Real-time Threat Assessment based on Hidden Markov Models

Ourania Theodosiadou[1,*], Despoina Chatzakou[1], Theodora Tsikrika[1], Stefanos Vrochidis[1], and Ioannis Kompatsiaris[1]

[1] Information Technologies Institute, Centre for Research and Technology Hellas

[*]Address correspondence to Ourania Theodosiadou, Information Technologies Institute, Centre for Research and Technology Hellas, 57001 Thessaloniki, Greece; raniatheo@iti.gr

ABSTRACT: An essential factor towards ensuring the security of individuals and critical infrastructures is the timely detection of potentially threatening situations. To this end, especially in the law enforcement context, the availability of effective and efficient threat assessment mechanisms for identifying and eventually preventing crime- and terrorism-related threatening situations is of utmost importance. Towards this direction, this work proposes a hidden Markov model-based threat assessment framework for effectively and efficiently assessing threats in specific situations, such as public events. Specifically, a probabilistic approach is adopted to estimate the threat level of a situation at each point in time. The proposed approach also permits the reflection of the dynamic evolution of a threat over time, by considering that the estimation of the threat level at a given time is affected by past observations. This estimation of the dynamic evolution of the threat level over time is very useful, since it can support the decisions by security personnel regarding the taking of precautionary measures in case the threat level seems to adopt an upward trajectory, even before it reaches the highest level. In addition, its probabilistic basis allows for taking into account noisy data. The applicability of the proposed framework is showcased in a use case that focuses on the identification of potential terrorist threats in public events on the basis of evidence obtained from the automatic visual analysis of the footage of surveillance cameras.

KEY WORDS: Threat assessment, Hidden Markov Models, hidden threat level, visual analysis

1 INTRODUCTION

The early detection of potentially threatening crime- or terrorism-related situations in the context of an event, a city, or even around the globe, is of paramount importance for security practitioners, so that they can better determine what protective security response may be required and also be better prepared to address potential attack incidents. Given, in particular, the significant impact that crime and terrorism may have both directly on humans and/or infrastructure, as well as indirectly to people's psychology, such as emotional collapse and a sense of vulnerability, this poses a significant threat to the well-being of the humanity as a whole. An effective threat assessment process would thus allow to identify and proactively react to threatening situations and potential security incidents.

Regarding the crucial issue of terrorism risk, there is no single definition that is widely adopted; in general, the notion of terrorism risk is related to threats, attacks, vulnerabilities, consequences of the attacks, uncertainties, and probabilities (Aven & Guikema, 2015). On the basis of the abovementioned facets of terrorism risk, this paper proposes a threat assessment framework capable of assessing threats in situations where a security incident may take place, such as events attended by the public (e.g., music festivals). Specifically, a method is proposed for estimating, at each time step, the **threat level** regarding a given situation, along with the probability of being in that threat level. The proposed method is based on a Hidden Markov Model (HMM), which is a doubly stochastic process consisting of a hidden process and an observation process, whereby the hidden process is not observable and can be estimated via a sequence of observations. In general, HMMs are probabilistic models that have been used successfully in several scientific domains, such as seismology (e.g., Z. Wu (2010)), speech recognition (e.g., Rabiner (1989, 1993)) and image processing (e.g., Bobulski and Adrjanowicz (2013)), as well as in the cybersecurity domain for modeling Intrusion Detection Systems (e.g., Årnes et al. (2005), Årnes et al. (2006), and Deshmukh et al. (2019), Yu-Ting et al. (2014)).

The adoption of an HMM in this work is based on the assumption that the threat level can be considered to be a hidden state (non observable). In other words, the *hidden process* in the proposed HMM represents the threat level of a situation for which we are interested in estimating its security status, while the *observation process* is considered to consist of factors that are assumed to affect the threat level of a situation, such as observed suspicious behaviors and actions. Therefore, the output of the proposed HMM is the hidden threat level of a situation at each time step, estimated (in essence "revealed") via a sequence of observations.

Compared to the often-followed semantic reasoning approaches which are based on a set of predefined rules (e.g. Souag et al. (2013) and S. Wu et al. (2018)), here a probabilistic approach is followed for the estimation of threat. This leads to the "revelation" of the dynamic evolution of a threat, while taking into account past observations for assessing the threat level at a given time. In addition, due to the fact that the hidden process is assumed to be a Markov chain, the proposed method can also be used for the prediction of the threat level based on the properties of Markov chains (see, for example, Norris (1998)). The applicability of the proposed model is illustrated with a use case aiming at assessing the threat level in a public event by taking into account observations obtained by the analysis of visual content gathered by surveillance cameras.

HMMs have been previously used for event anomaly detection in public places (e.g., Epaillard and Bouguila (2016)). However, in our case, our framework does not only detect an anomaly or an event of interest, but also provides a rating scale of the overall security status at each time step, based on the outcomes of various visual analysis processes. This rating scale is of considerable usefulness for the provision of early warnings at (near) real time, in case an upward evolution of the threat level is observed. To extract as much valuable information as possible, multiple automatic visual analysis processes are considered, namely object detection, face recognition, activity recognition, and crowd violence detection, which allow for an effective depiction (from a security perspective) of the overall situation during an event.

Overall, the main contribution of this work is the adoption of a probabilistic approach, based on the HMM framework, for the assessment of the threat level related to terrorism in situations like public events; to the best of our knowledge, this is the first time an HMM framework is applied in this particular context. Moreover, the proposed method allows not only for the estimation of the dynamic evolution of the threat level over time, but also provides a rating scale of the threat at each time step based on the observation processes of interest. Taking into consideration the abovementioned points, it can be inferred that the proposed threat assessment framework may prove to be considerably useful for providing support in decisions by security personnel regarding the taking of precautionary measures in case the threat level appears to follow an upward trajectory, even before it reaches the highest level, thus allowing for the more efficient management of human and monetary resources. In addition, the proposed model can also be used for noisy data due to its probabilistic reasoning. Furthermore, the well-known properties of Markov chains can also be used for the prediction of the hidden state. In fact, the use of the HMM framework in the assessment of threat level introduces a concept where the threat level, or in general the risk, regarding a situation is considered to be a hidden state, and can be "revealed" via the theoretical background of HMMs. On the whole, the coexistence of these features allows for real-time threat assessment regarding the security status of a situation through the provision of early warnings based on (potentially noisy) observations thus enabling the effective management of resources, a key objective for Law Enforcement and also for security personnel on critical infrastructures and enterprises.

The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 presents the proposed HMM-based framework for the assessment of threat. Section 4 describes an application of the proposed methodology concerning the estimation of the threat level in a public event, along with an illustrative example. Section 5 discusses the strengths and limitations of the proposed framework. Finally, Section 6 provides some conclusions and suggestions for further research.

2 RELATED WORK

A review of methods used for the threat assessment of a situation can be found in Steinberg (2009), where data-driven, model-driven, and hybrid methods are described. Focusing on probabilistic methods for the threat assessment of a situation, a Markov decision model in continuous time with a finite state space has been proposed for assessing the dynamic progress of threat in surveillance applications (Bäuerle & Ott, 2011; Ott, 2010), where rewards are assigned in every transition from one alarm state to another.

