Big Data and Artificial Intelligence Solutions for in Home, Community and Territory Security

Ashok Reddy Singam
Indiana University
711 N Park Ave
Bloomington, Indiana 47408
asingam@iu.edu

Anil Ravi
Indiana University
711 N Park Ave
Bloomington, Indiana 47408
anilravi@iu.edu

ABSTRACT

Anti-social activities became the most significant threat to national security because of their potential to bring massive damage to our homes, public infrastructure, economy, and people. The existing systems and methods haven't reached the level of sophistication to be able to consolidate the large volumes of relevant data from variety of sources and demographics. The present video surveillance systems use static cameras at fixed locations inside/outside the house to provide alerts when any event detected. However, they are not intelligent enough to understand the context, recognizing the people faces and voices, and differentiate between family members and strangers etc. The limitations of data collection, data mining and adoption of artificial intelligence led to ineffective systems which are not as predictive as they should be.

The concept of having an intelligent "ear-and-eye" monitoring at the home to constantly observe the surroundings both inside and outside can protect the house and personnel much more safer way. By extending this capability to the neighborhood and city through collaboration would create safe cities across the world. The key differentiating capability from existing systems is to use a micro drone with integrated video and voice with environment sensors to process the voice and facial data with machine learning algorithms. The limited range micro drones can freely move around the house based on the voice and video analytics while learning the friends, family members and strangers.

The technology advancement allows integrating the video, audio and social media data of targeted regions (homes, public places and extended areas) for comprehensive security analysis. Such systems can use advanced statistical methods, image classification and machine learning algorithms to predict and prevent the threats based on the severity probability.

KEYWORDS

i523, HID333, HID337, Artificial Intelligence, Neural Networks, Machine Learning, Micro Drone

1 INTRODUCTION

It is widely believed that information technology will play an indispensable role in making the world safer by supporting intelligence and knowledge discovery through collecting, processing, analyzing, and utilizing terrorism and crime related data[**?**]. Social network analysis (SNA) has been widely explored to support intelligence and law enforcement agencies in investigating the terrorist and criminal social networks. It is valuable in identifying terrorists, suspect subgroups, and their communication patterns.

However, in the present world, the systems are disparately processing the data and the decisions/conclusions are being made without considering multiple dimensions of the context. The large corporations, nations, and intelligence agencies are using their individual systems in isolation but not taking integrated approach to solve the problems in their entirety due to their political and economic interests.

Analyzing the individual human behaviors, interactions, transactions, and actions is the key element in identifying the potential threat in advance. Generating and analyzing such data from individual homes and extending the concept to larger groups is the idea behind this discussion.

The current technologies allow to collect the data from individual homes and roll up to the communities, cities and then to the nations across the world. Since this involves with the personal data from people directly, it is required to follow privacy-preservation policies and methods enforced by local/national government agencies. By accessing the household level data of individuals video, voice, social media and other business transactional data would allow to characterize, analyze and assess the people behaviors and motives which can be maintained and processed as needed by Big Data systems. These systems are very complex in nature due to the variety, volume and velocity of the data, where the Big Data technologies will play a significant role in realizing them. In addition to data collection and mining, if artificial intelligence is applied to analyze and evaluate the data then the crime prediction and prevention would be feasible.

In order to realize such systems, one would need several technologies and sub-systems in various layers to effectively collect, transfer, mining, learning and analyze the data. In the following sections some of the technologies/sub-systems that can be used to achieve the objectives of proposed conceptual model are described. The discussion here consists of reviewing the available papers/systems related to security informatics and understanding the technologies and methods used. The gaps perceived in the review are attempted to solve by proposing a new concept.

2 HOME SECURITY CONCEPT

This section describes a proposed scalable security system concept, which can be extended to community, city and beyond. The conceptual model has multiple sub-systems coordinate with each other to establish a robust home security system. In this model, a micro-drone integrated with video and audio will continuously monitor the house both inside and outside. An autonomous dual micro-drone model will have capability to view the surrounding

with high resolution frame rates and transfer the data to edge processing unit and/or cloud based HDFS server. The social media data of housemates (e.g., E-mail, Facebook, Twitter, WhatsApp, and other web/mobile applications) gets integrated in to HDFS server.

