Physical Indicators of Cyber Attacks Against a Rescue Robot

Tuan Vuong, Avgoustinos Filippoupolitis, George Loukas and Diane Gan
Smart Systems Technologies Department
School of Computing & Mathematical Sciences
University of Greenwich
London, UK
Email: {t.p.vuong, fa52, g.loukas, d.gan}@gre.ac.uk

***Abstract*—Responding to an emergency situation is a challenging and time critical procedure. The primary goal is to save lives and this is directly related to the speed and efficiency at which help is provided to the victims. Rescue robots are able to benefit an emergency response procedure by searching for survivors, providing access to inaccessible areas and establishing an on-site communication network. This paper investigates how a cyber attack on a rescue robot can adversely affect its operation and impair an emergency response operation. The focus is on identifying physical indicators of an ongoing cyber attack, which can help to design more efficient detection and defense mechanisms. A number of experiments have been conducted on an Arduino based robot, under different cyber attack scenarios. The results show that the cyber attack's effects have physical features that can be used in order to improve the robot's robustness against this type of threat.**

***Keywords*-emergency response; cyber security; rescue robots.**

I. Introduction

During an emergency response operation, numerous participants have to work simultaneously in order for the overall outcome to be successful. However, a disaster is very often associated with adverse conditions which make it impossible for first responders to perform their duty. Imagine, for example, a building collapsing as a result of an earthquake or of a terrorist attack. Emergency personnel searching the debris for survivors do not have access to all disaster locations, due to the following factors: the physical size of voids can be significantly smaller than the size of an adult, hazard (such as fire) can be present in specific areas and potential rescue passages can be too dangerous due to structurally unstable debris. Robotic vehicles can serve as extensions of emergency personnel by enabling them to access the aforementioned locations.

However, the operation of cyber-physical systems such as robotic vehicles often depends heavily on computer networks. A cyber attack against or through an associated network may impact the physical operation of the vehicle and impair the outcome of the rescue operation. This paper investigates the impact of a denial of service attack on an experimental robotic vehicle. Initial observations indicated that the robot's movement would quickly become erratic for a sufficiently high attack rate. The goal is to identify physical features for detecting a denial of service attack against the robot, instead of only using cyber features such as communication rate.

The rest of this paper is structured as follows: Section II begins with an overview of existing approaches that tackle the problem of cyber attacks on vehicles. A description of the robotic testbed is given in Section III, while Section IV presents the experimental results and elaborates on their significance. Finally, Section VI contains conclusions and directions for future work.

II. Related Work

A comprehensive review of cyber threats related to communication, sensing, information management and vehicular technologies used in emergency management is given in [1], while a taxonomy providing a global view of the respective attack types and defense mechanisms is presented in [2]. Cyber-physical systems have been the subject of numerous emergency response applications. The authors in [3] present a smart navigation system for disaster management while a distributed emergency management simulator which can operate in conjunction with a Wireless Sensor Network for real-time hazard monitoring is presented in [4]. An extended survey of cyber-physical systems geared towards emergency management is presented in [5], where the authors elaborate on current research related to sensor-assisted evacuation and asynchronous control of large scale emergency response systems. Moreover, the effects of malicious attacks to emergency management systems are investigated in [6]. Finally, the use of autonomous robots for the establishment of a communication network between trapped civilians and an operation centre is presented in [7] and [8].

Recent research [9] has demonstrated that cyber-physical attacks can target production automobiles, since these vehicles incorporate various sensing and computing modules that can interact with each other in multiple ways. Initial attacks infected the vehicle's electronic systems through the use of an audio file in the MP3 player device or through smartphone connected via bluetooth. One of the possible results of this attack is a change in the driving direction while the vehicle is in motion.

