A Global–Local Approach for Estimating the Internet's Threat Level

Spyridon Kollias, Vasileios Vlachos, Alexandros Papanikolaou, Periklis Chatzimisios, Christos Ilioudis, and Kostas Metaxiotis

Abstract: **The Internet is a highly distributed and complex system consisting of billion devices and has become the field of various kinds of conflicts during the last two decades. As a matter of fact, various actors utilise the Internet for illicit purposes, such as for performing distributed denial of service attacks (DDoS) and for spreading various types of aggressive malware. Despite the fact that numerous services provide information regarding the threat level of the Internet, they are mostly based on information acquired by their sensors or on offline statistical sampling of various security applications (antivirus software, intrusion detection systems, etc.). This paper introduces** *proactive threat observatory system* **(PROTOS), an open-source early warning system that does not require a commercial license and is capable of estimating the threat level across the Internet. The proposed system utilises both a global and a local approach, and is thus able to determine whether a specific host is under an imminent threat, as well as to provide an estimation of the malicious activity across the Internet. Apart from these obvious advantages, PROTOS supports a large-scale installation and can be extended even further to improve the effectiveness by incorporating prediction and forecasting techniques.**

Index Terms: **Computer virus, forecasting, intrusion detection, security, time series.**

I. INTRODUCTION

Currently, one of the most stimulating trends and research fields is "Internet of things" (IoT) that refers to a worldwide network of interconnected objects (called "things") that can be uniquely identified and interoperate seamlessly [1]. Actually, the IoT vision is to eventually interconnect people and objects over the Internet by realising an environment that will implement connectivity of "any-thing", "any-time", "any-place". The IoT applications are vast, covering numerous everyday fields and activities. Nonetheless, the full realisation of IoT faces many challenges such as security/privacy, energy efficiency, standardization/policy restrictions, quality of service (QoS) requirements and several other issues that require further research so that they can be addressed in an efficient way [2]. Furthermore, important challenges arise from the large volume of the collected and processed data.

As it can be easily understood, the continuous connection to the Internet (since it is required for the communication, interoperation and management of all things) poses several security issues. The reason is that the attack surface significantly increases alongside with the number of connected devices/things and, given the heterogeneousness among such devices, one should therefore expect the simultaneous existence of multiple exploits. Moreover, recent real-world examples of "malicious" clothes irons, kettles and fridges [3], [4] demonstrate that such exploitation scenarios do not longer belong to science fiction and should be taken into serious consideration. Furthermore, the wide range of personal electronic devices featuring Internet connectivity, once compromised, can also become sources of valuable private information (namely, user habits and behaviour), as well as becoming members of a wider botnet. Given the continually-increasing availability of public WiFi hotspots (many of them having weak or no security mechanisms) and the increased use of various Internet services (e.g., social networks and web surfing), the risk for an individual thing/device/user to fall victim of such attacks is significant. Furthermore, the malicious exploitation of many devices with Internet connectivity may also have a significant impact on the local network's normal operation (such as misuse of bandwidth, energy depletion of mobile nodes, triggering of alarms and so on). Related research has been also carried out and important findings have been announced about the security threats in IoT in the fields of sensor networks [5]–[7], smart grids [8], or even in the case of connected vehicles [9].

One way for dealing with such threats in a generic form, would be to evaluate the malicious activity of a network by examining the nodes' firewall log files (wherever this is feasible) and send this information to a central processing server, in order to obtain a "global view" of the threat landscape. As soon as an increase in the global malicious activity is detected, the server will inform the member nodes to tighten their security settings, in order to protect themselves. Our approach is essentially an early warning system which is capable of estimating the threat level across the Internet, using both a global and a local approach. A sufficient amount of sensors is required for systems like *proactive threat observatory system* (PROTOS) for measuring the threat level with an acceptable accuracy. Several frameworks for distributed detection have already been proposed, however they suffer from the following drawbacks:

- A large-scale installation is a feature of only some of them.
- None of them is able to determine whether a specific host is under an imminent threat or not.
- Some of them operate under a commercial license, requiring some sort of a paid subscription.

This paper is an extended version of the work presented in [10] and includes a detailed description regarding the architecture of one such scheme, as well as some results from an initial, small-

Manuscript received April 12, 2014.

S. Kollias and K. Metaxiotis are with the Department of Informatics, University of Piraeus, Greece, email: spyridon.kollias@gmail.com, kmetax@unipi.gr.

V. Vlachos and A. Papanikolaou are with the Department of Computer Science and Engineering, Technological Educational Institute of Thessaly, Larissa, Greece, email: vsvlachos@teilar.gr, alxpapanikolaou@gmail.com.

