On the Impact of Physical-Cyber world Interactions during Unexpected Events

B. S. Manoj
Indian Institute of Space science and Technology (IIST)
Trivandrum, India
Email: bsmanoj@iist.ac.in

Bheemarjuna Reddy Tamma
Indian Institute of Technology
Hyderabad, India
Email: tbr@iith.ac.in

Ramesh R. Rao
University of California San Diego
San Diego, CA 92093
Email: rrao@ucsd.edu

ABSTRACT
Physical world events have a strong and direct impact on the communication activity seen in the cyber world. In this paper, we present three physical world events where we conducted passive network traffic measurements to study the interaction between physical and cyber worlds. We consider the following types of events: an active shooter drill, a science festival scenario, and an emergency response drill involving a simulated dirty bomb attack. The network behavior during these events is contrasted with the regular network behavior. In some events, we observed substantial drop in network traffic whereas in some others, we noticed high traffic surge. Therefore, the deviation observed in the cyber world activity may be exploited to automate the detection of physical world events. The drills also involved setting up of wireless mesh network infrastructure to assist first responders in their rescue operations and provide Internet connectivity to attendees of science festival. Our passive network measurements provided valuable insights which would help us in configuring wireless mesh network testbeds more efficiently and thereby providing efficient coordination of the response activity and saving human lives and properties.

Categories and Subject Descriptors
C. 2. 0 [**Computer Communication Networks**]: C.2.3 Network Monitoring

General Terms
Measurement, Documentation, Performance, Human Factors.

Keywords
Unexpected events, cyber world behavior, emergency response, cyber-physical world interactions, wireless mesh networks, non-invasive network measurement, high network traffic deviation.

1. INTRODUCTION
The growth of modern computer communications systems has resulted in near ubiquitous cyber systems. However, as in most physical infrastructure such as roads, highways, and railways, the computer networks are also designed in an under-provisioned manner where the peak usage typically results in a state where the demand goes beyond the designed capacity. Most cyber systems are underutilized during regular usage cycles except some busy hour periods. The pattern of the usage of a computer network often helps in optimizing resource allocation in bandwidth constrained networks such as cellular wireless networks. Only very limited, mostly non-civilian, systems such as military cyber systems contain over-provisioned communication resources. As a result, during some unexpected physical world events, most cyber communication systems see load surges to the extent of even incapacitating the network.

Unlike in the past, the near ubiquitous cyber systems can capture important characteristics of the society. That is, the typical behavior of a network or the usage pattern of a cyber system can reveal the collective social characteristics of the user population. Therefore, through the observation of multiple facets of cyber systems, interesting social characteristics may be revealed.

We conducted multiple network data collection exercises during real or simulated physical world events and observed the behavior of network traffic. Our observations reveal that the physical world events cause substantial impact on the behavior of cyber systems. However, most importantly, the behavior of the cyber systems differs for different physical world events. There exists very limited literature that reports network traffic measurements or network behavior observations carried out during simulated or real world unexpected events. We report our observations because it provides interesting inputs for a variety of future works.

We present observations from three scenarios. First is an emergency response scenario where a simulated emergency response drill is conducted in a university campus building. The drill scenario was conducted to train the university police, the city police, and the city fire department to improve their preparedness to handle humanitarian crises such as the situation where an active shooter barges into a university research building and mindlessly killing the occupants. Such drill events are very useful in identifying (i) the possible delays encountered by the response agencies, (ii) bottlenecks during the evacuation process, and (iii) pitfalls associated with quick and collective decision making, and, thereby, improve the entire process of emergency response.

The second scenario we considered is an entirely different physical world event, a science festival, where large number of high school students, their parents, and scientists assemble in a large city park where moderate number of citizens usually visits. The science festival, attended by more than 50,000 people, resulted in unexpectedly high network traffic. The observations, such as this from the science festival, can help the civil

ACWR'11, December 18-21, 2011, Amritapuri, Kerala, India.

administration to redesign the network, provision additional resources, and change the architectures for communication in order to handle such large demands in certain areas of the city where the demand for cyber communication resources can fluctuate widely.

Finally, we present the network environmental changes resulting from another emergency response drill where simulated dirty bomb attack was enacted to the study the full scale emergency response plan prepared of the San Diego County.

The rest of this paper is organized as follows: Section 2 presents our work. In Section 2.1, we present the active shooter drill scenario and the network observations during the drill. Section 2.2 discusses the San Diego Science Festival and the network traffic behavior observed during the event. The detailed description of the third scenario of a full scale emergency response drill and associated network observations is described in Section 2.3. Finally, Section 3 concludes the paper.

2. IMPACT OF PHYSICAL WORLD EVENTS ON CYBER WORLD SYSTEMS

We studied three distinct scenarios where certain non-routine events took place. First is an emergency response drill conducted at University of California San Diego (UCSD) for studying the humanitarian response-related issues in the event of an Active shooter attack on a university research facility. Second, we present our observation from a large scale science festival, conducted at the San Diego Balboa Park, where more than 50,000 people assembled during a daylong event. Finally, we present our observations from the environment of an emergency response drill associated with a dirty bomb attack on a soccer field gallery.

