WCPS-OSL: A Wireless Cyber-Physical System for Object Sensing and Localization

Amal Lotfy AlHusseiny
Egypt-Japan Univ.
of Sc. and Tech. (E-JUST),
Dept. of Comp. Sc. and Eng.
Email: amal.youssef@ejust.edu.eg

Moustafa Youssef
Egypt-Japan Univ.
of Sc. and Tech. (E-JUST),
Dept. of Comp. Sc. and Eng.
Email: moustafa.youssef@ejust.edu.eg

Mohamed ELTowiessy
Pacific Northwest National Laboratory
The Bradley Dept. of Elec. & Comp. Eng.,
Virginia Tech
Email: toweissy@vt.edu

***Abstract*—We propose a novel Cyber-Physical System for object sensing and localization based on changes in the wireless signal strength with the focus on border protection as an application scenario. Our work is based on the principle that RF signals undergo reflection or refraction when encountering physical objects leading to variations in the received signal. Our system uses access points (APs) and monitoring points (MPs) as sensing and computational nodes. The existence of an object, for example a human or a vehicle, in the area of interest affects the signal strength transmitted by the APs and received by the MPs. The system has training and operation modes. Training occurs by injecting various objects into the field of operation with varying mobility patterns and recording the respective changes in the received signal strength. This produces signal maps that are stored for future matching during the operation mode. According to the type, size, location and number of objects (or intruders) in the operation mode, the system assigns a priority to the intrusion event, so as to deal with it properly. We therefore transform the problem of intrusion detection to a signal pattern matching one. Our proposed system shows a good probability of detection of objects such as standing humans and stationary cars. In addition, the system has a good ability to differentiate between humans, cars and other objects. We also investigate the challenges and open issues related to the system.**

***Index Terms*—Device-free identification, traffic estimation, object identification.**

I. Introduction

Cyber Physical Systems (CPSs) that combine both computing and physical elements are gaining momentum nowadays. CPSs are getting more and more complex as they need to fulfil a number of requirements including being able to get input and feedback from the surrounding physical environment, being distributedly managed and controlled, providing accurate real time performance, expanding over wide geographical areas, and being able to scale up and down easily [1], [2]. CPSs have a wide variety of applications including robotics, control systems, industrial implants, healthcare applications, and smart cities. One of the main applications of CPSs is security applications such as intrusion detection and tracking.

In this paper, we address the problem of designing a ubiquitous cyber physical object detection and localization system with a focus on border protection as an application scenario. Our approach is based on using standard wireless transmitters and receivers that cover large areas. The main idea is that the existence of humans and objects in a wireless environment affects the signal strength [3], [4], [5]. By monitoring and analyzing changes in the wireless signal strength we leverage this fact to perform object detection and identification. In this paper, we investigate the feasibility of the DfP detection and localization system and its ability to differentiate between different classes of object, mainly humans and cars. Such differentiation is crucial to prioritize different detection events.

Such CPS has a large set of applications including border protection, intrusion detection, and traffic estimation. For example, our envisioned system can be used on the borders to detect intruders and distinguish between hostile intruders and migrants in order to prioritize dealing with such events [6]. Such a system will require a minimal hardware to cover a large border area, thus achieving ubiquitous protection.

Our initial experiments shows that the signal strength can be used to detect activity periods. In addition, different features obtained from the received signal strength differentiate a standing human from a stationary car.

The remaining of this paper is organized as follows. Section II presents the proposed system architecture. Section III describes a typical scenario for the application of our system. Section IV shows the testbed and evaluation results. Section V discusses open issues and future work. Section VI discusses the related work. Finally the paper concludes in Section VII.

II. System Architecture

Our system is based on the concept of device free Passive (DfP) localization [3]. In DfP localization, the tracked entity needs neither to carry devices nor to participate actively in the localization algorithm. The main idea is to use installed wireless devices to detect and track the location of entities passively based on the fact that RF signals are affected by changes in the environment.