P. Chatzimisios and C. Ilioudis are with the Department of Information Technology, Alexander Technological Educational Institute of Thessaloniki, Greece, email: {peris, iliou}@it.teithe.gr.

Digital object identifier 10.1109/JCN.2014.000070

scale experimental deployment.

The remainder of this paper is structured as follows: Section II provides related work about various distributed thread detection frameworks that can be found in the literature. Section III presents a high-level description of the proposed system architecture, as well as the expressions for measuring the malicious activity. In Section IV, we present initial results from the experimental operation of PROTOS. Furthermore, in Section V, we discuss certain issues that have been identified during the deployment of PROTOS, as well as potential extensions like prediction and forecasting, targeting to improve the effectiveness of the system. Finally, Section VI summarises and concludes this paper by also providing future work.

II. RELATED WORK

For early warning systems like PROTOS, a sufficient amount of sensors is required in order to measure the threat level with an acceptable accuracy. In the literature, several frameworks for distributed detection have already been proposed, but none of them features a large-scale installation.

More specifically, one such example is the work in [11] proposes algorithms for the early detection of the presence of Internet worms, by using a suitable Kalman filter on the monitored illegitimated traffic. Their results demonstrate that their algorithms are able to detect worms at the early stages of their life, while the infection rate is still quite low (1%–2% of the vulnerable computers), as well as to give effective predictions of the number of vulnerable hosts. In [12] the architecture of a *distributed intrusion detection system* (DIDS) combines distributed monitoring of individual hosts with centralised data analysis, in order to be able to monitor heterogeneous systems. Each host is assigned a user ID (comprising, among others, and a host ID) to facilitate monitoring, although more work is required on connecting instances of the same user in a networked environment, should the user leave the monitored domain and then comes back in with a different user ID. The authors in [13] proposed a system that operates by analysing network traffic characteristics and attempts to detect patterns that denote the presence of a worm (e.g., highly repetitive packet content) and automatically generates content signatures. When tested on a small network, the scheme featured a low percentage of false positives. In the same way, the authors in [14] collect Internet control message protocol (ICMP) unreachable messages from selected network routers and then analyse them to identify patterns indicating malicious scanning activity as well as patterns that can identify a propagating worm. The proposed system is tested in a simulated environment, in order to assess its performance. Certain variants of PROTOS tailored for different topologies are also in operation. They mainly follow either peer-to-peer or other decentralised topologies [15], [16].

Well-known security vendors provide such worm detection services to their users, with Symantec's DeepSight [17] being perhaps the most famous system. Similar to that but focused on network hardware, Cisco has developed IronPort [18], which takes into consideration numerous parameters, in order to opine if a node of a network is secure or not. Both systems operate under commercial license. More specifically, DeepSight has a pricing plan which cannot be ignored and IronPort demands the presence of Cisco network hardware. As downside, these two systems cannot be adopted from individuals, small or medium companies. Nowadays, even large companies are reluctant to invest on such systems. Finally, DShield [19] is a well known system with more than 500,000 IP addresses measuring for current threat level.

Several research projects have focused on detecting threats in large-scale architectures. In the VIS-SENSE project, the researchers used visual analytics to develop more effective tools for border gateway protocol (BGP) monitoring and prefix hijack detection to illustrate how network visualisation has the potential to assist an analyst in detecting abnormal routing patterns in massive amounts of BGP data [20]. The research in the SPAMCLOUD project evaluates the degree of feasibility and applicability of Hadoop's MapReduce framework when applied to spam filtering in a large scale architecture [21]. HARMUR is a security dataset developed in the context of the WOMBAT project that aims at exploring the dynamics of the security and contextual information associated to malicious domains [22]. SGENT is a framework of honey-farms for detecting of malicious operational faults in computing systems, namely intrusions [23].

When it comes to sensor networks, since they mainly consist of resource-constrained nodes whose energy is a very precious asset, the focus is on simply detecting an abnormal or malicious behaviour, rather than determining the exact cause of the attack. The authors in [24] propose a secure routing protocol that takes into account the existence of multipath between sender and destination to transmit data in several paths, in order to prevent denial of service (DoS) attacks. Securing the communications among the wireless sensor network (WSN) nodes is quite a challenging task. Nevertheless, cryptographic techniques exist that can simplify certain parts of this task. Quite recently a secure hybrid wireless mesh protocol (HWMP) was proposed, identity-based cryptography (IBC)-HWMP, where control messages are secured using IBC, in order to simplify key management [25], [26].