2.1 Scenario I: UCSD Active Shooter Drill

An active shooter is defined as either a single individual or a small group of disgruntled men or women who collude to destroy human life in a single or sequence of gun abuses spanning short or medium time duration. There exist many recent disasters in the US and elsewhere of such active shooter incidents. The most recent incident in GeorgiaTech, GA, USA, a psychologically disturbed student took lives of dozens of students and several faculty before taking his own. In another incident, a tenure-denied faculty at University of Alabama, Huntsville, USA, took out a gun and shot multiple people attending a faculty meeting. Such incidents may result in a chaotic situation in universities where the response is typically difficult unless the response agencies coordinate very well. Even evacuation of certain academic laboratories requires complex procedures to be followed thus making response in sophisticated research facilities a complex activity. At other times, the active shooter may cover multiple buildings giving rise to confusion and chaos to responders even in locating the attacker or the possible trajectory of the attacker. Even in developing countries such as India school or university shooting incidents are reported occasionally. Our work reveals that monitoring cyber infrastructure may help authorities to get another dimension for detecting the occurrence of a physical world disaster or its spatio-temporal progression.

In this drill, referred to as University of California San Diego (UCSD) Active shooter drill, we study the impact of a simulated active shooting incident on the wired and wireless network serving the UCSD Leichtag building that occupied the research facilities in the Bio-medical research area. This drill was conducted jointly by UCSD police, San Diego City Police, and San Diego Fire Department, on October 16, 2007 in UCSD campus. The main part of the drill took place at the Leichtag building, located on south campus (School of Medicine) of UCSD. Figure 1 shows the map of the area where the drill was conducted.

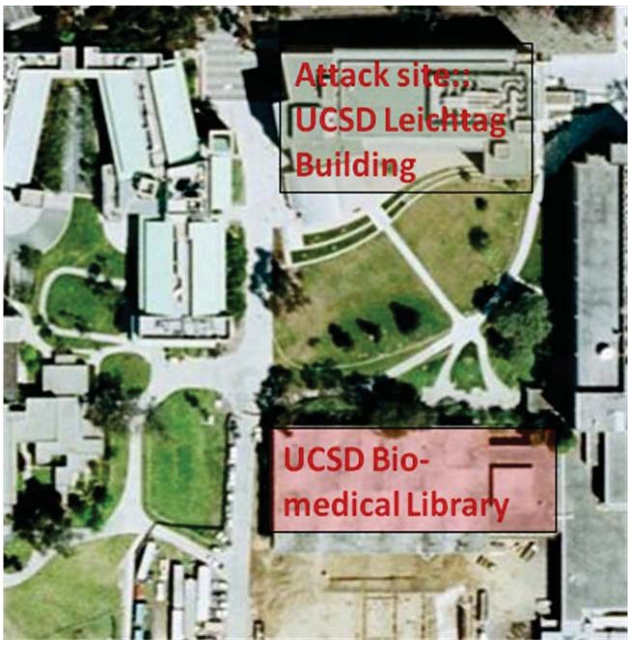

Figure 1. A map of the UCSD site where the Active Shooter Drill was conducted on 16th October, 2007.

We conducted four passive network traffic measurement campaigns during this drill. These are (i) wired network measurement on the traffic to-and-from the Leichtag building, (ii) Wireless LAN traffic measurement for inside and outside of the Leichtag building, (iii) wireless mesh network traffic monitoring for the CalMesh network deployed for supporting the simulated response activity, and (iv) CDMA cellular network measurement. This paper mainly presents the results from the first three measurement campaigns. In addition, our team deployed a Wireless Mesh Network (WMN) testbed based on the CalMesh platform [1]. The CalMesh network was deployed in the courtyard outside the building and surrounding grassy area, covering an approximate 100X200 yard area with the help of four CalMesh boxes. The main purpose of the WMN was to help the first responders to communicate among themselves as well as to provide backbone connectivity for the health sensors the first responders use. However, the presence of the WMN outside the courtyard did not impact our measurements.

2.1.1 Wireless Network Observations from UCSD Active Shooter Drill

The first set of studies that we conducted on the wireless channel is to measure the in-building traffic observed during the drill. We, therefore, measured the traffic on all channels at both the 4th floor

and the 2nd floor of the Leichtag building. To capture the traffic across all channels in an efficient manner, we employed CalNode devices [2] developed at UCSD-CalIT2. CalNode devices are capable of observing traffic on all channels by using an efficient time-based time-driven multi-channel traffic sampling mechanism [3]. Using CalNodes, we sampled all IEEE 802.11 channels in passive manner in both 2.4 GHz (11 channels) and 5.2 GHz (13 channels) ISM bands.

Figure 2 shows the traffic variation on the 4th floor of the building which showed a low traffic on most channels and the 802.11b Channels 1, 6, and 11 showed moderate 600 Kbps traffic during the drill. The 802.11a channels (marked 12-24 in the figure) are found to be completely unused in the building. However, the 2nd floor wireless traffic seemed to be even lower than the 4th floor traffic. As shown in Figure 3, the 2nd floor wireless traffic on Leichtag building is present only on two 802.11b channels, 6 and 11, with an average traffic of 275 kbps and 75 kbps traffic, respectively.