Apart from automobiles, another popular type of attack is related to unmanned vehicles such as military UAVs. Off-the-shelf software was used by Iraqi militants in order to intercept UAV video feeds. The original use of the software was satellite TV interception, however it could successfully apply to unencrypted military feeds as well [10]. This incident resulted in military aircrafts being retrofitted with video encryption modules. US military UAVs have also been the target of cyber-physical attacks. In 2011 numerous UAVs have been infected by viruses which resulted in the installation of key-logging software. The most probable motive for this attack was the creation of a mapping between the signals emitted by the pilot's keystrokes and the corresponding vehicle parts that were operated. Moreover, Iranian television broadcasted images of a US UAV and claimed that it was hijacked and landed intact using electronic warfare. Since military vehicles have been targeted and compromised by cyber attacks, it is evident that civilian UAVs used by the police or by emergency services can also be hijacked and potentially flown into a crowd. Researchers from the University of Texas have demonstrated this by using a helicopter drone [11]. Furthermore, researcher at Purdue University have investigated the autopilot mechanism of UAVs and have modelled numerous cyber attacks that could exploit it [12]. The authors of [13] have conducted a security assessment by performing cyber attacks on a robot running the Robot Operating System and found that it is vulnerable to insider threats and to being physically compromised. Finally, an enhanced telesurgery protocol is presented in [14] which aims at addressing the stringent requirements related to telesurgical robotics.

Research dealing with cyber-physical attack detection has mainly focused on integrity attacks against industrial control systems. Attackers modify the payload of a network packet and manipulate a cyber-physical system into performing the wrong physical action [15]. Replay attacks are another type of cyber-attack which is difficult to detect using generalist approaches. They target systems which are expected to be in steady time for a long period of time. The authors in [16] present a detection method for replay attacks, however it targets only a specific type of controllers (infinite horizon linear quadratic Gaussian controllers) and cannot be easily applied more broadly. Another approach for cyber-attack detection involves measuring anomalies between physical and cyber properties of a cyber-physical system. These methods are inherent to the nature of a cyber-physical system but must overcome numerous challenges, such as timing. The work presented in [17], [18] detects integrity and availability attacks against a storage tank control system by using the water level measurements reported by the SCADA module. The approach is based on the fact that water level can only change at rates related to pipe diameters and tank capacity. A similar approach based on semantic errors is presented [19] and uses temperature reading outside a specific range to detect an intrusion. The authors state that by integrating the intrusion detection module in the middleware layer of an embedded system, they can achieve better results due to simultaneous access to application logic and communication streams among distributed components.

The aforementioned approaches focus on cyber attacks against pedestrian and aerial vehicles, including potential detection and defense mechanisms. They do not address, however, this problem in the context of robotic vehicles used for emergency management. The aim of this works is to investigate cyber attacks targeted at robotic vehicles used during a disaster, in order to provide efficient and accurate detection mechanisms based on physical indicators.

III. The Robotic Testbed

Experiments where conducted using the robot illustrated in Figure 1. This is a 4WD robot controlled via an on-board Intel Atom computer running the Linux operating system. An Arduino micro-controller is responsible for driving the robot's motors. The robot is also equipped with a webcam mounted on a pan and tilt system. This provides a live feed of the robot's location which enables remote navigation and enhances situational awareness. The control of the robot is achieved via Wi-Fi, by relaying commands received over a TCP socket to the robot's control board. Finally, the rear wheel motors are fitted with magnetic encoders which provide information on the angular position of each wheel. The overall robotic system's architecture is depicted in Figure 2.

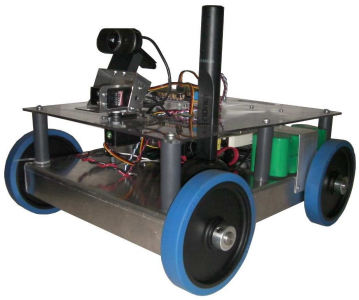

Figure 1. The robot used in our experiments

In order to focus the investigation solely on the physical effects of the cyber-attack and to eliminate any side factors which could potentially interfere with this goal, numerous modifications were made to the testbed.