Concerning the threat assessment related to terrorism and potential incidents, a discussion about the applicability of probabilistic approaches in such situations (Ezell et al.,

2010) has included Logic Trees (e.g., Dillon-Merrill et al. (2008)) and Bayesian Network analysis (e.g., Hudson et al. (2005)). Regression analysis has also been employed to model regional terrorism risk (Chatterjee & Abkowitz, 2011), taking into consideration the population density and the number of critical infrastructures in each region. Moreover, for the threat evaluation in air defense operations, models based on Bayesian Networks have been used for situation threat assessment (Kumar & Tripathi, 2016; Xu et al., 2014), while the importance of visual analytics in enhancing the threat assessment procedure has also been illustrated (Dahlbom & Helldin, 2013).

In addition, the assessment of threat is a crucial topic in the field of computer networks in terms of their cybersecurity. In this context, semantic reasoning methods have been used for security requirements (Souag et al., 2013; S. Wu et al., 2018), while probabilistic approaches have been employed by Intrusion Detection Systems (Årnes et al., 2006; Yu-Ting et al., 2014), where the use of HMMs has been proposed for the estimation of the transition probabilities between the different security states of a network system and the prioritisation of alarms. Also, a genetic algorithm has been proposed to be used so as to map the parameters of HMMs to the chromosome space attempting to determine the specific value of them for estimating the risk in a network (Li & Guo, 2009). Towards this direction, a framework has been defined for predicting multi-step attacks using HMMs (Sendi et al., 2012). In this case, the HMMs are used in the prediction stage of the proposed framework attempting to predict the future state of the network based on the past generated alerts so as to run an appropriate set of responses on the network according to the result of the prediction component. HMMs have also been combined with attack graphs for the evaluation of network security risk (Liu & Liu, 2016; Wang et al., 2020). More recently, a new algorithm, referred to as Fusion HMM, has been used to model the attacker's behavior (Deshmukh et al., 2019); this algorithm trains a set of diverse HMMs on k different low-correlated partitions of data and merges the predictions of these models using a nonlinear weight function.

In general, HMMs have proved to be an effective probabilistic tool in the estimation of non observable components which are related to the risk analysis of a situation in various scientific domains. For example, in seismology HMMs have been used to reveal the states of the stress field that causes earthquake occurrence via a sequence of earthquake data contributing to seismic hazard assessment (Votsi et al., 2013). Moreover, in meteorology a method based on HMMs have been developed to assess the risk of rainstorm disasters by connecting the rainstorm intensity with the rainstorm disaster risk (Wang et al., 2018). Finally, an HMM-based approach has also been used in the domain of crash risk prediction related to vehicular ad hoc networks in urban environments where the accident risk is a latent variable that can be estimated via observations such as velocity, weather conditions, risk location, nearby vehicles density, and driver fatigue (Aung et al., 2018).

The threat assessment framework proposed in this work estimates the threat level of a situation and considers this threat level to be a hidden state (non observable). Its estimation is implemented via the HMM framework, allowing for a dynamic assessment of the threat level over time. In general, the approach of considering risk as a latent variable and provide a periodical estimation of it via an HMM has also been implemented before in different domains, as illustrated in the related bibliography; especially, when considering Intrusion Detection Systems. However, to the best of our knowledge, this is the first time that a method is proposed for a periodic probabilistic estimation of the threat level considering terrorism in situations like public events, where a rating scale of the security status is provided at each time step. Aiming to showcase the applicability of the model, this work presents the estimation of threat level related to terrorism in public events, on the basis of the outputs of several visual analysis components that automatically process visual content obtained from surveillance cameras.

3 THREAT ASSESSMENT FRAMEWORK

This section presents the proposed HMM-based framework for the estimation of the threat level in a situation (e.g., a public event) at each time step. First, Section 3.1 provides a brief description of the HMM structure, which constitutes the main mathematical tool for the proposed model (for more details, see Cappé et al. (2006) and Rabiner (1989)), while Section 3.2 presents the proposed threat assessment approach.

3.1 Hidden Markov Models

An HMM is a doubly stochastic process with an underlying process that is hidden (i.e., not observable), and thus can only be estimated through another set of stochastic processes that produce the sequence of observations. The hidden process is a Markov Chain, in the sense that the conditional distribution of the hidden variable at time t depends only on the hidden variable at time $t-1$. Moreover, the value of the observed variable at time t depends on the value of the hidden variable at the same time. Generally, at discrete times, the hidden process is at some state and an observation is generated. Then, the hidden process changes its state based on its *transition probabilities.* The main target is to reveal the (hidden) states of the hidden Markov Chain given a certain sequence of observations.

By denoting the state space as $S = \{S_1, S_2, \ldots, S_n\}$, where n is the number of states, the state at time t as q_t, and the discrete set of m possible observation vectors as $V = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$, there are three main parameters that characterize an HMM:

1. the transition probability matrix $\mathbf{A} = \{\mathrm{a}_{ij}\}$, where the elements $\mathrm{a}_{ij} = P[q_{t+1} = S_j | q_t = S_i]$, $1 \leq i, j \leq n$, denote the transition probabilities from one state to another at a given time step;

2. the emission probability matrix $\mathbf{B} = \{b_j(k)\}$, where the elements $b_j(k) = P[\mathbf{v}_k \textit{ at time } t | q_t = S_j]$, $1 \leq j \leq n$, $1 \leq k \leq m$, capture the probability of an observation to occur at a specific time, conditioned on a certain state; and

3. the initial probability state distribution $\boldsymbol{\pi} = \{\pi_i\}$, $\pi_i = P[q_1 = S_i]$, $i = 1, 2, \ldots, n$, which denotes the initial probabilities (i.e., at $t = 1$) of being at each state.

In order to represent all the parameters of an HMM, the notation $\lambda = (\mathbf{A}, \mathbf{B}, \boldsymbol{\pi})$ is typically used.

Given an observation sequence $O = \mathbf{O}_1\mathbf{O}_2 \ldots \mathbf{O}_T$, $\mathbf{O}_t \in V$, $t = 1, 2 \ldots, T$ (T denotes the length of the observation period), the most efficient method to estimate the parameter set λ is implemented via the Baum-Welch iterative algorithm (see, for example, Rabiner (1989)), which provides local maxima of the probability $P[O|\lambda]$, as there is no analytical solution to the problem of maximizing the probability of the observation sequence. In addition, HMMs can also be used for the prediction of the state based on the well-known formula for Markov chains, i.e.,

$$\boldsymbol{\pi}_t = \boldsymbol{\pi}\mathbf{A}^t \ , \tag{1}$$

where $\boldsymbol{\pi}_t$ is the state distribution at time t. Relation (1) states that the probability of being in a state at time t is determined by the transition probability matrix and the initial state probability distribution.

3.2 Threat Assessment based on HMMs

This work proposes to estimate the threat level regarding a particular situation (e.g., public event), at each time step, based on the use of an HMM framework. By defining threat levels, and not simply raising alarms whenever something suspicious is identified, the security state is periodically estimated. This estimation can be of considerable importance, since it may result in supporting decisions to take precautionary measures in case the threat level starts increasing considerably, thus saving human and monetary resources, while avoiding false alarms.