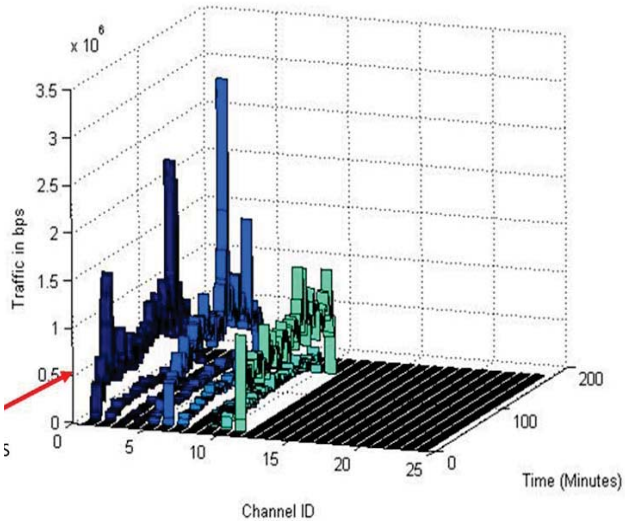

Figure 2. Wireless traffic on the 4th floor of Leichtag building during the UCSD Active shooter drill.

UCSD campus was completely covered by the campus Wi-Fi networks since more than nine years and, therefore, penetration of laptops was high among the students and faculty. Wireless was one of the predominant methods in most parts of the engineering departments. Therefore, we expected the drill to show its signs on the wireless traffic. In order to study the traffic deviation as a result of the drill, we followed our measurements on wireless traffic on the subsequent days of the drill as well as the subsequent Tuesdays (since October 16, 2007 falls on a Tuesday). However, contrary to our expectations, we noticed no significant difference on the wireless traffic in the building. Subsequently our interactions with the researchers in the building proved that the wireless channel usage in that building is minimal and many researchers depended on the wired network for their communications needs. This fact was underscored by our observations on the wired network traffic.

2.1.2 Wired Network Observations from UCSD Active Shooter Drill

To further study the impact of the UCSD Active shooter drill on the communications in the Leichtab building, we obtained the traffic measurement on the wired network. The UCSD edge router and the Leichtag building core IP router were the two measurement points used for wired traffic measurement. We mainly depended on the historical traffic between IP routers in Leichtag Building and any host in that building for the former measurement. Table 1 shows the wired network measurement statistics. To compare the impact, we also collected the measurements for multiple Tuesdays in October 2007.

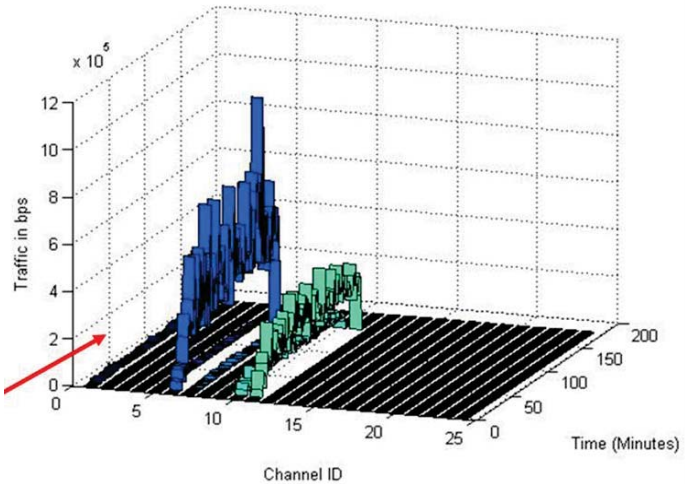

Figure 3. Wireless traffic from Leichtag building 2nd floor during UCSD Active shooter drill.

Table 1. Wired Network Measurement Statistics during (9AM-12PM) the UCSD Active shooter drill.

Day	Total data	Packets/Sec	Total packets
Tuesday, Sep 18, 2007	6.1 GB	848 Pkts/sec	9.15 Mi Pkts
Tuesday, Oct 2, 2007	4.9 GB	618 Pkts/sec	6.3 Mi Pkts
Tuesday, Oct 9, 2007	6.3 GB	769 Pkts/sec	8.3 Mi Pkts
Tuesday, Oct 16, 2007 (Drill day)	**2.3 GB**	**352 Pkts/sec**	**3.7 Mi Pkts**

We conducted two comparison studies with wired network measurements. First is the comparison of Tuesday's traffic. The campus drill was held on October 16th, 2007, a Tuesday, and, therefore, we compared the traffic on that day with the traffic during several Tuesdays prior to the drill. Some of the

observations made from the wired network experiments are briefed here.

Figure 4 shows the average wired network traffic in bytes/seconds observed in Leichtag building. Due to the impact of the simulated active shooter incident on 10/16/2007, the traffic observed a 61% decrease compared to the three prior Tuesdays (see Figure 4). Similar difference is observed for the total traffic in terms of bytes observed on Tuesdays as can be found in Figure 5. Though the number of bytes, in MB, differs on each Tuesday, the average traffic reduction due to the simulated incident on 10/16/2007 remained approximately at 61%.

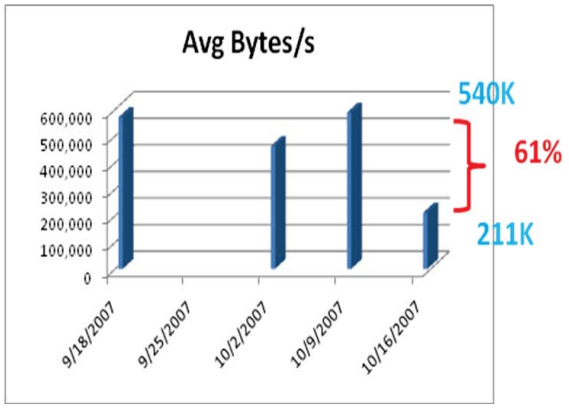

Figure 4. Average Bytes/s traffic observed on Tuesdays.