Friction: While the robot moves on the floor, the variable friction between the floor surface and the wheels can interfere with speed and steering control. To avoid this, the robot was positioned on a stand, effectively lifting

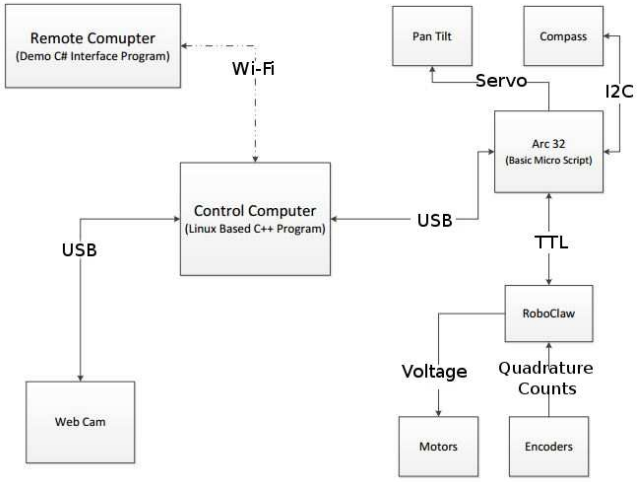

Figure 2. The robotic system's architecture

it from the floor and providing consistent friction to all four wheels. This setup also enabled overcoming the space limitations of the research lab and to conduct experiments involving long movement paths.

Network Interface: While launching a cyber-attack against the rescue robot, it is possible that parameters affecting the wireless communication between the controller and the robot (such as signal strength) interfere with the functionality of the robot. Since the focus was on the physical effects of the attack, a wired Ethernet connection was used for communication.

Power Supply: Under normal operation conditions the robot is powered by a 24V battery pack. After running lengthy experiments it was observed that the battery depletion rate was significantly affecting the motors' power, which had a direct impact on measurements regarding the robot's speed. To remove this factor from affecting our results, the battery pack was replaced with a desktop DC power supply. This also removed the battery life limitation and conduct lengthy experiments.

IV. Denial of Service Attack Against a Robotic Vehicle

To identify possible physical indicators resulting from a cyber attack, a Denial of Service (DoS) attack is launched against the rescue robot and the effects related to the movement of the robot are measured. This Section gives the details of the approach used along with the experimental results.

A. Robot Movement Monitoring

As mentioned in Section III, the rear robot wheels are equipped with magnetic encoders. Each of these devices, reports a value for the angular position of the wheel at any given time. The encoders communicate their measurements to the Arduino micro-controller, which in turn sends the relevant data to the Intel Atom on-board computer. The encoder values were used to calculate the angular speed of the wheels, which is directly related to the robot's linear speed for a given value of the wheels' radius. A value of 30ms was chosen as the sampling period for the encoders, which is the highest monitoring rate supported by the encoders.

As a comment related to the experimental equipment, we should note that the values reported by the magnetic encoders suffer from oscillations. After multiple experiment runs, we determined that this is due to limitations of the respective hardware. The side-effects of this are visible in the angular speed figures of Sections IV-C and IV-D. In these Sections we chose to show the raw experimental data, without applying any kind of smoothing (e.g. a moving average).

B. DoS Attack Characteristics

We used a multi-threaded Denial of Service attack script to flood the robot's network interface with TCP traffic. As mentioned in Section III, we used a wired connection to communicate with the robot. Figures 3 and 4 illustrate the incoming and outgoing traffic rate at the robot's network interface under normal operation and under an ongoing DoS attack.

Table I
Average network traffic at robot interface(bytes/s)

	Attack-off	Attack-on
Outgoing	822.9	595860.8
Incoming	585.5	7858101.2

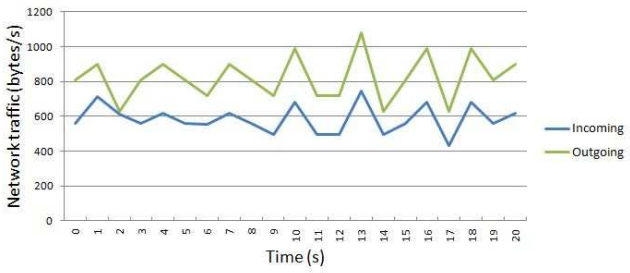

Figure 3. Robot network interface traffic under normal operation

C. Scenario 1: Constant Robot Speed

Our first scenario involves the robot moving at a constant speed. The robot's speed is set by a remote software application and its value can range from 0 to 127. For this scenario we chose a speed value of 94, which results in an angular speed depicted in Figure 5 where the robot operates