Referring to Figure 3b, our proposed system consists of signal transmitters, such as standard access points, and monitoring points, such as standard wireless enabled devices. The access points emit wireless signals whose signal strength is affected by the surrounding environment while wireless monitoring points monitor and analyze the changes in RSSI to detect and identify changes in the surrounding environment. An object, e.g. a human or a vehicle, existing in the wireless access point range affects the signal strength received by the

COLLABORATECOM 2011, October 15-18, Orlando, United States

DOI 10.4108/collaboratecom.2011.17

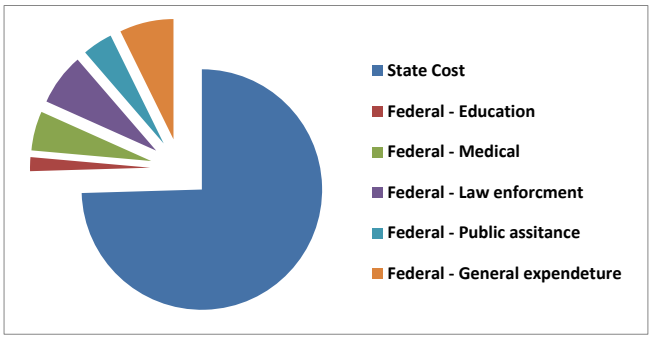


Fig. 2: Percentage of cost of illegal immigration per year in the US over the different sectors [9].

wireless monitoring point. Wireless signal propagating through any object will experience different interference in the form of attenuation, reflection, refraction, and/or diffraction [7]. The size, geometry and material of the object determine the kind of interference and its amount. usually, metallic objects tend to reflect the signal, while wood, concrete or water tend to absorb and refract the signal [8].

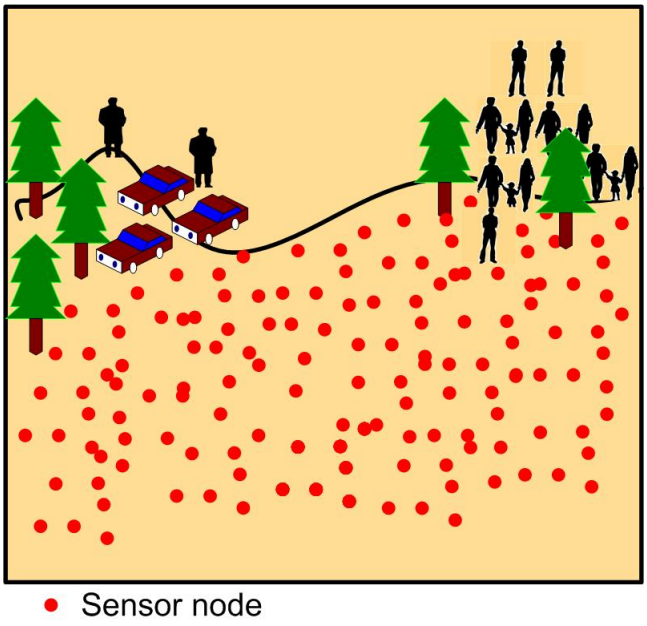
We distinguish between three functionalities: detection, identification, and tracking. Detection refers to determining that there is an activity in the area of interest as compared to silence. Identification refers to identifying the characteristics of the object that caused the activity, e.g. differentiating between a human and car. This also includes identifying the object size, number of objects, among others.

The system can also be used to identify the location of the intrusion and track the intruder in the area of interest. The localization technique we propose is based on building an offline fingerprint of the RSS of the object at different positions in the area of interest. A fingerprint captures the relation between signal strength and distance in the area of interest. Whenever an intrusion is detected, our system matches the the received signal strength pattern to those saved in the fingerprint map to find the location of the intrusion.

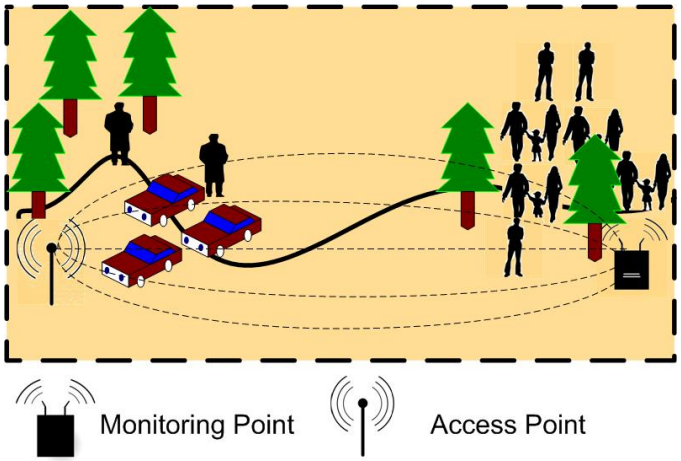
III. A Case Study: A Border Protection Scenario