In our approach, the threat level of a situation is considered to be a hidden state, and the hidden process represents the threat level of a situation which can be estimated ("revealed") via a sequence of observations. Based on the aforementioned assumptions, the state space of the proposed HMM for the assessment of threat in a situation is denoted as $S = \{S_1, S_2, \ldots, S_n\}$, where n is the number of the defined hidden threat levels. Without loss of generality, the number of threat levels could be assumed to be $n = 3$ corresponding to:

- Low (L): an attack is unlikely;
- Moderate (M): an attack is likely; and
- High (H): an attack is highly likely.

Of course, any number of threat levels can be modeled.

The state space of the proposed HMM is defined as $S = \{S_1, S_2, S_3\} = \{L, M, H\}$ and X_t, $t = 1, \ldots, T$ denotes the hidden state at time t which corresponds to the threat level. Moreover, the states communicate with each other, meaning that there are non-zero transition probabilities between the defined threat levels as shown in Fig. 1, where the direction of arrows denotes the existence of non-zero transition probabilities from one hidden state to another at a given time step.

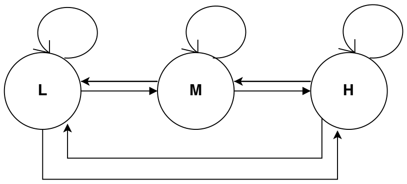


Figure 1: Markov chain for the hidden threat levels.

Considering the observation process of the proposed HMM for the estimation of the threat level, this may include risk factors that are assumed to affect the security status of a situation, such as the detections of suspicious incidents/moves based on cameras/sensors. The observation vector $\mathbf{O}_t$ produced at time t is defined to be of the form $\mathbf{O}_t = (O_{t,1}, O_{t,2}, \dots, O_{t,k})$ and each of the k entries in $\mathbf{O}_t$ corresponds to the value of a risk factor at time t, i.e., $\mathbf{O}_t \in V = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$, where $\mathbf{v}_i$, $i = 1, 2, \dots, m$ denotes the m possible observation vectors produced at time t.

The components of the parameter set $\lambda = (\mathbf{A}, \mathbf{B}, \boldsymbol{\pi})$ are of the form:

$$\mathbf{A} = \begin{pmatrix} \mathrm{a}_{11} & \mathrm{a}_{12} & \mathrm{a}_{13} \\ \mathrm{a}_{21} & \mathrm{a}_{22} & \mathrm{a}_{23} \\ \mathrm{a}_{31} & \mathrm{a}_{32} & \mathrm{a}_{33} \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} P[O_t{=}\mathbf{v}_1|q_t{=}S_1] & P[O_t{=}\mathbf{v}_2|q_t{=}S_1] & \dots & P[O_t{=}\mathbf{v}_m|q_t{=}S_1] \\ P[O_t{=}\mathbf{v}_1|q_t{=}S_2] & P[O_t{=}\mathbf{v}_2|q_t{=}S_2] & \dots & P[O_t{=}\mathbf{v}_m|q_t{=}S_2] \\ P[O_t{=}\mathbf{v}_1|q_t{=}S_3] & P[O_t{=}\mathbf{v}_2|q_t{=}S_3] & \dots & P[O_t{=}\mathbf{v}_m|q_t{=}S_3] \end{pmatrix} \text{ and}$$

$$\boldsymbol{\pi} = (\pi_L, \pi_M, \pi_H).$$

The structure of the proposed HMM is illustrated in Fig. 2. At discrete time t, the hidden Markovian process X_t of threat level is assumed to be at some state, and an observation $\mathbf{O}_t$ is generated according to the emission probability matrix $\mathbf{B}$. Then, the hidden process changes its state based on the transition probability matrix $\mathbf{A}$. The parameters $\mathbf{A}$, $\mathbf{B}$, and $\boldsymbol{\pi}$ can be estimated via the Baum-Welch algorithm based on historical data, which consist of a sequence of threat levels regarding a situation caused by a sequence of observations. If no such data are available, domain knowledge by experts in the field (such as security practitioners and Law Enforcement) can be leveraged for providing estimates for these parameters.

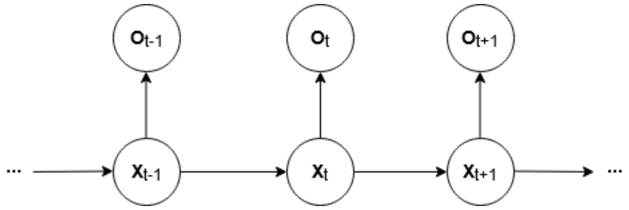


Figure 2: Structure of the proposed HMM.

The output of the proposed HMM is expected to be the most probable hidden threat level at time t, conditional on the observation sequence until time t. In other words, the posterior probability $\gamma_{t,i} = P[S_i|\mathbf{O}_1\mathbf{O}_2\ldots\mathbf{O}_t]$, $i = 1, 2, 3$, is calculated at each time step t and denotes the likelihood of being in state S_i at time t, conditional on the observation sequence until this time. The calculation of the posterior probability depends on the calculation of the forward probability denoted by $\alpha_{t,i} = P[\mathbf{O}_1\mathbf{O}_2\ldots\mathbf{O}_t, q_t = S_i|\lambda]$, $i = 1, 2, 3$, as demonstrated in Algorithm 1. It is noted that Algorithm 1 is given in the general case where n states (i.e., threat levels) are considered.

Algorithm 1 Calculation of the posterior probability

Input: $\lambda = (\mathbf{A}, \mathbf{B}, \boldsymbol{\pi})$, $\mathbf{O}_t$
Output: $\boldsymbol{\gamma}_t$

```
for $i = 1$ to $n$ do
    if $t = 1$ then
        $\alpha_{t,i} \leftarrow b_i(\mathbf{O}_t)\pi_i$
    else
        $\alpha_{t,i} \leftarrow b_i(\mathbf{O}_t)\sum_{j=1}^{n}\alpha_{t-1,j}\mathrm{a}_{ji}$
    end if
    $\gamma_{t,i} \leftarrow \frac{\alpha_{t,i}}{\sum_{j=1}^{n}\alpha_{t,j}}$
end for
return $\boldsymbol{\gamma}_t$
```

It should be highlighted that the proposed model adopts a probabilistic approach for the estimation of the threat level at each time step. Moreover, the dynamic evolution of the threat level over time is “revealed”, as the estimation of the hidden state at time t depends on the past observations.

Based on the estimation of the threat level at each time step, along with its posterior probability, we could also gain more information concerning the security state of a situation by defining costs for each hidden state (i.e., threat level). The term “cost” in this case could be interpreted as an indicator of the vulnerability of the security situation, reflecting that as the threat level increases, the cost of the possible consequences will increase too. For example, more human resources are anticipated to be used to handle a situation where the threat level is estimated as high, and more damages/losses are expected to be caused at the same level. Therefore, it is assumed that a cost C_i is attributed to the hidden state S_i, $i = 1, 2, 3$. In our case a cost vector is defined as $\mathbf{C} = (C_1, C_2, C_3) = (C_L, C_M, C_H)$, where C_L, C_M, C_H stand for the costs assigned to the hidden states Low, Moderate, and High, respectively. Moreover, it is (reasonably) assumed that $C_L < C_M < C_H$.