III. ARCHITECTURE

A. High-Level Overview

The system PROTOS consists of different software and hardware layers. An overview of the system's architecture is presented in Fig. 1. The most important and critical part of the whole system is the PROTOS sensor, which periodically scans the local firewall log file and extracts the entries representing blocked packets and/or connection attempts. The number of sensors is vital for obtaining an accurate measurement of the global threat level. The more the sensors, the better the accuracy will be. Although there are no significant challenges from a software point of view, the whole system demands for a satisfactory amount of individual sensors. It can be installed to a wide range of computers, ranging from an average PC to a mainframe server. The sensors that are installed on systems with public IP addresses provide more accurate information about the "global" threat level; systems that are behind network address translation (NAT) can provide significant information for the internal net-

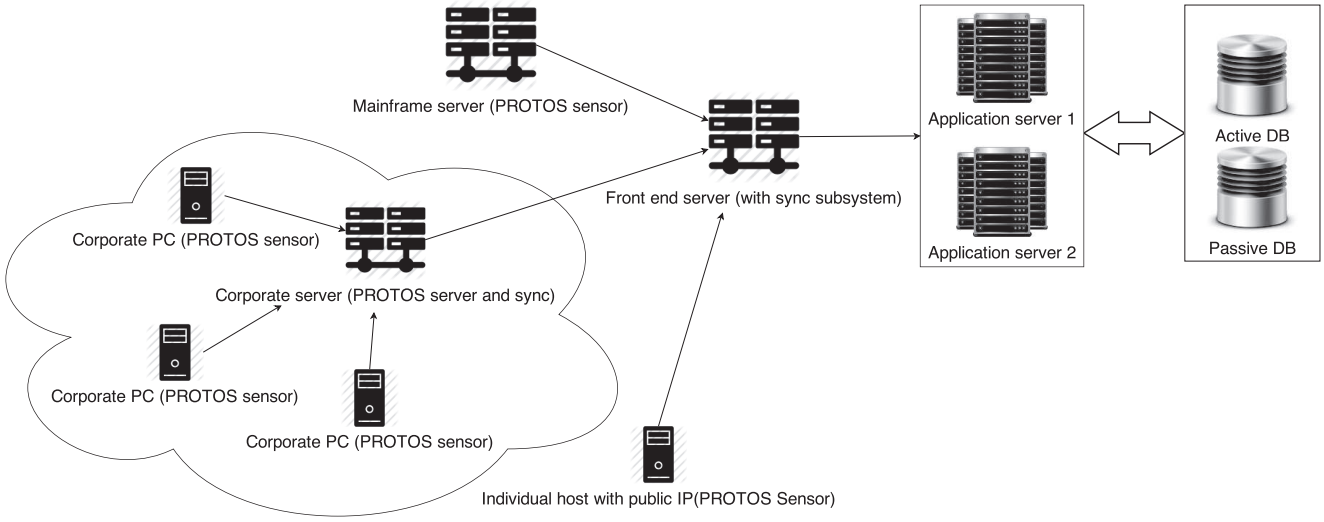

Fig. 1. Overview of the PROTOS system architecture.

work ecosystem. This kind of intelligence can be utilised from administrators to realise any inside threat.

Another critical system is the PROTOS server, which is responsible for collecting and aggregating the intelligence received by its sensors and the corporate internal servers. It must feature high availability to receive the information provided by its collateral systems on a 24/7 basis, without any interruptions. Apart from the reception system, the server's hardware must be powerful and optimised to run small, yet intensive, tasks in little time. It is worth noting that two databases (active and passive) are being used for ensuring high system availability. The active database is the primary one and should it become unavailable for some reason, the passive one takes over.

Moreover, a sync subsystem between corporate servers with PROTOS server instance and the main PROTOS server instance must be installed, in order to have almost real-time synchronisation regarding the collected information from internal corporate hosts.

Furthermore, two additional subsystems have been implemented: A cross-platform desktop application and a web application, which depict all the aggregated intelligence in an intuitive GUI.

```
{ "clientid": "f38ef048-621e-5a29-93bf-d7843099c27e",
  "rate1": "1.52",
  "rate2": "2.47",
  "tcount": "50",
  "localip": "192.168.1.1" }
```

Fig. 2. Example record containing the summary sent to the server, in JSON format.

```
{ "datetime": "2013-02-03 12:45:20",
  "action": "DROP",
  "protocol": "TCP",
  "srcip": "192.168.1.64",
  "dstip": "192.168.1.2",
  "srcport": "63576",
  "dstport": "443",
  "size": "52",
  "tcpsyn": "2937187733",
  "tcpack": "0",
  "tcpflags": "S",
  "tcpwin": "8192",
  "icmptype": "-",
  "icmpcode": "-",
  "info": "-",
  "path": "RECEIVE" }
```

Fig. 3. Example record of the full details sent to the server, in JSON format.