Illegal immigration is a major problem worldwide that causes a lot of social, economical and legal implications for both developing and developed countries (Figure 2). A study released by the Federation for American Immigration Reform (FAIR) [9] estimates that the 13 million illegal immigrants and their U.S.-born children now costs federal and local taxpayers $113 billion a year. This is about $1,117 per household yearly.

On another hand, illegal drug trade is another example of across border illegal activities that is increasing over time. According to a UN report [10], global drug trade generated an estimated $321.6 billions in 2003. This sum is equivalent to 0.9% of the world's GDP or higher than the GDP of 88% of the countries in the world. These illegal activities and others require a novel protection technique that is characterized by ubiquity, scalability, high real time performance, and being able to handle geographical and management distribution. A



(a) Border protection scenario using sensors for intrusion detection.



(b) Border protection scenario using access points and monitoring points for intrusion detection.

Fig. 3: Border protection scenario

border protection scenario is considered a good fit for the proposed CPS.

As a specific example, consider a border patrol on a border area responsible of preventing illegal border crossings, trafficking, smuggling or other similar criminal activities. The patrol uses High Mobility Multi-purpose Vehicles (HMMWVs) to respond to the detected illegal activities. Each HMMWV is equipped with high computing and communication capabilities. The patrol also equipped with Unmanned Ground Vehicles (UGVs) to interfere in high danger situations.

A lot of criminal activities can happen at border including illegal immigrants trying to cross the border or a smaller group of drug and weapon smugglers also trying to cross the borders. Different events need different level of response depending on their priority. For example, if these two events happen

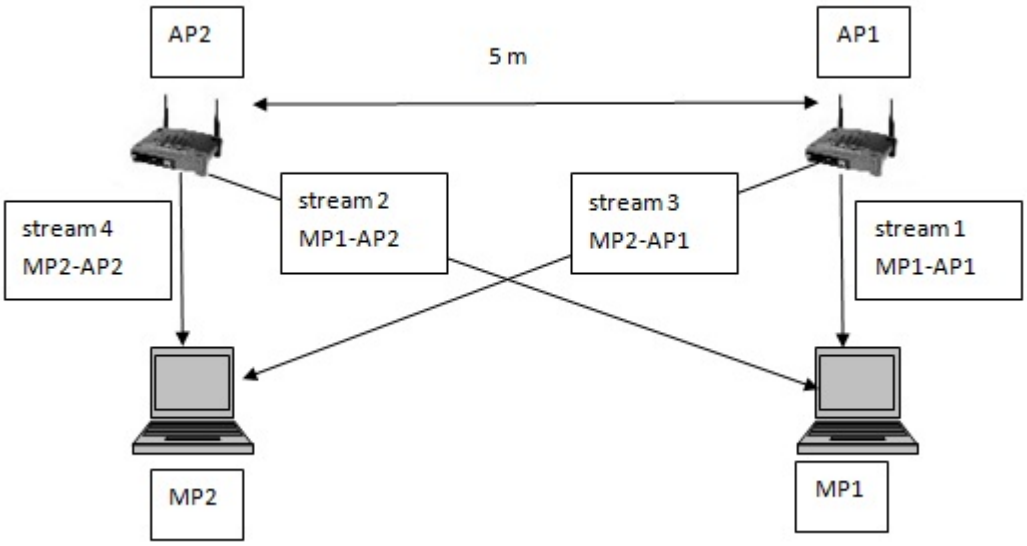


Fig. 1: Experiment layout.

concurrently, the patrol may choose to send a small force to the drug and weapon dealers and a lager force equipped with HMMWVs and UGVs to the large group of immigrants. If the smaller group of drug and weapon dealers also has vehicles and weapons, then the system can give higher priority to that intrusion event and act accordingly.