Based on the aforementioned approach, the mean value of the cost at each time t can be considered to be a risk score denoted by R_t, i.e.,

$$R_t = \sum_{i=1}^{3} \gamma_{t,i} C_i \ , \tag{2}$$

where $\gamma_{t,i}$, $i = 1, 2, 3$, denotes the posterior probability at time t. The minimum value of R_t is given by relation

$$min(R_t) = 1 \times C_L + 0 \times C_M + 0 \times C_H \ , \tag{3}$$

and the maximum value by relation

$$max(R_t) = 0 \times C_L + 0 \times C_M + 1 \times C_H \ . \tag{4}$$

The aforementioned approach can also be adopted in any situation where the observations are considered to be noisy. Next, an application of the proposed methodology is presented considering the assessment of threat in a public event based on the outputs of visual content analysis.

4 THREAT ASSESSMENT BASED ON VISUAL CONTENT ANALYSIS

This section presents an application of the proposed HMM methodology towards the estimation of the threat level in a public event, at each time step, by considering as risk factors the outputs (observations) of visual analysis (VA) processes.

4.1 Visual Analysis Processes

In this section, the observation vectors related to the analysis of visual content that are taken into consideration by the proposed framework for the assessment of threat are presented. These observations are considered to be recorded at discrete time steps, by one or more surveillance cameras (sensors), and extracted based on the following VA processes:

(i) *object detection*, which focuses on identifying and locating a predefined set of objects of interest (see, for example, Bochkovskiy et al. (2020)),

(ii) *face recognition*, which is able to identify specific individuals on the basis of their faces (see, for example, Learned-Miller et al. (2016)),

(iii) *activity recognition*, which involves recognizing actions of interest performed for instance by humans and vehicles (see, for example, Jobanputra et al. (2019)), and

(iv) *crowd violence detection*, which focuses on detecting outbreaks of crowd violence (see, for example, Gkountakos et al. (2020)).

Regarding the *object detection (OD)* process, objects that could be of interest (depending on the context) are, for example, knives, firearms, backpacks, bottles, etc. Taking into consideration the importance of the different objects based on the effect they may have on the security status, it can be suggested to assign different weights to different objects. Assuming that there are p object types of interest, w_i denotes the weight assigned to every object that belongs to the object type i, $i = 1, 2, \ldots, p$, and it is assumed without loss of generality that $w_1 \leq w_2 \leq \cdots \leq w_p$ based on the effect of the object type i to the security status of a situation. A (threat) score which takes into consideration the number of different objects detected, their weights, and the confidence scores for each detection is proposed by relation (5) as follows:

$$TS_{t,OD} = \sum_{i=1}^{s_1} CS_i w_1 + \cdots + \sum_{i=1}^{s_p} CS_i w_p \ , \tag{5}$$

where

- s_i: the number of objects detected by the visual analysis process that belong to the object type i, $i = 1, 2, \ldots, p$;
- CS_i: the confidence score of the i-detected object of interest as determined by the visual content analysis process for object detection;
- w_i: the assigned weight to the object of type $i = 1, 2, \ldots, p$.

High values of $TS_{t,OD}$ (based on the selected weights for the objects of interest) may indicate an increasing threat level in a situation that should be paid attention to.

Regarding the *activity recognition (AR)* process, activities that could indicate suspicious acts when performed in a specific context may include, for instance, "person walking fast", "person coming out from a building from illegal entrance", "person driving dangerously", etc. Similarly to the OD process, different weights could be assigned to different types of activities concerning their importance and impact on threat level. Assuming that there are l activity types of interest, w_i denotes the weight assigned to every activity that belongs to the activity type i, $i = 1, 2, \ldots, l$, and it is assumed without loss of generality that $w_1 \leq w_2 \leq \cdots \leq w_l$ based on the effect of the activity type i to the security status of a situation. A (threat) score similar to the one illustrated in relation (5) is proposed as follows:

$$TS_{t,AR} = \sum_{i=1}^{r_1} CS_i w_1 + \cdots + \sum_{i=1}^{r_l} CS_i w_l \ , \tag{6}$$

where

- r_i: the number of activities recognized by the visual analysis process that belong to the activity type i, $i = 1, 2, \ldots, l$;
- CS_i: the confidence score of the i-recognized activity of interest as determined by the visual content analysis process for activity recognition;

- w_i: the assigned weight to the activity of type $i = 1, 2, \ldots, l$.

As also noted for relation (5), high values of $TS_{t,AR}$ in relation (6) (based on the selected weights for the activities of interest) may indicate an increasing threat level in a situation that should be paid attention to.

Finally, as regards the *face recognition (FR)* and *crowd violence detection (CVD)* processes, the recognition or detection of at least one person of interest or at least one crowd violent move in a public event, respectively, can be considered to affect significantly the security status of the situation.

Next, an HMM model is developed for the assessment of threat based on the outputs of the VA processes.

4.2 HMM-based Threat Assessment using Visual Content Analysis

In this section the proposed HMM model is presented for the estimation of the threat level at each time step based on the outcomes of the VA processes described in Section 4.1. At first the estimation is based on the data acquired from one surveillance camera (Section 4.2.1), and then a method is proposed to take into consideration the outputs of multiple cameras (Section 4.2.2).

4.2.1 Threat Assessment based on a Single Surveillance Camera

In this section, an HMM model is developed for the estimation of the threat level of a situation based on the outputs of the VA analysis components taking into consideration the data obtained from a single camera. In the proposed HMM constructed for the assessment of threat based on the outcome of the four VA processes, the observation produced at time t is considered to be a four-dimensional vector $\mathbf{O}_t = (O_{t,1}, O_{t,2}, O_{t,3}, O_{t,4})$, where $O_{t,1}$ stands for OD, $O_{t,2}$ stands for FR, $O_{t,3}$ stands for AR, and $O_{t,4}$ stands for CVD.

Specifically, as regards OD (i.e., the first entry of $\mathbf{O}_t$), two different options are defined: (1) $S_{t,OD} < a_{OD}$, (2) $S_{t,OD} \geq a_{OD}$, where a_{OD} is a threshold defined for the score given in relation (5). To clarify the values that could be used for the threshold a_{OD} an example is given. In this example, the objects of interest are bottles, backpacks, knives, and firearms, and the related weights are presented in Table 1. In this case, we can set $a_{OD} = 2.5$

based on the hypothesis that the detection of one knife or firearm with confidence score 0.5 constitutes a considerable threat (the confidence score is related to the accuracy of the related algorithms used for OD). It is noted that any number of different types of objects can be used; this will not affect the total number of parameters in the proposed HMM and consequently the computational cost regarding the periodical estimation of the threat level, since the number of different types of objects and their respective weights (from a security perspective), eventually serve as inputs to relation (5) to derive the relevant threat score with the two defined options in terms of the output.

Table 1: Weights assigned to the objects of interest.

Objects of interest	**Weight**
Bottle	1
Backpack	2
Knife	5
Firearm	5

The use of relation (5) as the first entry of the observation vector in the proposed HMM allows the assignment of non-zero probabilities not only to the detection of objects that constitute a serious threat and could cause a change in the security status, such as knives or firearms, but also to a combination of objects being observed that seemingly could not constitute a serious threat when observed on their own, such as a considerable number of bottles or backpacks.