B. Detailed Description

As has already been mentioned, PROTOS relies upon the PROTOS sensor, which is responsible to collect the required information from each individual host. An update mechanism has also been developed, in order to be able to automatically update to new versions, not only for providing bug fixes, but also for coping with potential changes in the way the native firewall logs the blocked packets. The update mechanism is a crucial part of the sensor, as it allows it to maintain its viability. In addition, relying on users to perform manual updates is subject to negligence, thus rendering the given sensors useless and consequently jeopardising the effectiveness of the whole system. The collected data is being stored locally on a lightweight database, to facilitate processing. Each PROTOS sensor sends to the server the locally intercepted malicious rates every 30 s and the full details of the blocked packets every 6 h.

The aforementioned time intervals were empirically chosen, as a good balancing between system overhead (local disk activity, server load, network bandwidth) and ability to react timely in case an epidemic is detected. Further optimisation of these time intervals is possible, provided that detailed profiling takes place on a wide range of platforms, using appropriate metrics, so as to deduce the best possible configuration on a per-platform basis. The transmission of these values to the server takes place through two different web services, using messages in JSON format (Fig. 2 and Fig. 3).

An SQLite file is the lightweight database containing one

table where all the required information of blocked packets is stored, such as:

- Protocol
- Timestamp
- Source IP
- Destination IP
- Source port
- Destination port
- Action taken
- Additional protocol-specific information (e.g., TCP flags)
- Other platform-specific information.

The PROTOS server orchestrates all the critical and crucial parts of the PROTOS system. The server is in charge of collecting the data, aggregating them and storing them to the database. Future functionality will include the ability to send notifications to both the administrators and the individual users, so as to warn them about an imminent threat.

Furthermore, work is in progress so as to implement a collaboration between the server and the sensor in order to provide automatic protection to the systems that run PROTOS sensor. For instance, in case an epidemic is detected, the sensor could instruct the system to tighten its security level by blocking the IPs that have been classified as malicious.

The web services are made available through an Apache web server and the community edition of MySQL is used as the database for storing the information sent from the sensors. The database consists of two tables. In the first one, the raw data packets received from each individual sensor are stored; the second table holds the calculated aggregated malicious activity. The latter is calculated every 30 s, based on the received data.

A local installation of a PROTOS server can serve the requirements of enterprise networks. It will be fully functional within the company's ecosystem and able to run as a stand-alone instance. In addition, if required, it will be possible to to cooperate with the main PROTOS server.

A web application has also been developed, in order to provide a visual overview of the current global malicious activity, according to the information provided by the active sensors. Its functionality will be enhanced in the future to include ability to retrieve:

1. Past data of the recorded malicious activity.
2. Metadata regarding the malicious activity, such as most used ports, top source IPs, and most used protocols.

The web application has been implemented using HTML and JavaScript libraries. The information is retrieved by calling the appropriate web services through AJAX interfaces and the diagrams are updated every 30 s, reflecting the latest trends.

Last but not least, a cross-platform desktop application is being developed using Java technologies. The UI uses JavaFX to depict the malicious activity, epidemic rate and top metadata information. The user is able to choose a specific time interval or view results in real time, for either the local activity (if a sensor has been installed to the system) or the global activity. Furthermore, the desktop application is able to provide diagnostics information, in order to ensure the correct operation of the installed sensor.

The PROTOS system architecture follows the n-tier architecture model, as depicted in Fig. 4.

C. Measuring the Malicious Activity

The typical operation of a PROTOS sensor is as follows: It checks the firewall log file every 30 s and calculates the number of the intercepted attacks in the form of dropped/denied packets. By using (1) and (2) it estimates the rate of the locally-intercepted malicious activity and the epidemic rate, respectively. In these equations, t is the ordinal number of a fixed time interval, n is the client identifier, h_t^n is the number of security incidents received by node n in the time interval t. The "time window" used in a number of t time intervals is $k, k \in (0, t-1)$.

$$p_t^n = \frac{h_t^n - \frac{\sum_{i=t-k}^{t-1} h_i^n}{k}}{\frac{\sum_{i=t-k}^{t-1} h_i^n}{k}}, \tag{1}$$

$$q_t^n = \frac{p_t^n - \frac{\sum_{i=t-k}^{t-1} p_i^n}{k}}{\frac{\sum_{i=t-k}^{t-1} p_i^n}{k}}. \tag{2}$$

Thereafter, the sensor transmits this information to the server, which computes the global malicious activity, based on (3).