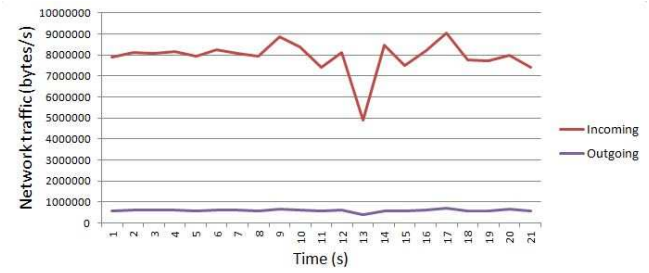

Figure 4. Robot network interface traffic under DoS attack

without the presence of a DoS attack. This graph is the result of sampling the wheel encoders with a period of 30ms, as mentioned in Section IV-A.

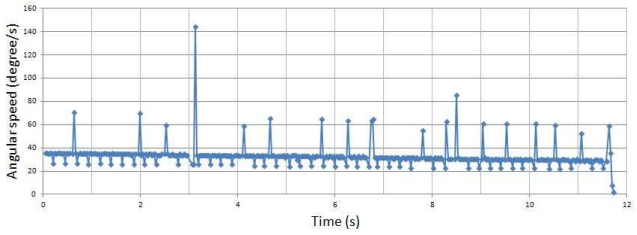

Figure 5. Angular speed vs. time under normal operation

The next stage of this scenario involves the robot moving with the same selected speed, but while sustaining a DoS attack as described in Section IV-B. The result of this setting is depicted in Figure 6.

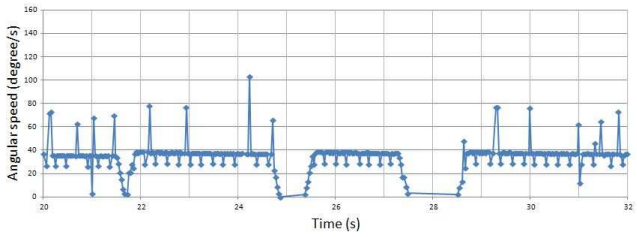

Figure 6. Angular speed vs. time under DoS attack

D. Scenario 2: Variable Robot Speed

Our second scenario involves the robot changing between two speed levels (slow - high). Our aim is to evaluate the effect of the DoS attack on the responsiveness of the robot with respect to navigation commands. The slow speed setting we chose is 81 and the high speed setting is 94. The timing of the speed changes, illustrated in Table II, is achieved by an automated script running on the remote controller computer and communicated to the robot over a wired network.

Figures 7 and 8 depict the angular speed of the robot's wheels versus time, without and with DoS attack respectively.

Table II
VARIABLE SPEED TIMING

Speed	Speed Value	Duration(ms)	Start	End
Low	81	6000	0	6000
High	94	6000	6000	12000
Low	81	6000	12000	18000

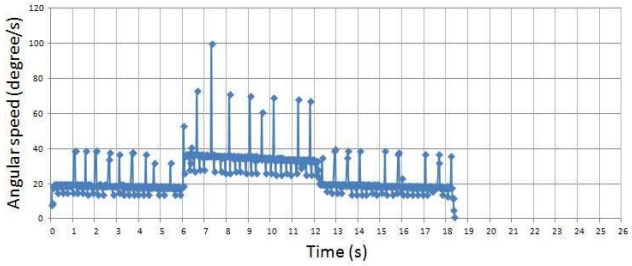

Figure 7. Angular speed under normal operation

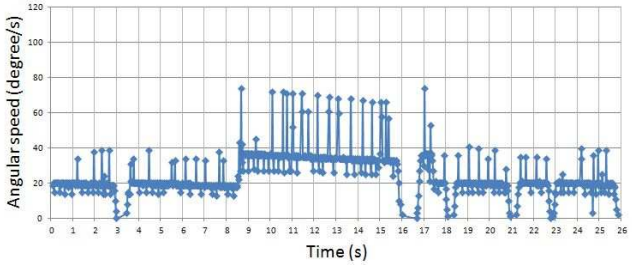

Figure 8. Angular speed under DoS attack

E. Physical Indicators

Our results clearly indicate that launching a cyber attack against a rescue robot is accompanied by physical effects which impair the vehicle's movement. More specifically, we have identified two significant physical indicators related to a cyber attack.