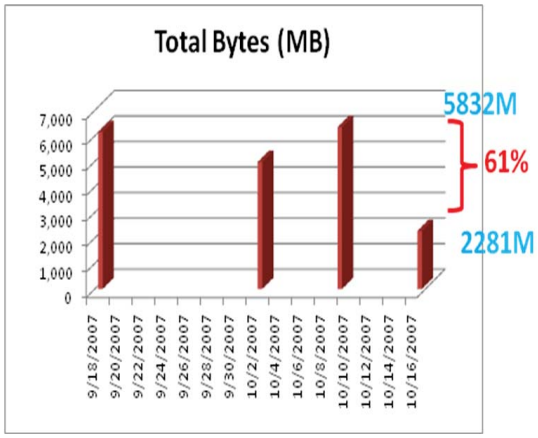

Figure 5. Total Bytes observed on Tuesdays.

Figure 6 shows the average traffic in terms of packets/sec observed. The difference in the average packets/sec that we observed for several Tuesdays prior to 10/16/2007 and during the drill day remained lower than the traffic in terms of bytes/sec. Even then, the decrease in the traffic on 10/16/2007 due to the simulated drill is significant with an average reduction of 53%. Similar difference is noticed for the total packets that we observed during the 9am-12noon time slot on Tuesdays as observed from Figure 7. The traffic reduction on the day of simulated incident remains approximately at 53% compared to the rest of the prior Tuesdays.

In addition to the comparison of traffic on Tuesdays with that of the drill day, we also collected wired network traffic for the rest of the weekdays on the third week of October 2007. The measurements made on the rest of the week days are compared with the measured traffic on 10/16/2007. The observed traffic on 10/16/2007 remained at 211K Bytes/sec whereas the rest of the week averaged traffic of approximately about 413Kbytes/sec as can be found from Figure 8. This amounted to a difference of 48.93% decrease in traffic, which is mainly due to the simulated active shooter drill incident.

Figure 9 shows the total bytes transferred over the wired network during the week of the UCSD Active shooter drill. According to the result in Figure 9, the total traffic showed a decrease of approximately 48% on 10/16/2007 compared to the rest of the days of the week. We also noticed high variation on the total traffic during the rest of the week's measurements. Even with high variance, all subsequent days had higher traffic in comparison to the traffic on 10/16/2007.

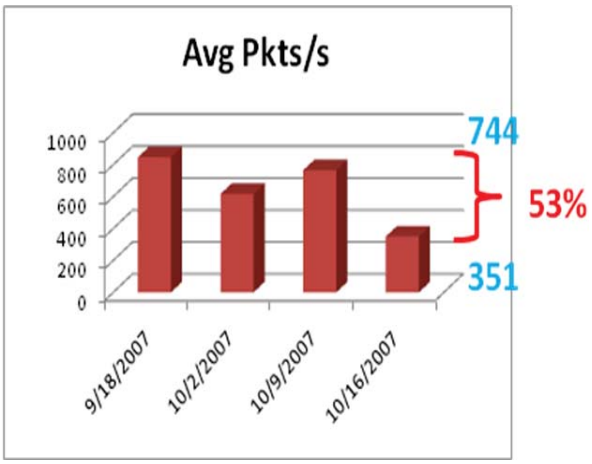

Figure 6. Average Packets/s traffic observed on Tuesdays.

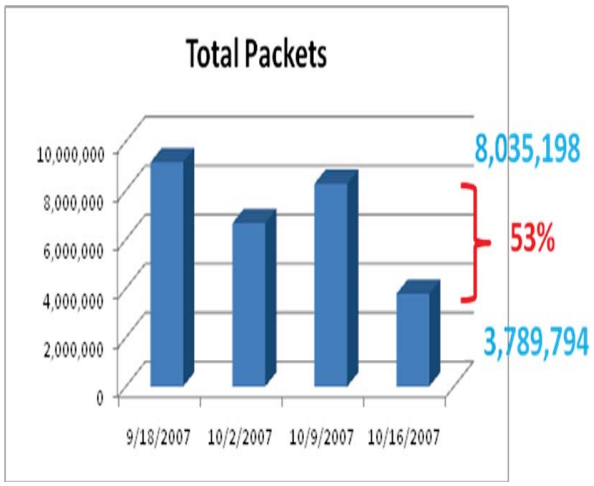

Figure 7. Total Packets observed on Tuesdays.

Similar to the traffic in terms of bytes/sec and total bytes during the week of drill, we also noticed significant decrease in traffic in terms of average packets/sec as well as total packets. The rest of the week averaged a traffic approximately 629 packets/sec in comparison to 351 packets/sec on 10/16/2007, leading to a decrease of 44.16%. This can be observed in Figure 10.