Prioritizing different events based on the expected level of danger and severity allows the border patrol to interact properly and to distribute available forces accordingly specially in case of having multiple simultaneous breaches. To detect such events and identify their components, traditional sensor networks can be deployed (Figure 3a). However, such systems suffer from the huge cost needed for installation and maintenance of the used sensors and energy limitations.

The proposed system (Figure 3b) depends on installing a small number of wireless transmitters and receivers to cover the border, achieving ubiquitous intrusion detection. Also, such system is envisioned to be able to determine the number, size and material of the entities existing in the area of interest.

IV. Evaluation

A. Testbed

To evaluate our system, we used two Cisco Aironet 1131AG series APs and two Dell Latitude E6510 with Intel Centrino N 6200 AGN wireless NIC acting as MPs. The access points (APs) represent the transmitting units while the wireless receivers represent the Monitoring Points (MPs). One or more of the MPs acts as our system server responsible for aggregating received data and processing them. The server knows the locations of other MPs and of APs. Each of the MPs records the RSSI from each access point transmitted signal. This configuration gives us four streams of raw data for processing. Figure 1 shows the layout of the hardware used.

We experimented with different configuration: (1) a silence period, (2) a stationary human, (3) a stationary car. Our goal is to investigate the feasibility of differentiating between these three cases.

B. Data Collection

We use the Received Signal Strength Indicator (RSSI) values reported by the wireless cards as indicator for the existence of the tracked object through out our experiments. In the infrastructure mode of the 802.11 protocol, APs broadcast beacons, usually every 100 ms. When a frame is received by a card, it not only extracts and supplies data to the higher layers, but also notes the RSSI values which are reported in the header of the link layer frame.

C. Object Effect

Figure 4 shows the raw and smoothed signal strength values for the four streams under different configurations. The mean and variance of the signal strength are summarized in Table I.

The figure shows the following observations:

- The mean and variance of the signal strength can be generally used to differentiate between the silence and activity periods.
- Using a single stream is unreliable by itself. For example, the average signal strength of the first stream cannot be used by itself to differentiate between the silence period and a standing human. Therefore, fusion between the different streams is needed to enhance the overall system accuracy.
- The car presence affects the mean of the signal strength significantly. This is due to its metallic material that significantly affects the signal strength.
- The human effect on the mean signal strength is less significant, as compared to the car effect. Therefore, other