Robot Halting: The first physical indicator we identified by inspecting the experimental results, is the robot's movement pattern. Figures 6 and 8 clearly show that when the robot is under a DoS attack, its movement becomes erratic. More specifically, in Figure 6 we can observe that the robot halted four times. Moreover, each of the halts has a different duration. A similar behaviour is shown in Figure 8, where the robot's speed varies throughout the course of the experiment. We can observe that in this case the robot halted six times.

Delay in Responding to Navigation Commands: A second significant physical feature that emerges from the robot's behaviour when it is under a DoS attack, is depicted in Figure 8. We can clearly see there is a delay of 2.5s in transitioning from the low to the high speed setting. Moreover, the overall duration of the robot's movement is prolonged by 7s.

V. A Hybrid Cyber-Physical Attack Detection Scheme

Our aim is to combine our derived physical indicators with traditional network intrusion detection schemes to provide a more efficient detection and defense mechanism. As we demonstrated in our experiments, attacking the robotic vehicle resulted in both network and physical effects. In this section we present initial experimental results of a hybrid approach, which uses our physical indicators combined with an Intrusion Detection System.

The physical indicator used was robot halting, as discussed in Section IV-E. We decided to use Snort [20] as our Intrusion Detection System (IDS) since it is the most widely adopted IDS technology. We installed Snort on the robotic vehicle's computer and configured it to detect an ongoing cyber-attack. Snort uses rules in order to raise an alert for an ongoing cyber-attack. More specifically, the user must define a threshold which specifies the minimum number of DoS packets received before Snort creates a new alert.

Our experiment consisted of two phases. In the first phase (from 0 to 10 seconds) we attacked the robot with a low rate DoS traffic. As we can see in Figure 9, there is physical indication of an attack while Snort does not raise an alert. In the second phase (from 10 to 25 seconds) we increase the rate of DoS traffic. This triggered an alert from Snort as well as stronger physical indications (i.e. longer robot halting periods).

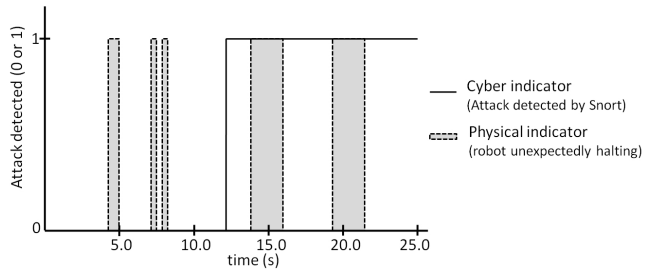

Figure 9. Attack detection using IDS combined with physical indicators

Our experimental results demonstrate the significance of using physical indicators for cyber-physical attack detection. Our physical detection element gave an early indication of the attack, before Snort was able to detect it. After Snort starts detecting the attack, the stronger physical indication can be used to further confirm the detection.

VI. Conclusions and Future Work

In this paper we have presented our experimental results regarding the physical effects of a cyber attack on a rescue robot. Our approach is based on a Denial of Service Attack launched against the robotic vehicle. We investigated two different robot movement scenarios and collected angular speed measurements coming from the magnetic encoders at the vehicle's wheels. Our experiments indicate that the cyber attack results in physical effects which significantly disrupts the movement of the robot.