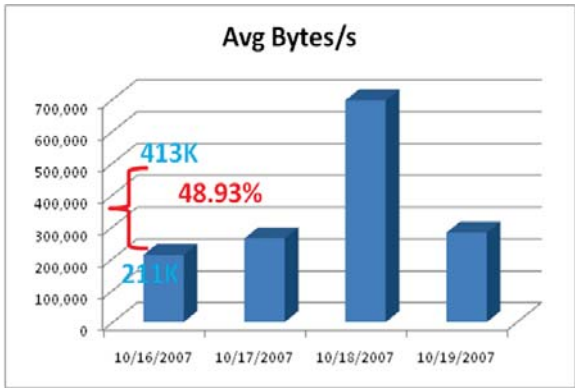

Figure 8. Wired traffic (Bytes/sec) measurements.

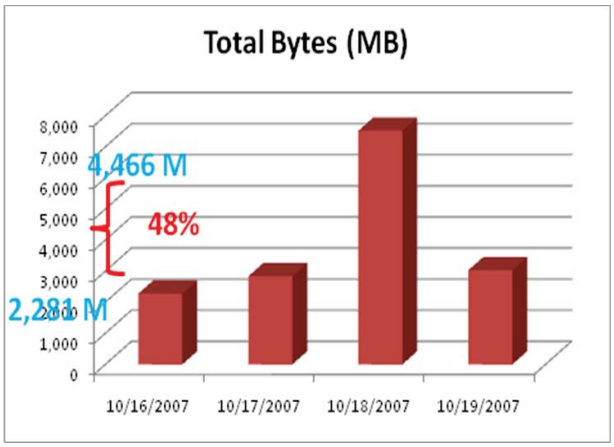

Figure 9. Total bytes transferred in Leichtag building during the week of the drill.

Similarly, Figure 11 shows that the total number of packets transferred in Leichtag building also showed a decrease at 44.1% during the 9AM-12noon time window during which the drill was conducted. The total number of packets that we observed during the above mentioned time window was averaged to 6.78million packets whereas due to the drill, only 3.78 million packets were transferred.

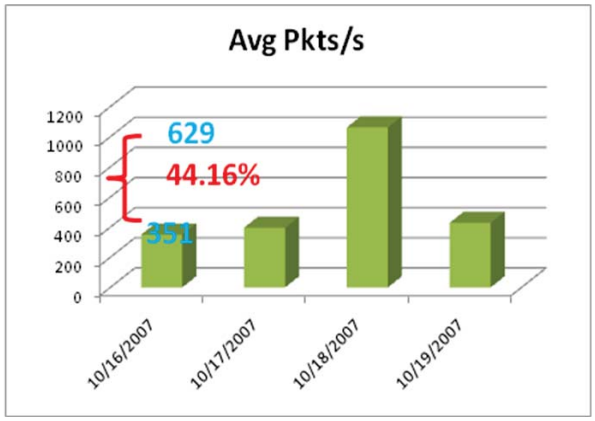

Figure 10. Average packets/s observed on wired network during the week of the drill.

The wired network measurements from Leichtag building, the site of the UCSD active shooter drill, revealed one example of the impact of the physical world events on the cyber-world activity. In this case, even when the event is a simulated incident, the impact on the cyber world was substantial. In conclusion, the impact that we observed on the network traffic can potentially be used for remotely detecting physical world troubles or unexpected events using cyber-world measurements.

2.2 Scenario II: San Diego Science Festival 2009

The second scenario where we conducted data collection experiments is during the Balboa Science Festival 2009 conducted at the San Diego Balboa Park on April 4th, 2009. Balboa park is San Diego city's biggest and most attractive park and it is home to many museums, joy ride parks, art galleries, play houses, zoological park, and the world famous San Diego Zoo. During both working days and holidays, Balboa park attracts a

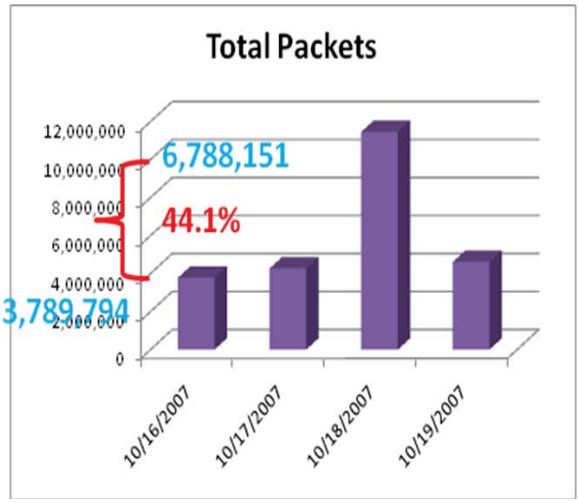

Figure 11. Total packets/s observed on wired network during the week of the drill.

large number of visitors from the city as well as outside. The San Diego Science Festival was conducted during the hours 8:30 AM to 6:00 PM on April 4th, 2009. The festival attracted more than 50,000 additional visitors to the park that includes students from 5th grade through high school and their parents, teachers, scientists, hobbyists, and general public. The purpose of the science festival was to encourage a larger fraction of students from California to take scientific careers. To achieve the aim of the festival, there were several stalls that set up attractive scientific demonstrations and experiments. Balboa park provided Internet connectivity to the visitors using a free public Wi-Fi network. The park's public Wi-Fi network used only channels in the 2.4GHz spectrum. In addition to the public Wi-Fi network, an additional production WMN was deployed to provide higher bandwidth to the stalls. This production network used a fixed channel 10 (in the 2.4GHz Wi-Fi spectrum) for providing the bandwidth services to the stalls. In both the cases, the physical world event seemed to drastically alter the cyber environment. In order to compare the impact of the festival on the cyber environment, we additionally conducted measurements on three subsequent Saturdays including 14th and 21st, March 2009 and 12th April 2009. These dates are chosen to compare the network behavior observed on 4/4/2009, a Saturday.