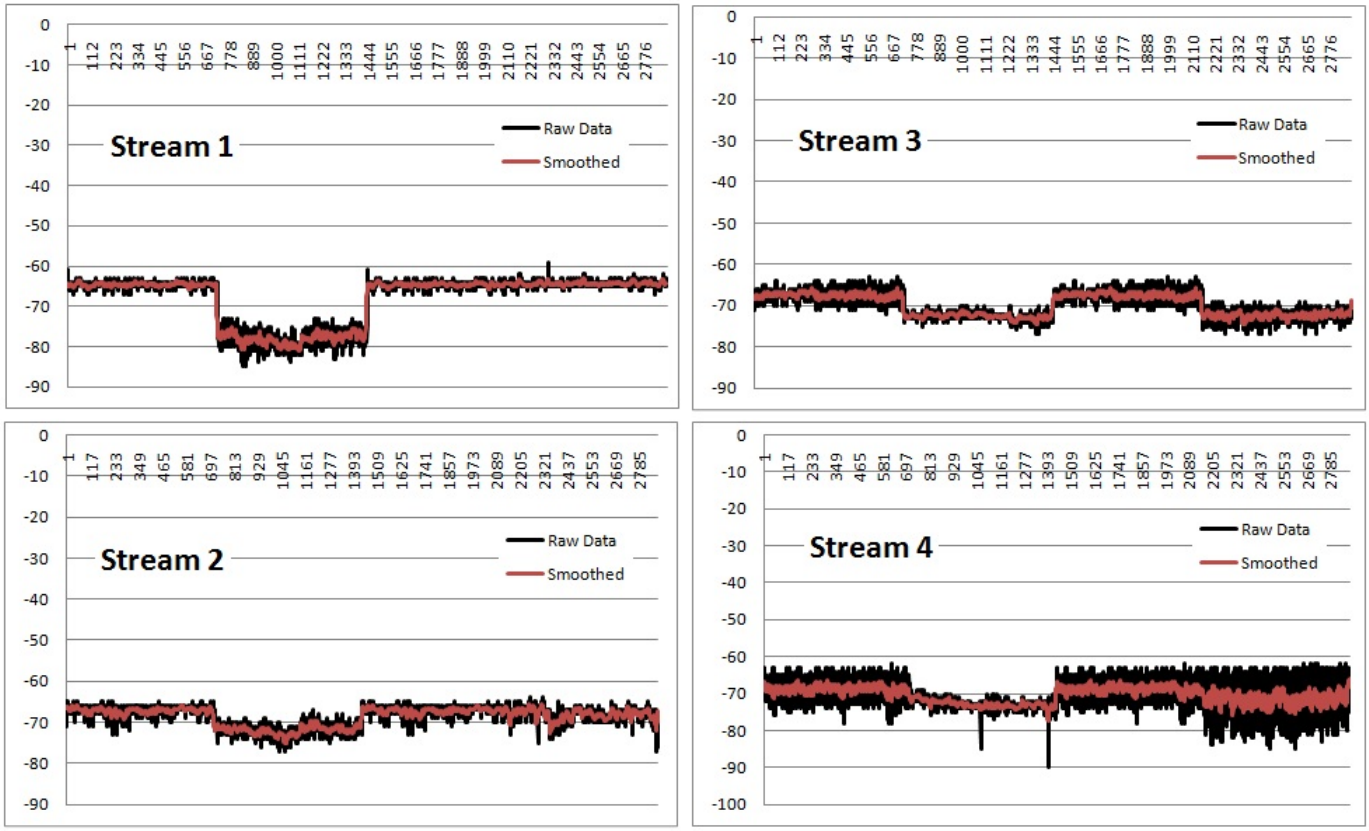


Fig. 4: A silence period for the first 4 minutes (720 sample) followed by 4 minutes with a stationary car in the middle of the area of interest followed by a silence period for 4 minutes and finally a stationary human for 4 minutes. Sampling rate: 3 samples/sec.

	Mean				Variance			
	Silence 1	**Stationary Car**	**Silence 2**	**Stationary Human**	**Silence 1**	**Stationary Car**	**Silence 2**	**Stationary Human**
Stream 1	-64.61	-77.98	-64.61	-64.34	0.81	6.70	0.82	0.77
Stream 2	-67.14	-71.91	-67.14	-68.12	1.84	3.17	1.84	3.73
Stream 3	-67.41	-72.57	-67.41	-72.37	4.42	1.40	4.42	3.72
Stream 4	-68.73	-72.89	-68.75	-71.56	17.76	3.39	17.74	57.61

TABLE I: Summary of the mean and standard deviation of the four streams for the raw data in Figure 4.

features need to be combined with the signal mean for detecting the human presence.

- The existence of an object in the area of interest leads to a change of the variance of the received signal strength.
- The change in the mean and variance can be positive or negative. This depends on the interference pattern caused by the existence of the object in the area of interest which can be constructive or destructive.
- The effect of the object is more clear at the transition instance, i.e. the point in time when a change occurs from silence to activity or vice versa. This suggests that developing methods that depend on detecting transitions should lead to better accuracy.

V. Open Issues and Future Work

This paper acts as a proof of concept that the DfP localization concept can be used for a number of CPS applications, with an emphasis on the order protection scenario. An extensive study and more experiments are needed to characterize the proposed system constraints and parameters. In addition, other types of identification, such as number of objects, and object tracking still need to be studied.

Our study focuses on detecting the existence of an object and whether it is possible to differentiate between the effect of a human and car on the received signal strength. We leave for future work the determination of the number of existing objects within the area of interest and the differentiation between wider range of objects and materials.

Another important aspect of our study is detecting the speed

of the object. This has to be related to the RSSI sampling rate according to the Nyquist theorem. Detecting the speed of the objects have a wide range of application, including traffic estimation and object identification.

Another direction for our work is to experiment with different NICs and access points and the effect of using heterogeneous hardware.

