infrastructure. IFIP Advances in Information and Communication Technology, Springer Publishing. (2017)

11. Cermak, M., Tovarňák, D., Lastovicka, M., Celeda, P.: . A performance benchmark for Net Flow data analysis on distributed stream processing systems. (2016). 919-924. 10.1109/NOMS.2016.7502929.

12. Mehmood, T., Md Rais, H.B.: Machine learning algorithms in context of intrusion detection," 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2016, pp. 369-373. (2016) doi: 10.1109/ICCOINS.2016.7783243.

13. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., Kim, K. J. : A survey of deep learning-based network anomaly detection. Cluster Computing. (2019). https://doi.org/10.1007/s10586-017-1117-8

14 Sànchez, Francisco Luque and Hupont, Isabelle and Tabik, Siham and Herrera, Francisco, Revisiting crowd behaviour analysis through deep learning: Taxonomy, anomaly detection, crowd emotions, datasets, opportunities and prospects, Information Fusion, Elsevier, (2020).

15. Burstedde, C., Klauck, K., Schadschneider, A., Zittartz, J.: Simulation of pedestrian dynam ics using a two-dimensional cellular automaton. Phys. A 295, 507–525 (2001)

16. Guo, R., Huang, H.: A mobile lattice gas model for simulating pedestrian evacuation. Phys. A 387, 580–586 (2008)

17. Helbing, D., Molnar, P.: Social force model for pedestrian dynamics. Phys. Rev. E 51, 4282–4286 (1995)

18. Zhou, B., Tang, X., Zhang, H., Wang, X.: Measuring crowd collectiveness. IEEE Trans. Patt ern Anal. Mach. Intell. 36, 1586–1599 (2014)

19. Zhou, B., Wang, X., Tang, X.: Random field topic model for semantic region analysis in crowded scenes from tracklets. In: IEEE Conference on Computer Vision and Pattern Recog--nition (CVPR), pp. 3441–3448 (2011).

20. Sabeur, Z.A., Doulamis, N., Middleton, L., Arbab-Zavar, B., Correndo, G., Amditis, A.: Multi-modal computer vision for the detection of multi-scale crowd physical motions and behavior in confined spaces. In: Advances in Visual Computing, pp. 162–173. Springer, New York (2015)

21. Arbab-Zavar, B., Sabeur, Z.: Multi-scale crowd feature detection using vision sensing and statistical mechanics principles. Machine Vision and Applications (2020) 31:26 https://doi.org/10.1007/s00138-020-01075-4

22. Shi, J., Tomasi, C.: . Good features to track, pp. 593–600. (1994)