2.2.1 Observations from San Diego Science Festival 2009

Figure 12 shows the total packets we observed across all channels in the 2.4 GHz spectrum. Compared to the three Saturdays' traffic, on the day of Science Festival the traffic was on average 0.9 million packets over a sample period of 75 minutes spanning 12noon through 1.15pm. This traffic is about 20 times more than the average Saturdays' traffic we observed. Note that our sampling method captures only about 10% of the traffic seen on the 11 channels in the 2.4GHz spectrum. Therefore, in order to obtain the absolute total number of packets, we need to extrapolate the sampled total packets shown in Figure 12. Similarly, in Figure 13, we observed the traffic in bits/sec that showed approximately more than 30 times the average typical Saturdays' traffic on the science festival day.

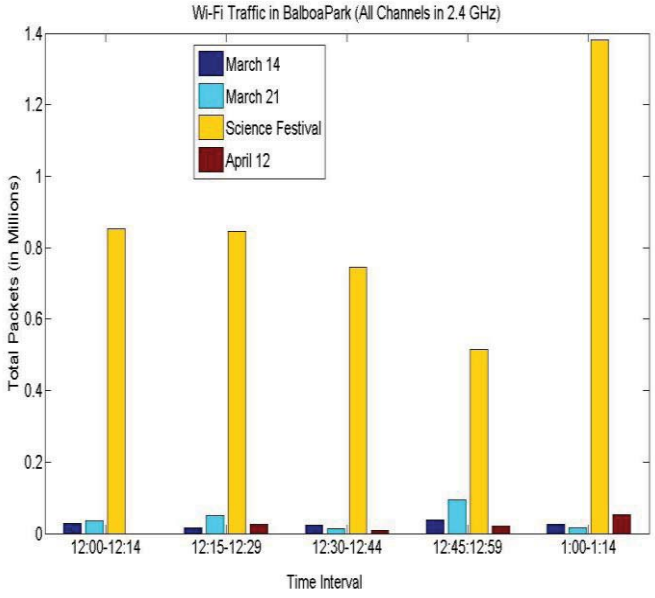

Figure 12. Total packets across all 2.4GHz channels on science festival day and subsequent Saturdays.

Figure 14 shows the number of active clients during the short time intervals that we observed on the day of festival compared to three other Saturdays. It can be noticed that more than five times the usual number of clients were visible during the festival day in our measurements. Note that only a fraction of the science festival participants may have used the network resources. From the above results, it can be noticed that a physical world event such as a large scale festival that causes large gathering of people can create substantially higher network traffic load.

Clearly, the Science Festival created a huge increase in the cyber world activity than the UCSD Active shooter drill which caused substantial decrease in the traffic. That is, the deviation in the cyber network behavior from the typical can be different in different scenarios.

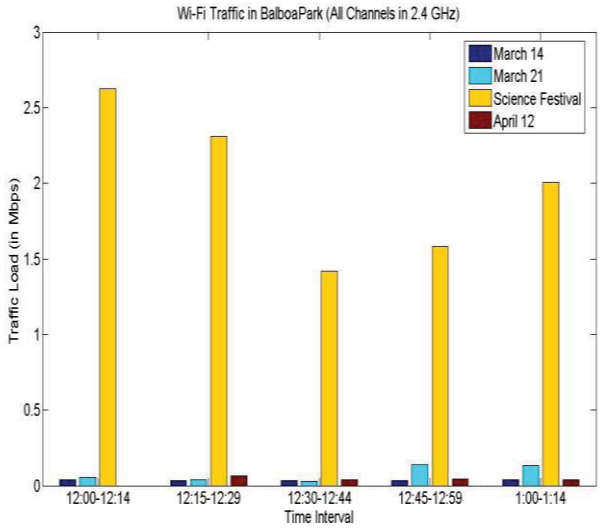

Figure 13. Traffic load (Mbps) during Science Festival.

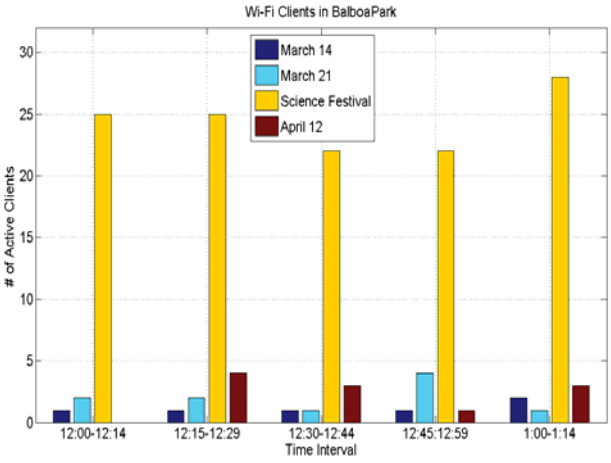

Figure 14. Active clients in the wireless environment.