Regarding FR and thus the second entry of $\mathbf{O}_t$, two different options are defined:

1. all persons of interest are recognized with a confidence score $CS < a_{FR}$,

2. at least one person of interest is recognized with a confidence score $CS \geq a_{FR}$,

where $a_{FR} \in [0, 1]$ is a threshold defined for the recognition of persons of interest.

As for AR, i.e., the third entry of $\mathbf{O}_t$, the following two options are defined: (1) $S_{t,AR} < a_{AR}$, (2) $S_{t,AR} \geq a_{AR}$, where a_{AR} is a threshold defined for the score given in relation (6). To clarify the values that could be used for the threshold a_{AR} an example is given. In this example the activities of interest are “person walking fast”, “person coming out from a building from illegal entrance” and “person driving dangerously”, and the related weights are presented in Table 2. In this case, we can set $a_{AR} = 3$ based on the hypothesis that the detection of two people at time t coming out from an illegal entrance with confidence score 0.5 constitutes a considerable threat (the confidence score is related to the accuracy of the related algorithms used for AR). Similar to the OD case, it is noted that any number of different types of activities can be used; this will not affect the total number of parameters in the proposed HMM and consequently the computational cost regarding the periodical estimation of the threat level, since the different types of activities and their respective weights (from a security perspective) eventually serve as inputs to relation (6) to provide an estimation of the threat score with the two defined options in terms of the output.

Table 2: Weights assigned to the activities of interest.

Activities of interest	**Weight**
Person walking fast	1
Person coming out from an illegal entrance	3
Person driving dangerously	4

Similarly to the OD entry in the observation vector, the use of relation (6) as the third entry of the observation vector in the proposed HMM allows the assignment of non-zero probabilities to a combination of recognized activities that seemingly could not affect the security status.

Finally, regarding CVD, and thus the fourth entry of $\mathbf{O}_t$, the following two options are defined:

1. all the crowd violence moves of interest are detected with a confidence score $CS < a_{CVD}$,
2. at least one crowd violence move of interest is detected with a confidence score $CS \geq a_{CVD}$,

where $a_{CVD} \in [0, 1]$ is a threshold defined for the detection of crowd violence moves of interest.

The thresholds a_{FR} and a_{CVD} should be defined based on the accuracy of the algorithms used for providing the results in the respective visual processes. For example, in the case of FR, the threshold a_{FR} could be determined based on the mean value of the confidence scores of true positives related to the algorithm that is used. The same applies to the

Table 3: Observation vectors for VA

Observation	$\mathbf{v}_1$	$\mathbf{v}_2$	$\mathbf{v}_3$	$\mathbf{v}_4$
Value	$(1,1,1,1)$	$(2,1,1,1)$	$(1,2,1,1)$	$(1,1,2,1)$
Observation	$\mathbf{v}_5$	$\mathbf{v}_6$	$\mathbf{v}_7$	$\mathbf{v}_8$
Value	$(1,1,1,2)$	$(2,2,1,1)$	$(2,1,2,1)$	$(2,1,1,2)$
Observation	$\mathbf{v}_9$	$\mathbf{v}_{10}$	$\mathbf{v}_{11}$	$\mathbf{v}_{12}$
Value	$(1,2,2,1)$	$(1,2,1,2)$	$(1,1,2,2)$	$(2,2,2,1)$
Observation	$\mathbf{v}_{13}$	$\mathbf{v}_{14}$	$\mathbf{v}_{15}$	$\mathbf{v}_{16}$
Value	$(2,1,2,2)$	$(2,2,1,2)$	$(1,2,2,2)$	$(2,2,2,2)$

determination of a_{CVD}.

Taking into consideration that these data may contain noise, the model proposed based on the HMM framework results in filtering the noise by using probabilistic reasoning (see the transition and emission probability matrices A_{VA} and B_{VA}, respectively).

Overall, there are 16 different possible observation vectors $\mathbf{O}_t$ that can be produced at each time step, i.e., $\mathbf{O}_t \in V = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{16}\}$, which are defined at Table 3. The values 1 and 2 that are assigned to the components of the observation vector $\mathbf{v}_i$, $i = 1, 2, \ldots, 16$ in Table 3 denote the occurrence of the first and the second defined option respectively, regarding the OD, FR, AR, and CVD processes.

As mentioned in Section 3.2, the hidden process of the proposed HMM represents the threat level regarding a public event, and the state space is defined as $S = \{S_1, S_2, S_3\} = \{L, M, H\}$, in which the states communicate with each other (see Fig. 1). Therefore, the constructed HMM in this case is defined by the triplet $\lambda_{VA} = (\mathbf{A}_{VA}, \mathbf{B}_{VA}, \boldsymbol{\pi}_{VA})$ and the parameters are of the form:

$$\mathbf{A}_{VA} = \begin{pmatrix} \mathrm{a}_{11} & \mathrm{a}_{12} & \mathrm{a}_{13} \\ \mathrm{a}_{21} & \mathrm{a}_{22} & \mathrm{a}_{23} \\ \mathrm{a}_{31} & \mathrm{a}_{32} & \mathrm{a}_{33} \end{pmatrix},$$

$$\mathbf{B}_{VA} = \begin{pmatrix} P[O_t{=}\mathbf{v}_1|q_t{=}S_1] & P[O_t{=}\mathbf{v}_2|q_t{=}S_1] & \ldots & P[O_t{=}\mathbf{v}_{16}|q_t{=}S_1] \\ P[O_t{=}\mathbf{v}_1|q_t{=}S_2] & P[O_t{=}\mathbf{v}_2|q_t{=}S_2] & \ldots & P[O_t{=}\mathbf{v}_{16}|q_t{=}S_2] \\ P[O_t{=}\mathbf{v}_1|q_t{=}S_3] & P[O_t{=}\mathbf{v}_2|q_t{=}S_3] & \ldots & P[O_t{=}\mathbf{v}_{16}|q_t{=}S_3] \end{pmatrix} \text{ and}$$

$$\boldsymbol{\pi}_{VA} = (\pi_{L,VA}, \pi_{M,VA}, \pi_{H,VA}).$$

As discussed, the parameters $\mathbf{A}_{VA}$, $\mathbf{B}_{VA}$, and $\boldsymbol{\pi}_{VA}$ can be estimated via the Baum-Welch algorithm based on past data provided by the cameras. However, they can also be assigned manually in collaboration with security operators and Law Enforcement that have relevant experience and domain expertise; this alternative could be an option in case data for estimating the parameters are not easily accessible. For example, it could be assumed that $P[\mathbf{O}_t = \mathbf{v}_{16}|q_t = S_1] \approx 0$, i.e., it is highly unlikely to detect high scores for all four visual processes, given that the threat level is low. Using Algorithm 1, the output of the constructed HMM in this case would provide the most probable (hidden) threat level of the public event at time t conditional on the observation sequence that arises from the visual analysis processes until this time.