$$p_{\text{avg}} = \frac{\sum_{i=1}^{n} p_i^t}{n}. \tag{3}$$

Should the calculated estimate of the global malicious activity exceed a predefined upper threshold, the server instructs the sensors to increase their security level by applying a set of predefined countermeasures. Similarly, if the global malicious activity drops under the lower threshold, the sensors loosen their security settings and resume their normal operation. The values for these thresholds have been determined both empirically and via simulations. In particular, their aim is to render the system able to respond timely and correctly in anticipated malware epidemics. If the lower threshold is set at a very low value, it will cause an overreaction of the system; namely, the countermeasures will constantly be enabled, thus leading to a loss of the system's functionality, due to the disabled/blocked services. On the other hand, setting a very high value to the higher threshold will limit the system's ability to timely detect any incoming threats and therefore its ability to adequately protect its members. The values for the lower and upper threshold have mainly emerged from the work in [27], as well as through the simulated experiments conducted in [16] and [28]. In addition, we examine the possibility to allow users to set custom threshold values, thus overriding the default settings.

IV. EXPERIMENTAL OPERATION

The system, in its current form, is operational and the basic functions have been implemented. The service modules are working on a 24/7 basis without creating any critical issues. The PROTOS client has been installed in a small number of workstations and some initial data has been gathered. PROTOS is available for both 32-bit and 64-bit of Microsoft Windows OS, as well as for Linux and Mac OS X. There is work in progress on developing a secure update mechanism for the respective client. The system's scalability has also been assessed in a laboratory environment, by using simulated data.