VI. Related Work

Cyber Physical systems are systems that combine computational equipment and physical equipment. Their applications range from distributed control systems to security applications. The main characteristics of CPS, summarized in [1], are the availability of input and feedback from the physical environment, distribution of management and control, uncertainly regarding readings, status, and trust ,real-time performance requirements, distribution geographically with components in locations that lack physical security and scalability requirements.

Security challenges of CPS are presented in [1], [2]. Some of these challenges are interpreting the huge amount of raw data available, sharing information and control in such distributed system, vulnerability to malicious abuse of individual subsystems, maintaining timelines and synchronization in such distributed system and validation of the system collected data and behavior. These challenges have been the focus of prior research, e.g. [11], [12].

Our previous work in [3] proposes a location determination system that does not require the presence of a physical device attached to the person being tracked or the tracked device to participate actively in the localization process. The device free positioning system (DfP) works by monitoring and processing changes in the received signals strength at a number of monitoring points to detect changes in the environment corresponding to the existence of the person being tracked. Our proposed system leverages the DfP concept to provide a ubiquitous object detection and tracking system that can be used in many applications, including border protection.

VII. Conclusion

In this paper, we introduced a ubiquitous object detection and identification system that is based on the DfP localization concept. Up to our knowledge, this is the first intruder detection system that utilizes and coordinates both cyber and physical resources to perform its function. The system learns signal change patterns during training, which are then matched with detected patterns during operation. Our system is able to detect, localize and prioritize intrusions. The detection and localization are based on the change of the RSSI pattern due to the existence of a physical object within the area of interest. Our results provide a proof of concept and feasibility for the proposed system. The performed experiments focus on detecting the existence of an object and whether it is possible to differentiate between the effect of a human and that of a car on the received signal strength. The results showed good probability of detection for standstill objects. We leave for future work the determination of the number of existing objects within the area of interest, the differentiation between a wider range of objects and materials, and the detection of the speed for moving objects. So far, we experimented with one brand of NICs and one brand of access points. We still need to experiment with different NICs and access points. We also need to study the effect of using heterogeneous hardware.

Acknowledgment

This work is supported in part by a grant from the Egyptian Science and Technology Development Fund (STDF) and in part by a TWAS-AAS-Microsoft Award.

References

[1] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS: S&T Workshop on Future Directions in Cyber-physical Systems Security*. Citeseer, 2009.

[2] P. Pal, R. Schantz, K. Rohloff, and J. Loyall, "Cyber-physical systems security-challenges and research ideas."

[3] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 222–229.

[4] A. E. Kosba, A. Abdelkader, and M. Youssef, "Analysis of a device-free passive tracking system in typical wireless environments," in *NTMS*, 2009, pp. 1–5.

[5] M. Seifeldin and M. Youssef, "A deterministic large-scale device-free passive localization system for wireless environments," in *PETRA*, 2010.

[6] R. M. Eltarras, "Biosense: Biologically-inspired secure elastic networked sensor environment," Ph.D. dissertation, The Faculty of the Virginia Polytechnic Institute and State University, 2011.

[7] M. Youssef and A. Agrawala, "Small-scale compensation for wlan location determination systems," in *IEEE Wireless Communications and Networking Confernece (WCNC 2003)*, vol. 3. IEEE, 2003, pp. 1974–1978.

[8] "Dynamic radio management," Extreme Networks Technical Brief, Tech. Rep., 2007.

[9] http://www.fairus.org/, 2011.

[10] http://www.boston.com/news/world/europe/articles/2005/06/30/un_report_puts_worlds_illicit_drug_trade_at_estimated_321b/S, 2005.

[11] J. Haack, G. Fink, W. Maiden, D. McKinnon, and E. Fulp, "Mixed-initiative cyber security: Putting humans in the right loop," in *The First International Workshop on Mixed-Initiative Multiagent Systems (MIMS)*, 2009.

[12] W. Maiden, I. Dionysiou, D. Frincke, G. Fink, and D. Bakken, "Dual-trust: a distributed trust model for swarm-based autonomic computing systems," *Data Privacy Management and Autonomous Spontaneous Security*, pp. 188–202, 2011.