4.2.2 Threat Assessment based on Multiple Surveillance Cameras

In terms of surveillance, it is expected that more than one cameras would be available for the surveillance of a situation. Assuming that there are z cameras used, an HMM can be constructed for each one of the cameras. A question arises whether the threat levels estimated by each camera could be combined in order to estimate the "overall" threat level of the situation. For that purpose, two alternatives could be suggested.

The first alternative adopts an approach that uses common reasoning. That is to say, the "overall" level of threat in a situation is considered to be the maximum level of threat estimated by the HMMs applied to the z available cameras which provide coverage for a specific event.

The second alternative adopts a more probabilistic approach for defining the "overall" threat level by using a score similar to the one defined in relation (2). In other words, the definition of costs concerning the hidden states (i.e., threat levels) is proposed. In our case a cost vector is defined as $\mathbf{C}_{VA} = (C_{L,VA}, C_{M,VA}, C_{H,VA})$, where $C_{L,VA}$, $C_{M,VA}$, $C_{H,VA}$ stand for the costs assigned to the states Low, Moderate, and High, respectively. Moreover, it is assumed that $C_{L,VA} < C_{M,VA} < C_{H,VA}$.

Based on the aforementioned approach, we could define the risk score given in relation (2) for each HMM per camera (the parameters $\mathbf{A}_{VA}$, $\mathbf{B}_{VA}$, $\boldsymbol{\pi}_{VA}$, and $\mathbf{C}_{VA}$ are assumed to be the same for all HMMs), i.e.,

$$R_{t,j} = \sum_{i=1}^{3} \gamma_{t,i} C_{i,VA} \ , \ j = 1, 2 \ldots, z \ , \tag{7}$$

where $\gamma_{t,i}$, $i = 1, 2, 3$, denotes the posterior probability at time t. Relation (7) produces the mean value for the cost concerning each camera at time t. The total risk of the system at time t (concerning all the z cameras) can be calculated by the relation

$$R_{t,VA} = \sum_{j=1}^{z} R_{t,j} \ . \tag{8}$$

The minimum value of the risk score based on relation (7) that could be assigned to each camera is defined as

$$R_{min} = 1 \times C_{L,VA} + 0 \times C_{M,VA} + 0 \times C_{H,VA} \ , \tag{9}$$

and the maximum value is defined as

$$R_{max} = 0 \times C_{L,VA} + 0 \times C_{M,VA} + 1 \times C_{H,VA} \ . \tag{10}$$

Consequently the minimum and maximum risk score at each time step for the whole system with the z cameras based on relations (9) and (10) are defined as

$$min(R_{t,VA}) = z \times R_{min}$$

and

$$max(R_{t,VA}) = z \times R_{max} \ .$$

Next, an illustrative example is presented concerning the application of the proposed model for the assessment of threat in a public event.

4.3 Illustrative Example

In this section, an illustrative example of the model for one surveillance camera (Section 4.2.1) is presented in order to provide a more comprehensive picture of the proposed framework process. To this end, simulated data are used, as data from surveillance cameras are not publicly available due to their sensitivity; such data though are typically available to Law Enforcement operators. The estimation of the model's parameters could be further improved based on the feedback provided by domain experts (such as Law Enforcement Agents and security practitioners).

With regard to the model described in Section 4.2.1, which builds upon the outcome of various visual analysis processes, the time step for the estimation process should be set to a value reflecting real operational needs. For example, it could be set to $t = 10sec$ considering the fact that a modification in the threat level of a public event based on the visual analysis processes can be caused within a very short time.

Moreover, attempting to have a realistic model for the provision of simulated data and taking also into consideration experts' view for this issue, the values of the parameter set $\lambda_{VA} = (\mathbf{A}_{VA}, \mathbf{B}_{VA}, \boldsymbol{\pi}_{VA})$ of the HMM could be suggested to be

$$\boldsymbol{\pi}_{VA} = (1, 0, 0),$$

$$\mathbf{A}_{VA} = \begin{pmatrix} 0.9764054 & 0.02357956 & 1.49999\times10^{-5} \\ 0.0065439 & 0.9734561 & 0.02 \\ 3.002962\times10^{-6} & 3.096996\times10^{-6} & 0.999994 \end{pmatrix},$$

while the values of matrix $\mathbf{B}_{VA}$ are presented in Table 4.

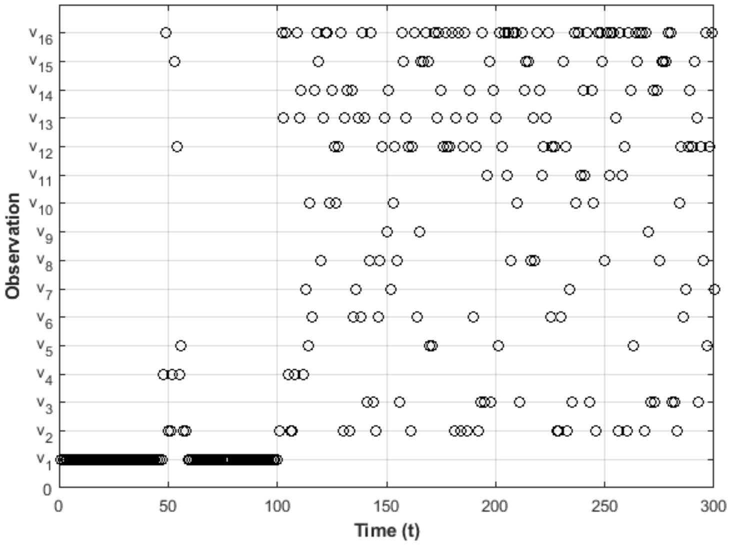
Based on the defined parameters for the HMM, a simulated path of 300 observations is generated (see Fig. 3a) in order to have a comprehensive view about the way the proposed method works; of course, more than 300 observations vectors can be used. As illustrated in Fig. 3a, an observation vector $\mathbf{v}_i$, $i = 1, 2, \ldots, 16$ is produced at each time step. The estimated threat levels for that path (see Algorithm 1) are illustrated in Fig. 3b where it can be seen that the threat level alternates among Low, Moderate, and High. The fact that the threat level is estimated as high for the last part of the sequence of observations (see Fig. 3b) does not imply that the threat level cannot be estimated as moderate or low once more observations become available; this result simply reflects the specific simulated underlying data (see Fig. 3a).

Table 4: Values of $\mathbf{B}_{VA}$ per row.