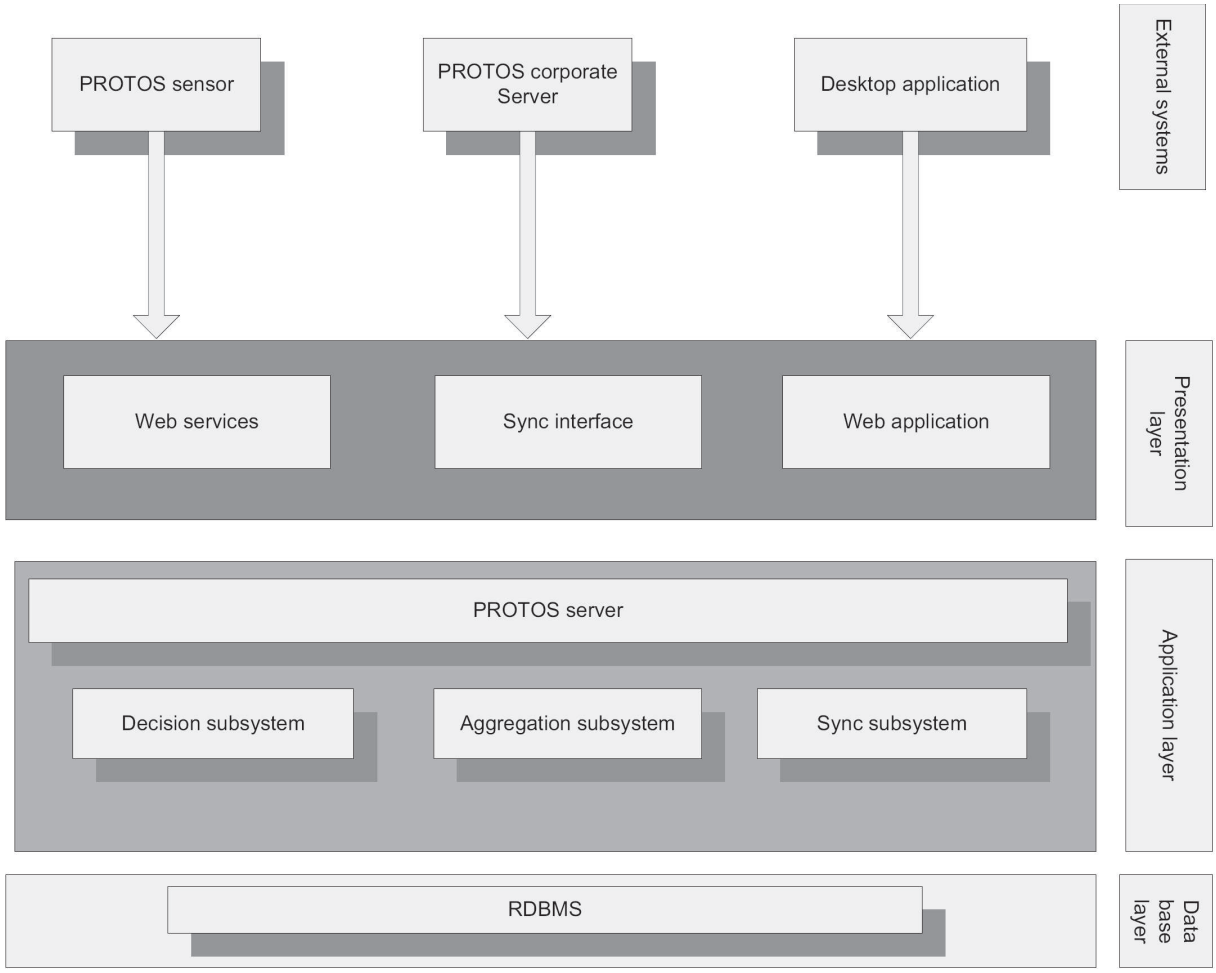

Fig. 4. The PROTOS n-tier architecture.

The PROTOS system was initially put into operation on 4th April 2013 and currently has more than 230 unique clients connected to it. Of course, not all of them are concurrently in operation; an initial statistical analysis showed that a few decades of sensors are usually transmitting data to the server at any given instance. The sensors' scope is currently limited to the Greek cyberspace, as they have been deployed in three major Greek cities (Athens, Patras, and Larissa). It is expected that the geographical coverage will increase soon, as several users have already opted for participating.

As far as the system's performance is concerned, the CPU load is mainly observed for the various database-related (MySQL) tasks. The database server is responsible for:

- Inserting the received data whenever they arrive from the sensors. Hence, the more the sensors, the higher the load. At the same time, the table columns containing each record's timestamp are indexed.
- Processing the aggregated intelligence of the last 30 s, for each user observing the live plot, either from the web site or the local client (the so-called "universal client").
- Processing intelligence on demand (currently under development).
- Calculating the aggregate intelligence by running a scheduled task every 30 s.

Hence, within the aforementioned context, the observed peak CPU load of the database server daemon was 45%. Quite a common case is to have approximately 20 to 30 unique clients transmitting data to the server. In such cases, especially if the intercepted malicious activity is relatively low, the corresponding processing power requirements are almost negligible. In particular, MySQL daemon requires 75 MB of RAM and 300 MB of swap file, whereas the CPU load fluctuates between 0%–1%. Given that the server of this experimental operation is a virtual machine (VM) on quite old hardware, we are confident that running it on suitable, high-performance hardware it should be able to support a high number of sensors.

The system modules of PROTOS have shown that they are not inducing any significant overhead to the overall performance of the clients. PROTOS sensor will be capable of running on systems with low-end hardware specifications, varying from netbooks to cheap laptops. More specifically, when the client service was loaded on an MS Windows XP (SP3) PC bearing an AMD Athlon 64 3000+ and 1 GB of RAM memory, it consumed 11.5 MB of RAM. Whenever the service process scanned and processed the firewall log file (namely, every 30 s), a peak CPU usage of 17% was noticed. The client has also been successfully deployed on a Raspberry Pi host (bearing an ARM CPU), running Ubuntu Linux as an indicative example of a non-x86 ar-

chitecture. A number of available platforms are been currently evaluated, but the fact that several popular Linux distributions already support the ARM architecture significantly simplifies the implementation on ARM-equipped sensors. As has already been mentioned, PROTOS supports a variety of additional operating systems as well (e.g., Mac OS X, Linux), although it is currently dependent on their native firewall. A full evaluation of the prototype system has been planned for the near future, in terms of scalability and overhead of both the server and the client. It will also be investigated whether individual and corporate users are willing to use PROTOS with a software firewall other than the operating system's native firewall.

Fig. 5 demonstrates the intercepted activity over a 3-hour-long period on 3rd February 2014. In particular, the time series depicts the number of blocked packets, as they have been recorded in 30-second-long intervals. In a local network there may be certain devices (e.g., broadcast packets from printers) or applications (e.g., file syncing) that tend to send broadcast packets. Since such packets get blocked by the hosts' firewalls, any sensors installed on them will report some "malicious activity", represented by the short periodic peaks. Using this information, the server calculated both the malicious activity and the epidemic rate for the given period of time, which are exhibited in Fig. 6. It is worth clarifying that, due to the order the calculations are performed, an observed peak in the number of blocked packets within the time interval t will appear in the malicious activity graph at $t + 1$ and in the epidemic rate graph at $t + 2$.