This will establish a known context with complete information of individuals residing in the house by analyzing the contacts, communication exchange (phone calls, SMS, E-mails), trade transactions, and family/friends/foe information. With the combination of video, voice and social network data a comprehensive home security system can be achieved which not only protects the house but also individuals by having superior knowledge about all the activities. This will require Big Data infrastructure along with machine learning algorithms in various sub-systems.

This conceptual model can be realized with available technologies and can be architected such that it will become a basic building block for scalable system.

Some of the existing technology companies making us to believe realization of proposed concept:

- *Squadrone System*: A Pioneer in producing intelligent deep learning drones for real-time surveillance
- *Neurala*:A leader in deep learning and neural network software for drones
- *Nvidia*: The world leader in visual computing technologies and leading GPU manufacturer

2.1 Dual Micro-Drones with Video and Audio

The prevailing drone technology is reaching higher levels of sophistication allowing newer concepts to be realized in surveillance applications. In this proposed concept a micro-drone with integrated video, voice and environmental sensors (temperature, humidity, and accelerometers) can be designed along with learning algorithms to add intelligence. In the basic system, there will be two micro-drones to cover both in-side and out-side of the house (can consider adding more depending on the size of the house/facility) monitoring activities all the time. The drone hardware and software detects and recognize all moving objects through deep learning algorithms such as Regional Convolution Neural Networks (R-CNN). Li Wand and Dennis Sng[**?**] have reviewed the recent progress of deep learning in object detection, object tracking, face recognition, image classification and scene labeling. The deep models have significantly improved the performance in these areas, often approaching human capabilities. The reasons for this success are two-folded. First, big training data are becoming increasingly available (e.g. data streams from a multitude of sensors) for building up large deep neural networks. Second, new advanced hardware (e.g. GPU) has largely reduced the training time for deep networks.

The concept of micro-drone video and audio sub-system is to recognize human face and voice and establish the association. After the human object is created with face-voice association, the human characteristics, behaviors, social contacts, social media accounts, family/friends contact database and personal identification will be mapped. This person object (one of the housemate) will be constantly trained with large set of data during the learning period. Once the person object is matured with enough intelligence then the system will be ready for monitoring and analyzing the data of the person he/she actually mapped to. Multiple person objects will be created to map all the persons live in that house. The duo micro-drones are intelligent enough to recognize all the persons in the house and understand their behaviors, motives, actions, schedules, plans and their complete activities as time progresses.

These micro-drones freely move around the house to monitor the family, friends, foes, strangers, and people who ever happen to be in the house surroundings and visit to meet housemates. Micro-drones are smart enough to sense the people emotions based on the expressions, conversations and actions to predict the future consequences and get ready for protective actions (e.g., alerting appropriate people and agencies). Also, micro-drones are equipped with sensors to detect environment conditions (temperatures, wind, rain and humidity etc..,) to take good care of themselves by reaching back to dock/home stations while ensuring that security precautions are addressed.

Since micro-drones are autonomous with self-maneuvering and self-diagnostics capabilities, they will take care of self-charging, protecting themselves from being damaged by staying away from objects and people.

The technologies available to realize such a micro-drone consists of: autonomous multicopters, high resolution built-in 360 degree video cameras, high speed network link, high speed GPUs, environment sensors, software with machine learning algorithms for various capabilities discussed above.

2.2 Big Data Infrastructure for Data Handling

Big data can be acquired, stored, processed, and analyzed in many ways. The big data source has different characteristics, including the frequency, volume, velocity, type, and veracity of the data. In the proposed conceptual model, multiple sub-systems generate the big data from variety of sources such as video, voice, environment sensors (temperature, humidity, wind etc.). Also big data will be generated from all major social media accounts of individual house mates such as Twitter, Facebook, YouTube, Instagram, E-mails and WhatsApp in addition to GPS location, mobile phone calls and text messages.