2.3 Scenario III: Full Scale Emergency Response Drill (Operation Golden Eagle) at San Marcos State University

The third scenario that we studied is a full scale emergency response drill, pseudo-named as Operation Golden Eagle, conducted on May 10, 2010 at San Marcos State University where a simulated dirty bomb blast was conducted at a soccer field. Figure 15 shows a view of the San Marcos state University's soccer field in the immediate aftermath of the emergency response drill when the bomb blast was triggered. From the figure, the smoke from the blast may be observed and the simulated victims, including players and spectators, can be seen. The bomb was assumed to be located on the gallery and was supposed to contain dirty nuclear material.

Figure 15. A view of the ground-zero during San Marcos full scale drill (smoke rising above the ground-zero and victims are seen).

As a response activity, UCSD WIISARD-SAGE project deployed an advanced emergency response platform that included a large collection of medical sensors and a central resource management system. In order to transport the medical sensor data to the resource management center, we deployed a WMN that consists of a dozen CalMesh nodes. Since we do not have the historical traffic in that location, we present the temporal progression of the wireless environmental characteristics here. We present the received signal strength observed in each channel of the spectrum.

In Figure 16, we observed the average and peak channel RSSI amplitude (bottom-most plot), and topographic heat graph (middle graph) and traffic Vs time (top plot) obtained by using the wireless monitoring tool WiSpy [5]. In this figure, it can be noticed that the average of RSSI peaked about -68dBm to -60dBm with peak RSSI spanned in the range -40dBm to -30dBm. However, in comparison to this, Figure 17 shows the corresponding results during 11am-11.30am during the five hour long drill. It can be seen that the environment has changed quite a lot during the half an hour progression of the drill. First, the peak and average RSSI (bottom graph in Figure 17) are closer to -60dBm than -70dBm in the Figure 16. Besides, the channel 10 seems to be clearly facing higher traffic as a result of the response activities used the CalMesh network that operated on channel 10. Similar changes in the cyber environment, as a result of the physical world activities, were noticed during the entire drill.

Another example is the traffic progression of the channels as a function of time that depicts the impact on cyber world due to physical world events. Figure 18 shows the temporal and spectral variation of traffic (in bits per second) during Operation Golden Eagle. Compared to other channels, notice that Channel 10 is the heaviest loaded and the load varies as the drill proceeded to the conclusion. The peak traffic, at the end of the drill, is a result of a throughput capacity test by flooding the network by the researchers who deployed the network testbed.

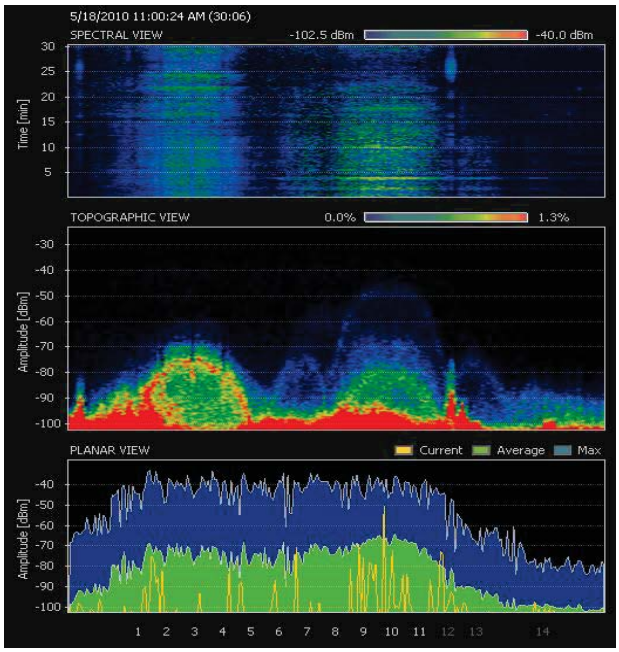

Figure 16. Wireless environmental characteristics at 10.30-11am during Operation Golden Eagle drill at San Marcos, CA on May 10, 2010.

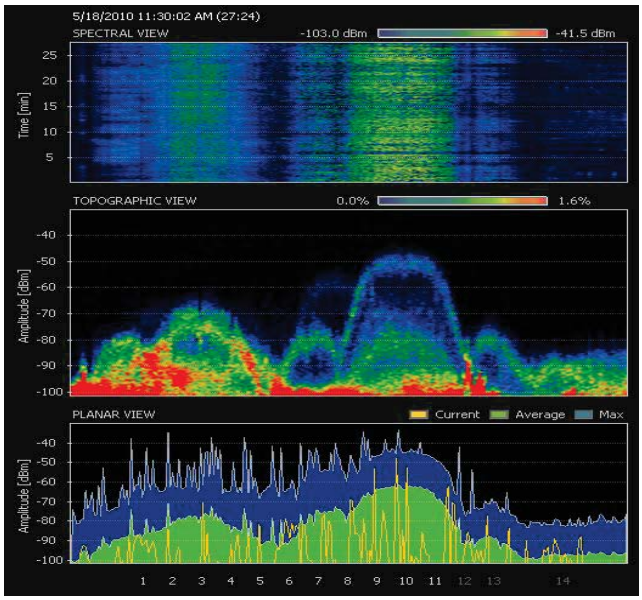

Figure 17. Wireless environment changes during 11am-11.30am during Operation Golden Eagle.