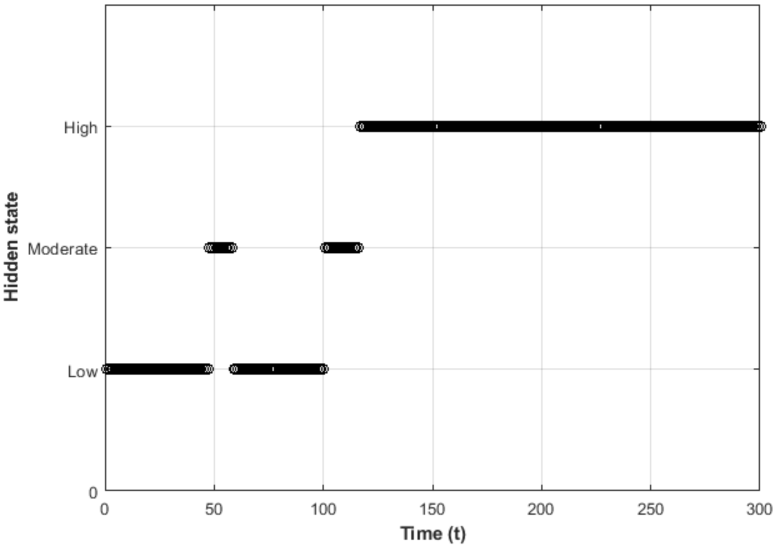
$\mathbf{O}_t$	$P[\mathbf{O}_t = \mathbf{v}_i \vert q_t = S_1]$	$P[\mathbf{O}_t = \mathbf{v}_i \vert q_t = S_2]$	$P[\mathbf{O}_t = \mathbf{v}_i \vert q_t = S_3]$
$\mathbf{v}_1$	0.99584	10^{-5}	10^{-5}
$\mathbf{v}_2$	0.001	0.1	0.099
$\mathbf{v}_3$	0.001	0.02	0.083
$\mathbf{v}_4$	0.001	0.46998	0.001
$\mathbf{v}_5$	10^{-5}	0.02	0.032
$\mathbf{v}_6$	10^{-5}	0.01	0.032
$\mathbf{v}_7$	0.001	0.07	0.032
$\mathbf{v}_8$	10^{-5}	0.01	0.032
$\mathbf{v}_9$	10^{-5}	0.01	0.032
$\mathbf{v}_{10}$	10^{-5}	0.01	0.032
$\mathbf{v}_{11}$	10^{-5}	0.01	0.032
$\mathbf{v}_{12}$	2.5×10^{-5}	0.054	0.083
$\mathbf{v}_{13}$	2.5×10^{-5}	0.054	0.083
$\mathbf{v}_{14}$	2.5×10^{-5}	0.054	0.083
$\mathbf{v}_{15}$	2.5×10^{-5}	0.054	0.083
$\mathbf{v}_{16}$	0	0.054	0.26099

Moreover, if the cost vector assigned to the states of the proposed HMM is set to be $\mathbf{C} = (1, 5, 10)$, the risk score at each time step based on relation (7) is shown in Fig. 4. The choice of the suggested values in the cost vector is based on the idea that cost value assigned to each level increases as the threat level increases. It is shown in Fig. 3b and 4 that the estimation of the threat level and the risk score based on the simulated observation sequence (see Fig. 3a) are in accordance to the effect that an observation vector may have on the security status of the situation based on past observations. The revelation of the dynamic evolution of the threat level at (near) real time (as shown in Fig. 3b and 4) is considerably useful, as it may result in taking precautionary measures when an upward trend is observed (for example when the estimation of the threat level has already reached the moderate level) in order to handle potential threats.

Finally, for the implementation of Algorithm 1 for a simulated path of 300 observations and the three defined threat levels, we used the software environment of R-4.0.1, while the time required for the execution of the algorithm was approximately 0.7 sec with Intel Core i5-3210M CPU @ 2.50GHz, 6.00 GB (RAM).



(a)



(b)

Figure 3: (a) Simulated path of 300 observations, (b) Estimated hidden threat level (time step t=10sec)

5 DISCUSSION

In this work an HMM-based approach is proposed for the estimation of the threat level in situations like public events. The underlying concept is the consideration of the threat level

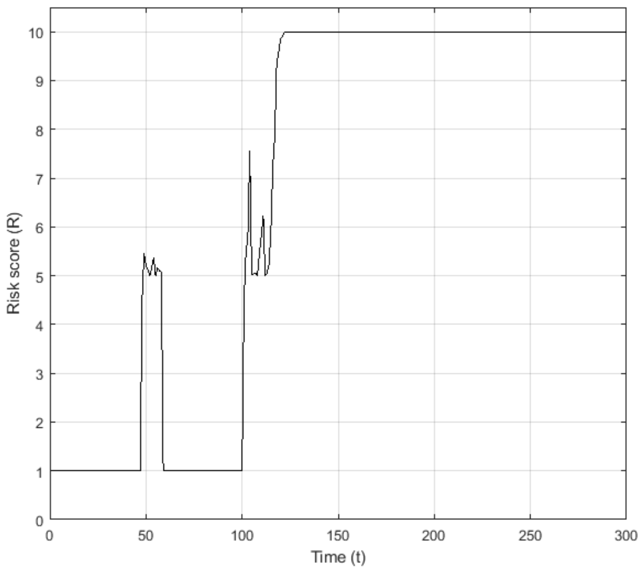


Figure 4: Estimation of R_t with time step $t = 10sec$.

as a hidden state which is estimated ("revealed") via a sequence of observations, including factors that could potentially affect the security status of the situation of interest.

One of the main advantages of this approach is that it allows for the dynamic estimation of the threat level over time, since past observations are also taken into account for the threat assessment at each time step. Moreover, it results in providing a rating scale of the threat at each time, based on the observation processes of interest. In this work, a rating scale of three threat levels (low, moderate, and high) is adopted, but additional threat levels can be considered in cases where such finer-grained considerations support better the purpose and scope of the threat assessment framework. In addition, due to the probabilistic reasoning of the proposed method, it can also be used in cases where the underlying data are noisy aiming to filter the noise and minimise its effect in the estimation process. Finally, the well-known properties of Markov chains could also be exploited for the prediction of the hidden state.

Taking into consideration the abovementioned points, it could be argued that the proposed threat assessment framework may prove to be considerably useful in enhancing decision making by security personnel regarding the taking of precautionary measures in case the threat level appears to follow an upward trajectory, even before it reaches the highest level. This eventually may contribute to the reduction of human effort and costs which is of vital importance towards the effective management of resources for the protection of public spaces, critical infrastructures, and enterprises.

Besides its many strengths, this work also has some limitations. First, relevant public datasets to be used for the estimation of the parameters may not be available for the particular application domain of the proposed threat assessment framework, since surveillance data are not typically publicly available due to their sensitivity. Nevertheless, even in the absence of such data, the parameters can still be defined in collaboration with domain experts.

Moreover, another limitation considers the size of the emission probability matrix and consequently the (computational) cost regarding the estimation of its entries when taking into consideration more parameters for the assessment of the threat level. For instance, in this work, the size of the emission probability matrix is 3×16, since there are three threat levels defined and sixteen different observation vectors based on the four visual analysis processes. However, in case additional features are considered, the size will become even larger, resulting in an increase in the number of parameters that need to be estimated. In the case that these parameters are provided by domain experts, they may find such a task challenging. In the case that available datasets are used for such purposes, they will need to be considerably large in size in order to achieve an accurate estimation for a large number of parameters; this may be a challenging issue when considering security data. To handle this limitation and control the matrix size, a grouping of features can be implemented and different HMMs can be applied to each of the constructed groups similarly to the approach described in Section 4.2.2 about fusing the outputs from multiple surveillance cameras.

6 CONCLUSIONS

This work proposed the adoption of an HMM in order to provide an assessment of the threat level regarding a situation. The threat level is assumed to be a hidden state and, therefore, the hidden process of the proposed HMM corresponds to the level of threat. The observation process could include factors that are considered to cause changes in the security status of a situation. The application of the proposed methodology was analyzed in a use case based on the automated analysis of visual content (namely object detection, face recognition, activity recognition, and crowd violence detection) concerning the estimation of the threat level in a public event.