The Big Data infrastructure would organize the data through multiple data layers such as collection hub, staging hub and Data Lake. Apache Hadoop has emerged as the de facto standard way of storing all of this *Big Data*, mostly in the form of commercial implementations from HortonWorks, Cloudera and MAPR. Associated technologies such as Flume, HBAse, Hive, Kafka, MapReduce, Spark and Storm offer different ways to get information into and out of Hadoop Distributed File Systems (HDFS) so it can be shared with analytics engines, enterprise applications and user interfaces.

2.3 Data Privacy Preservation Models

In the proposed conceptual system, multiple layers of sub-systems collect the individual home level information and uses anonymization models to preserve the privacy of individuals. The objective is hiding the sensitive personal information such as personal identities but publishing the rest of the data, an anonymized version of relational data. The data that will be sent out to be used for next level (community/region) fed to privacy preservation algorithms such as k-anonymity protection models which are being used in real-world systems known as ”Datafly”, ”-Argus” and ”k-Similar”.

The k-anonymity methods ensure that at least k records with respect to every set of quasi-identifier attributes are indistinguishable. There are other alternative methods such as l-diversity and m-invariance can be applied as well to apply different constraints on anonymity. For social network integration in to proposed system, models can use subgraph generalization approach to preserve the privacy, which has been discussed in the paper "Privacy-Preserved Social Network Integration and Analysis for Security Informatics"

2.4 Video Data Integration and Analysis

The high quality video image frames will be processed to analyze the situational awareness. Learning hierarchical representation of video image data by using deep architecture models is the key component of video analytics. By using the deep learning algorithms to perform object detection, object tracking, face recognition, image classification and scene labeling would enable to establish a comprehensive situational awareness in the home security context. For example, facial expressions manifest not only emotions but also allied actions, behavioral patterns and give a lot of useful data when it comes to helping law enforcement and forensics agencies. Video analytics can be achieved based on data curation, sentiment analysis, and other advanced solutions. Expressions like "happy", "sad", "angry", "scared", "surprised" or "neutral" form the basis of video analytics.

This method and approach can be extended to city and region levels by rolling up the data from individual homes. In the context of city and regional security, video analytics would help in people management, vehicle management, behavior monitoring. For example, in the public events deep learning enabled systems can perform crowd detection, queue management, people counting, people scattering, people tracking; in the vehicle management, systems can perform vehicle classification, traffic monitoring, license plate recognition, road data gathering. Also, behavior monitoring can be achieved through motion detection, vandalism detection, face detection, privacy masking, and suspicious activity detection. With the advent of new technologies in computing speed there are several Graphics Processing Units (GPU) integrated with high quality image sensors introduced by technology companies such as NVidia can be used in the conceptual model.

2.5 Voice Data Integration and Analysis

The live voice recording integrated with video analysis provides better and accurate insight in to situation awareness for predicting and preventing the potential threats much faster. Traditional voice analytics tools rely on keywords and phonetics. These solutions are not well enough in deriving context and relevancy. With big data and AI advancements, now it is even possible to analyze for things like stress levels, lies, emotional content and more from audio data. Deep learning is becoming a mainstream technology for speech recognition and has successfully replaced Gaussian mixtures for speech recognition and feature coding at an increasingly larger scale. Google's Speech Recognition API built using deep learning neural network algorithms is one of the voice analytics software available in the market, which can be used in the proposed conceptual model.

In the proposed conceptual model, the complete characterization of housemates can be performed using deep learning algorithms. This will help to recognize the voice of the persons within the house and build the context. Also, the learning algorithms continue refining the voice characterization of the persons and extend the voice database to other family members and friends. This key aspect of associating voice to the person would help resolving the contextual issues if any arises during behavior assessment.