Finally, in Figure 19, we present another dimension of the relationship between the physical world events and the corresponding cyber world impact. In this figure, the number of active clients observed during the Operation Golden Eagle has clearly followed the drill duration as marked in the figure.

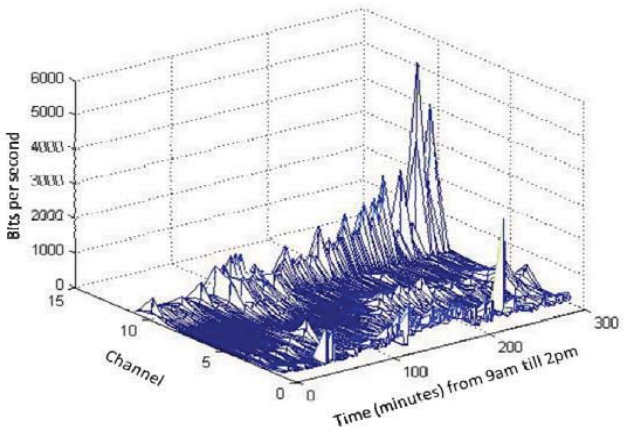

Figure 18. Temporal variation of channel traffic during Operation Golden Eagle.

The active users in the wireless network grew as the drill is in full swing at 10.15am and remained high till near the completion of the drill 12.45pm. After about 12.45pm, there was a drill conclusion exercise during which network performance measurements were conducted. Therefore, the active clients behavior reflected that fact as well. The observation tells us that the physical world events can result in clear and substantial changes in the cyber world events.

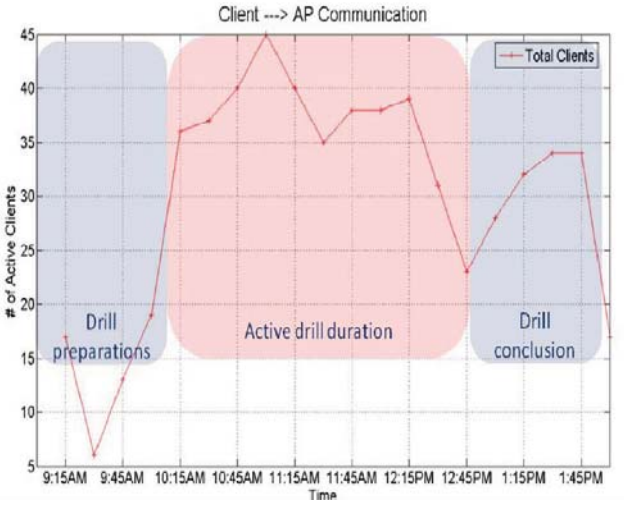

Figure 19. Relationship between the physical world drill and the number of active clients (cyber network users): the active clients clearly followed the event's schedules.

3. CONCLUSIONS

The effect of events in the physical world is increasingly visible in the cyber world. We conducted several medium and large scale real world experiments to quantify the impact of physical world events on the cyber world. We presented our experiments from three scenarios: (i) UCSD Active Shooter drill, (ii) San Diego Science Festival 2009, and (iii) Operation Golden Eagle Drill at San Marcos State University. We noticed substantial impact on cyber world activity due to unexpected events as deviation can range from 40% reduction to about 30 times increase of the average network traffic during regular times.

In UCSD Active shooter drill, we observed wired network traffic drop from 44% to 61% whereas during the San Diego Science Festival 2009, we observed a traffic load increase of 20-30 times the regular traffic.

Since the relationship between physical world events and cyber world behavior is so strong, detecting cyber world changes may help quickly detect many characteristics of the physical world such as the occurrence and progress of the unexpected events in the world. Some early examples for such applications can be found in [7][8].

4. ACKNOWLEDGEMENT

This work was done when the first and second authors were at the California Institute of Telecommunications and Information Technology (CalIT2), University of California San Diego, CA. Parts of this work was supposed by the NSF sponsored projects Responding to Crises and Unexpected Events (RESCUE) and Responsphere and the WIISARD-SAGE project sponsored by the National Library of Medicine.

5. REFERENCES

[1] CalMesh V 1.0: http://calmesh.calit2.net

[2] CalNode : http://calnode.calit2.net

[3] B. R. Tamma, N. Baldo, B. S. Manoj, R. R. Rao "Multi-Channel Wireless Traffic Sensing and Characterization for Cognitive Networking," PROCEEDINGS OF IEEE ICC 2009, JUNE 2009.

[4] WIISARD-SAGE: http://www.wiisard.org

[5] WiSpy wireless monitoring tool: http://*www.metageek.net/products/wi-spy*

[6] Brian Braunstein et. al., "Feasibility of Using Distributed Wireless Mesh Networks for Medical Emergency Response," Proceedings of AMIA Annual Symposium 2006, pp. 86–90, September 2006.

[7] Y.-C. Chiu and P. B. Mirchandani, "Online Behavior-Robust Feedback Information Routing Strategy for Mass Evacuation," *Intelligent Transportation Systems, IEEE Transactions on* , vol.9, no.2, pp.264-274, June 2008.

[8] A. Jrad, H. Uzunalioglu, D. J. Houck, G. O'Reilly, S. Conrad, and W. Beyeler, "Wireless and wireline network interactions in disaster scenarios," *IEEE Military Communications Conference 2005 (IEEE MILCOM 2005),* Vol. 1, pp.357-363, October 2005.