Overall, the use of HMMs adopts a probabilistic approach in the assessment of threat, and results in "revealing" the dynamic evolution of the threat over time, while also providing a rating scale of the security status at each time; this is particularly useful for the provision of early warnings in case an upward evolution of the threat level is observed at (near) real time. Moreover, the proposed method can also be used for predictions due to the well known properties of Markov chains. Generally, due to its probabilistic reasoning, this approach can be used for the assessment of threat in cases where the observation process is noisy and there are non-zero probabilities for false positives/negatives.

Regarding next steps, since the estimation of the threat level in this work is mainly related to the security status of a situation, e.g. public event, more sources of information can also be taken into account for this estimation to combine them resulting in a more comprehensive overview of the existing threat.

References

Årnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M. E. G., & Knapskog, S. J. (2005). Real-time risk assessment with network sensors and intrusion detection systems. *International conference on computational and information science*, 388–397.

Årnes, A., Valeur, F., Vigna, G., & Kemmerer, R. A. (2006). Using hidden markov models to evaluate the risks of intrusions. *International Workshop on Recent Advances in Intrusion Detection*, 145–164.

Aung, N., Zhang, W., Dhelim, S., & Ai, Y. (2018). Accident prediction system based on hidden markov model for vehicular ad-hoc network in urban environments. *Information*, *9*(12), 311.

Aven, T., & Guikema, S. (2015). On the concept and definition of terrorism risk. *Risk analysis*, *35*(12), 2162–2171.

Bäuerle, N., & Ott, J. (2011). Markov decision processes with average-value-at-risk criteria. *Mathematical Methods of Operations Research*, *74*(3), 361–379.

Bobulski, J., & Adrjanowicz, L. (2013). Two-dimensional hidden markov models for pattern recognition. *International Conference on Artificial Intelligence and Soft Computing*, 515–523.

Bochkovskiy, A., Wang, C.-Y., & Liao, H.-Y. M. (2020). Yolov4: Optimal speed and accuracy of object detection. *arXiv preprint arXiv:2004.10934*.

Cappé, O., Moulines, E., & Rydén, T. (2006). *Inference in hidden markov models*. Springer Science & Business Media.

Chatterjee, S., & Abkowitz, M. D. (2011). A methodology for modeling regional terrorism risk. *Risk Analysis*, *31*(7), 1133–1140.

Dahlbom, A., & Helldin, T. (2013). Supporting threat evaluation through visual analytics. *2013 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 155–162.

Deshmukh, S., Rade, R., & Kazi, D. (2019). Attacker behaviour profiling using stochastic ensemble of hidden markov models. *arXiv preprint arXiv:1905.11824*.

Dillon-Merrill, R. L., Parnell, G. S., & Buckshaw, D. L. (2008). Logic trees: Fault, success, attack, event, probability, and decision trees. *Wiley Handbook of Science and Technology for Homeland Security*, 1–22.

Epaillard, E., & Bouguila, N. (2016). Proportional data modeling with hidden markov models based on generalized dirichlet and beta-liouville mixtures applied to anomaly detection in public areas. *Pattern Recognition*, *55*, 125–136.

Ezell, B. C., Bennett, S. P., Von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. *Risk Analysis*, *30*, 575–589.

Gkountakos, K., Ioannidis, K., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2020). A crowd analysis framework for detecting violence scenes. *Proceedings of the 2020 International Conference on Multimedia Retrieval*, 276–280.

Hudson, L. D., Ware, B. S., Laskey, K. B., & Mahoney, S. M. (2005). An application of bayesian networks to antiterrorism risk management for military planners, Technical Report, Department of Systems and Engineering and Operations Research, George Mason University.

Jobanputra, C., Bavishi, J., & Doshi, N. (2019). Human activity recognition: A survey. *Procedia Computer Science*, *155*, 698–703.

Kumar, S., & Tripathi, B. K. (2016). Modelling of threat evaluation for dynamic targets using bayesian network approach. *Procedia Technology*, *24*, 1268–1275.

Learned-Miller, E., Huang, G. B., RoyChowdhury, A., Li, H., & Hua, G. (2016). Labeled faces in the wild: A survey. In *Advances in face detection and facial image analysis* (pp. 189–248). Springer.

Li, W., & Guo, Z. (2009). Hidden markov model based real time network security quantification method. *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, *2*, 94–100.

Liu, S., & Liu, Y. (2016). Network security risk assessment method based on hmm and attack graph model. *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 517–522.

Norris, J. R. (1998). *Markov chains*. Cambridge University Press.

Ott, J. T. (2010). *A markov decision model for a surveillance application and risk-sensitive markov decision processes* (Doctoral dissertation). Fakultät für Mathematik, Karlsruher Instituts für Technologie.

Rabiner, L. R. (1989). A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, *77*(2), 257–286.

Rabiner, L. R. (1993). Fundamentals of speech recognition. *Fundamentals of speech recognition.*

Sendi, A. S., Dagenais, M., Jabbarifar, M., & Couture, M. (2012). Real time intrusion prediction based on optimized alerts with hidden markov model. *Journal of networks*, *7*(2), 311.

Souag, A., Salinesi, C., Wattiau, I., & Mouratidis, H. (2013). Using security and domain ontologies for security requirements analysis. *2013 IEEE 37th Annual Computer Software and Applications Conference Workshops*, 101–107.

Steinberg, A. N. (2009). Foundations of situation and threat assessment. *Handbook of multisensor data fusion: theory and practice*, 437–501.

Votsi, I., Limnios, N., Tsaklidis, G., & Papadimitriou, E. (2013). Hidden markov models revealing the stress field underlying the earthquake generation. *Physica A: Statistical Mechanics and its Applications*, *392*(13), 2868–2885.

Wang, C., Wu, J., Wang, X., & He, X. (2018). Application of the hidden markov model in a dynamic risk assessment of rainstorms in dalian, china. *Stochastic Environmental Research and Risk Assessment*, *32*(7), 2045–2056.

Wang, C., Li, K., & He, X. (2020). Network risk assessment based on baum welch algorithm and hmm. *Mobile Networks and Applications*, 1–8.

Wu, S., Zhang, Y., & Chen, X. (2018). Security assessment of dynamic networks with an approach of integrating semantic reasoning and attack graphs. *2018 IEEE 4th International Conference on Computer and Communications*, 1166–1174.

Wu, Z. (2010). A hidden markov model for earthquake declustering. *Journal of Geophysical Research: Solid Earth*, *115*(B3).

Xu, C., Wang, Y., & Ai, W. (2014). Situation assessment in the warships-airplanes joint operation based on parameter learning in bayesian network. *Proceedings of 2014 IEEE Chinese Guidance, Navigation and Control Conference*, 2604–2609.

Yu-Ting, D., Hai-Peng, Q., & Xi-Long, T. (2014). Real-time risk assessment based on hidden markov model and security configuration. *2014 International Conference on Information Science, Electronics and Electrical Engineering*, *3*, 1600–1603.