2.6 Social Media Data Integration

In the conceptual model, along with the video and voice association, if the individual social media activity is monitored his/her behavior can be predicted to assess the motivations and potential actions. The social media accounts can be integrated in to big data system to collect the data from applications such as Facebook, Twitter, Instagram, WhatsApp, E-mails, and SMS etc.

By analyzing behaviors observed on social media, we can categorize these behaviors into individual and collective behavior. User activities on social media generate behavioral data, which is massive, expansive, and indicative of individual preferences, interests, opinions, and relationships. This behavioral data provides a new lens through which we can observe and analyze individual and collective behaviors of people.

Natural language processing (NLP) algorithms along with reasonable quantity of training data can lead to understand sentimental behavior, which is one of the key elements for security informatics. This capability can be applied to proposed conceptual model to ensure that system is analyzing the social network data.

2.7 Learning Algorithms and Predictive Analysis

The two critical machine learning algorithms needed to realize the proposed concept are for the face and voice recognition. Deep learning models are potential candidates for these two tasks. Deep learning architectures have different variants such as Deep Belief Networks (DBN)[**?**], Convolutional Neural Networks (CNN)[**?**], Deep Boltzmann Machines (DBM)[**?**] and Stacked Denoising Auto-Encoders (SDAE)[**?**], etc. The most attractive model is Convolutional Neural Networks which have achieved very promising results in both computer vision and speech recognition.

The ability to estimate the occurrence of future events using expertise, observation and intuition is critical to the human decision-making process. From a biophysical perspective, there is strong evidence that the neocortex provides a basic framework for memory and prediction in which human intelligence emerges as a process of pattern storage, recognition and projection rooted in our experience of the world and driven by perception and creativity. There is increasing consensus among cognitive psychologists that human decision making can be seen as a situation-action matching process which is context-bound and driven by experiential knowledge and intuition. Significant advances have been made in the integration of predictive modeling with social and behavioral factors, in both equation-based approaches, and probabilistic evidentiary reasoning approaches[**?**].

3 COMMUNITY DRONE NETWORK

The intelligent drone home security system would enable to provide comprehensive situational awareness at home level. The proposed drones are limited in their coverage area which is strictly enforced by regulatory/intelligence/government agencies. Since this inteli-drone is scalable to extend the coverage by just adding another device, it can be conceivable to create a network of inteli-drones to cover a given community. The community drone network is collection of security drones covering a specific region within a city which will ensure that relevant data is delivered to law enforcement and intelligence agencies. This would require one of the drones in the network to be nominated as *Gateway Drone* to communicate with law enforcement/intelligence agencies. Each drone will have the capability to become a *Gateway Drone* as needed. When the new drone is installed it will automatically look for existing *Gateway Drone* in that community, which if exists then it will join the network and gets registered. If no *Gateway Drone* is recognized, the new drone claims or becomes *Gateway Drone*.

3.1 Gateway Drone

The *Gateway Drone* represents a specific community, which will maintain all the home addresses within that community along with associated personnel per the privacy preservation policies set forth by the regulatory/intelligence agencies. The *Gateway Drone* performs dual function (1) ensure that constantly communicates with *Police Drone* or *City Drone* and (2) monitor its own house security aspects.

The *Gateway Drone* is critical drone in the regional/city security context as it will provide all sensitive information timely to alert the agencies with potential threat.

The *Gateway Drone* will discharge or transfer its role when it is no longer capable of doing so due to any technical and/or any other issues. When existing *Gateway Drone* is dropped off from its role then all the drones within the network will be alerted and one of the drones that is closer to the *Police Drone* or *City Drone* will become the *Gateway Drone*.

4 CITY/EXTENDED REGIONAL DRONE NETWORK

The proposed conceptual model defines city level security network as a combination of multiple *Community Drone Networks* together. In a given city there can be 'n' number of *Community Drone Networks* based on the households, public places, and commercial entities. A network of *Gateway Drones* forms as a *City Drone Network* with one of the drones nominated as *City Gateway Drone*.