The significance of these observations lies in the fact that they can be used inside a hybrid attack detection system operating in real-time on the rescue robot. Our initial results demonstrate that using physical indicators can enhance the detection of an attack. In future work we will investigate the integration of our physical indicators with an attack detection and prevention mechanism. A potential next step would be the development of a self-aware system [21] that would use the physical identifiers to generate early warnings of a cyber attack and effectively defend against it. Moreover, we will conduct further experiments under different scenarios that look at other physical aspects of the robot such as its power consumption.

References

[1] G. Loukas, D. Gan, and T. Vuong, "A review of cyber threats and defence approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205–236, 2013.

[2] ——, "A taxonomy of cyber attack and defence mechanisms for emergency management networks," in *Proceedings of the Third International Workshop on Pervasive Networks for Emergency Management (IEEE PerNem 2013), San Diego, CA, USA*, 2013, pp. 18–22.

[3] A. Filippoupolitis and E. Gelenbe, "A distributed decision support system for building evacuation," in *Proceedings of the 2nd IEEE International Conference on Human System Interaction*. Catania, Italy: IEEE, New York, NY, USA, May 21-23 2009, pp. 323–330.

[4] N. Dimakis, A. Filippoupolitis, and E. Gelenbe, "Distributed building evacuation simulator for smart emergency management," *The Computer Journal*, vol. 53, no. 9, pp. 1384–1400, 2010.

[5] E. Gelenbe and F.-J. Wu, "Future research on cyber-physical emergency management systems," *Future Internet*, vol. 5, no. 3, pp. 336–354, 2013.

[6] E. Gelenbe, G. Gorbil, and F.-J. Wu, "Emergency cyber-physical-human systems," in *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*. IEEE, 2012, pp. 1–7.

[7] A. Filippoupolitis, G. Loukas, S. Timotheou, N. Dimakis, and E. Gelenbe, "Emergency response systems for disaster management in buildings," in *Proceedings of the NATO Symposium on C3I for Crisis, Emergency and Consequence Management, Bucharest, Romania*, 2009, pp. 1–14.

[8] S. Timotheou and G. Loukas, "Autonomous networked robots for the establishment of wireless communication in uncertain emergency response scenarios," in *Proceedings of the 2009 ACM symposium on Applied Computing*. ACM, 2009, pp. 1171–1175.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 447–462.

[10] S. Gorman, Y. J. Dreazen, and A. Cole. (2009, dec) Insurgents hack u.s. drones. [Online]. Available: http://online.wsj.com/news/articles/SB126102247889095011

[11] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *Proceedings of the ION GNSS Meeting*, 2012.

[12] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," *The American Institute of Aeronautics and Astronautics: Reston, VA, USA*, 2012.

[13] D. D. Mascarenas, J. McClean, C. J. Stull, and C. R. Farrar, "A preliminary cyber-physical security assessment of the robot operating system (ros)," Los Alamos National Laboratory (LANL), Tech. Rep., 2013.

[14] G. S. Lee and B. Thuraisingham, "Cyberphysical systems security applied to telesurgical robotics," *Computer Standards & Interfaces*, vol. 34, no. 1, pp. 225–229, 2012.

[15] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control*, ser. HSCC '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 31–45.

[16] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, 2009, pp. 911–918.

[17] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *eCrime Researchers Summit (eCrime), 2010*, 2010, pp. 1–9.

[18] B. Reaves and T. Morris, "Discovery, infiltration, and denial of service in a process control system wireless network," in *eCrime Researchers Summit, 2009. eCRIME '09.*, 2009, pp. 1–9.

[19] E. Naess, D. Frincke, A. McKinnon, and D. Bakken, "Configurable middleware-level intrusion detection for embedded systems," in *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, 2005, pp. 144–151.

[20] M. Roesch, "Snort - lightweight intrusion detection for networks," in *Proceedings of the 13th USENIX Conference on System Administration*, ser. LISA '99. Berkeley, CA, USA: USENIX Association, 1999, pp. 229–238. [Online]. Available: http://dl.acm.org/citation.cfm?id=1039834.1039864

[21] E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," *Comput. Netw.*, vol. 51, no. 5, pp. 1299–1314, Apr. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2006.09.009