V. FUTURE WORK

The functionality of PROTOS depends on the analysis of firewall log files, a task that its sensors perform for each host they are installed on. Nevertheless, there are cases where certain devices do not offer any sort of firewall functionality (e.g., smartphones and more "primitive" resource-constrained devices), as well as cases where access to the firewall log file is only possible by obtaining administrative access to the device, without having explicit functions for it (e.g., broadband modem/routers for home or office use). Therefore, one of the future tasks will involve the development of a firewall application for popular smartphone operating systems (e.g., Android and iOS), able to run transparently in the background whenever Internet access is enabled, so that its log file can be exploited by a suitable PROTOS sensor application. In addition, efficient and secure ways for gaining access to firewall log files produced by e.g., home broadband modem/routers should be investigated, where one of the greatest challenges is the diversity in both the functionality and characteristics of said devices.

Another issue worth investigating is the way information and control messages are communicated between the server and its sensors, in order to ensure maximum compatibility with different communication protocols, especially those for resource-constrained devices. For instance, if extensible markup language (XML) or simple object access protocol (SOAP) messages are to be used, they will have to be carefully crafted, so as to ensure compatibility with the more resource-constrained versions of the standards, such as the constrained application protocol–CoAP (a lightweight version of SOAP over CoAP was recently proposed in [29]). Although it may not always be possible for resource-constrained devices to offer PROTOS-sensor-like functionality, they could still benefit from the system's warning messages. In turn, the applicability of suitable mechanisms for ensuring both the integrity and the authenticity of the transmitted data will be investigated, such as digital signatures and hash functions.

As has already been mentioned, the PROTOS system requires a server, responsible for communicating with its sensors. Since a world-wide installation of a single server does not seem a plausible task, having multiple such servers, each one responsible for a given "reign" is a possible solution (similar to the way multiple Kerberos systems can be configured to co-operate among them [30]). In turn, this raises issues of how the borders of these "reigns" will be defined, how communication among different "reigns" will be performed, what kind of information will it contain and so on.

Most of the past research has put significant efforts into developing large-scale intrusion detection systems (IDS) and their successors, intrusion prevention systems (IPS). The importance of detection and prevention is definitely necessary, however, as the number of the interconnected devices rises, the development of global services that monitor the threat level across the Internet is equally important. Most of the IDS/IPS system aim at protecting small- to medium-sized networks by acquiring and analysing large amounts of data of the hosts they supervise, in order to detect malicious activity. The idea of PROTOS is based on the fundamentals of crowdsourcing intelligence which has been employed for solving various difficult problems. The first versions of the PROTOS system utilise well-known and widely-accepted epidemiological models which have been proved effective against biological as well as computer viruses, over the past years. The introduction of statistical forecasting models is currently under evaluation in order to obtain more accurate predictions of imminent threats. Theoretical research and empirical findings have proved that the available reaction timeframe against ultra-virulent malware and other threats cannot be achieved using the existing methods.

VI. CONCLUSION

Nowadays, the number of objects/things connected to the Internet exceeds the number of the connected people and the IoT significantly affects user's life in many different positive ways. However, there are still many important issues to be addressed, many of which are related to security risks and disclosure of personal information. At the same time, malevolent hackers devise highly-sophisticated ways of exploiting such devices for illicit purposes, the effects of which usually include both a significant world-wide impact and a small margin for reaction and treatment. Another aspect to be considered is the degree to which malicious activity is successfully detected and contained, since any kind of problematic behaviour in an IoT world (having billions of interconnected devices, sharing and running numerous applications) will directly impact the quality of services provided to users.

Our work introduced the PROTOS proactive system that is able to deal with such kinds of threats. A central server analyses data (related to malicious activity) that is collected by sensors

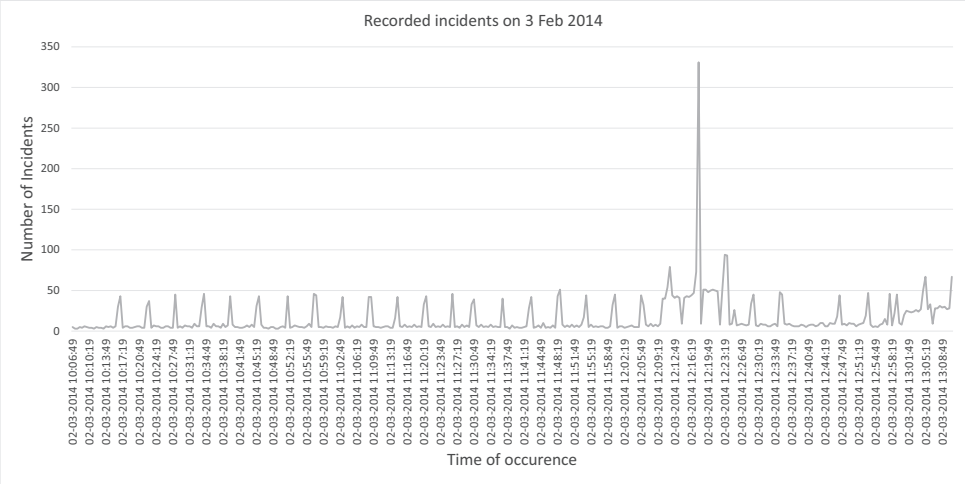

Fig. 5. Number of blocked packets in 30-second-long intervals on a given date.