Developing a fully autonomous and cooperative multi-drone system requires robust inter-drone communication. There has not been enough research to say with conviction what design would work best. The reliability and bandwidth requirements from the drone networks are diverse. The drone networks, therefore, have all the requirements of mobile wireless networks and more. Node mobility, network partitioning, intermittent links, limited resources and varying QoS requirements make routing in drone a challenging research task[**?**].

In the proposed conceptual model, since each drone will use WLAN infrastructure mode in addition to Adhoc mode, there will always be a reliable network available to exchange the information. The security drones will switch between Adhoc and infrastructure modes based on the network availability to pass on the information to *Gateway Drones*.

4.1 Drone Networking Challenges

The main challenges that drone networks facing are routing, seamless handover and energy efficiency. Routing has unique requirements - finding the most efficient route, allowing the network to scale, controlling latency, ensuring reliability, taking care of mobility and ensuring the required quality of service. In drone networks, additional requirements of dynamic topology (with node mobility in 2-D and 3-D), frequent node addition and removal, robustness to intermittent links, bandwidth and energy constraints make the design of a suitable protocol one of the most challenging tasks[**?**].

The handover latency and the packet loss during handover process may cause serious degradation of system performance and QoS perceived by the users. IEEE has standardized Media Independent Handover (MIH) services through their standard IEEE 802.21. These services can be used for handovers and interoperability between IEEE-802 and non-IEEE-802 networks, e.g., cellular, 3GPP, 4G. MIH, however, does not provide intra-technology handover, handover policies, security and enhancements to link layer technologies. However, MIH is a nascent technology that has not been widely deployed and evaluated[**?**].

Energy efficiency is a very important requirement in drone networks. Reducing the energy consumption helps in increase in network lifetime and useful payload that can be carried. Energy consumption can be reduced through transmission power control; load distribution or making nodes sleep[**?**].

5 CONCLUSION

In this discussion it has been perceived that existing security informatics systems are disparately implemented and consolidation of data and analysis at various layers hasn't been done efficiently. Considering that big data technologies are robust enough to collect the large volumes of data from variety of sources, a conceptual model is proposed to discuss the feasibility of integrated video, voice, and social media data of individuals to be collected and analyzed for applying the machine learning algorithms. With the technologies such as high speed computing and big data infrastructure, learning algorithms can be applied to solve face and voice recognition. The combination of video, voice, and social network data the proposed conceptual system can address some of the prevailing home, community and territory security challenges and issues.

ACKNOWLEDGMENTS

The authors would like to thank professor Gregor von Laszewski and his team for providing *LaTex* templates and assistance with *JabRef* tool to organize references.

A WORK BREAKDOWN

A.1 HID 333:Anil Ravi

- Identified Paper1 topic
- New Security System conceptual model
- Literature study

- Created Abstract and Introduction Sections
- Created Home Security Concept section
- Created Community Drone Network section
- Reviewed the draft paper

A.2 HID 337:Ashok Reddy Singam

- Editing Latex template using ShareLatex online tool
- Managed JabRef entries
- Created Video Data Integration and Analysis Section
- Created Voice Data Integration and Analysis Section
- Reviewed articles on Machine learning
- Created Learning Algorithms Section
- Reviewed the draft paper

B BIBTEX ISSUES

Warning–I didn't find a database entry for "NIPS2012-4824"

Warning–can't use both author and editor fields in Kantor2005

Warning–empty address in Kantor2005

Warning–numpages field, but no articleno or eid field, in Vincent2010

Warning–page numbers missing in both pages and numpages fields in Wang2015

(There were 5 warnings)

C ISSUES

DONE:

Example of done item: Once you fix an item, change TODO to DONE

C.1 Uncaught Bibliography Errors

Citations in text showing as [?]: this means either your report.bib is not up-to-date or there is a spelling error in the label of the item you want to cite, either in report.bib or in report.tex