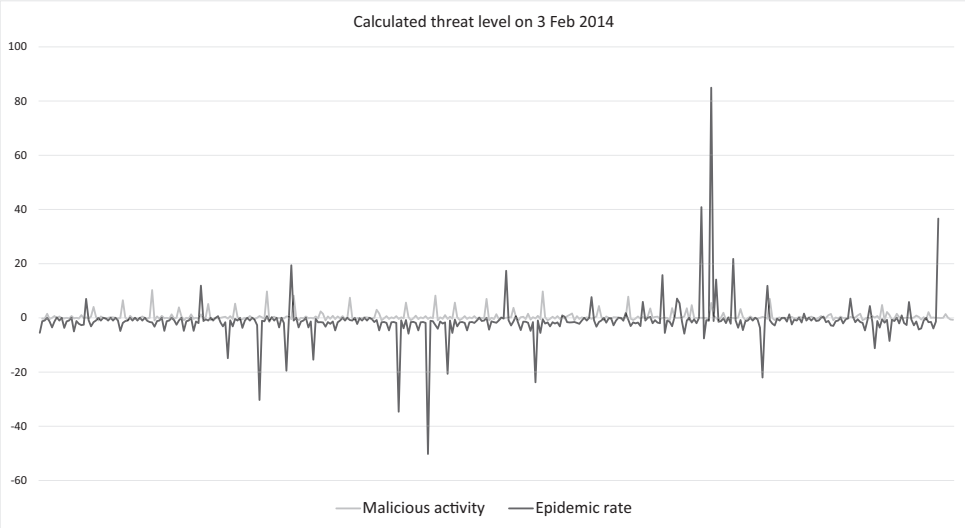

Fig. 6. Calculated malicious activity and epidemic rate on a given date.

operating on multiple hosts. The threat level is then calculated both at a local and global level in order to take the appropriate measures. Although, the developed system is currently in experimental operation, the obtained results are so far encouraging. Future work includes to deal with several open issues/challenges that were identified and have to be resolved in order for the system to be able to support a wider range of heterogeneous devices. Another research direction that can be considered is to develop and study suitable prediction and forecasting methods that can be applied to PROTOS, targeting to strengthen the system's effectiveness.

REFERENCES

[1] D. Evans, "The Internet of Things – How the next evolution of the internet is changing everything," white paper, *Cisco IBSG*, Apr. 2011.

[2] T. Kaukalias and P. Chatzimisios, "Internet of Things (IoT) – enabling technologies, applications and open issues," in *Encyclopedia of Information Science and Technology*, IGI Global Press, 3rd ed., 2014.

[3] (2013, Oct.). "Russia: Hidden chips 'launch spam attacks from irons'." BBC News. [Online] Available: http://www.bbc.com/news/blogs-news-from-elsewhere-24707337

[4] (2014, Jan.). "Fridge sends spam emails as attack hits smart gadgets." BBC News. [Online] Available: http://www.bbc.com/news/technology-25780908

[5] M. Covington and R. Carskadden, "Threat implications of the Internet of Things," in *Proc. CyCon*, June 2013, pp. 1–12.

[6] P. Kasinathan *et al.*, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proc. IEEE WiMob*, Oct. 2013, pp. 600–607.

[7] L. Fagen and X. Pan, "Practical secure communication for integrating wireless sensor networks into the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3677–3684, 2013.

[8] K. A. Ahmed, Z. Aung, and D. Svetinovic, "Smart grid wireless network security requirements analysis," in *Proc. IEEE GreenCom*, Aug. 2013, pp. 871–878.

[9] J. Soryal and T. Saadawi, "DoS attack detection in Internet-connected vehicles," in *Proc. ICCVE*, Dec. 2013, pp. 7–13.

[10] S. Kollias *et al.*, "Measuring the Internet's threat level: A global–local approach," in *Proc. IEEE PEDIWESA*, June 2014.

[11] C. C. Zou *et al.*, "Monitoring and early warning for internet worms," in *Proc. ACM CSS*, Oct. 2003, pp. 190–199.

[12] S. R. Snapp *et al.*, "DIDS (Distributed Intrusion Detection System)–motivation, architecture, and an early prototype," in *Proc. National Comput. Security Conf.*, 1991, pp. 167–176.

[13] S. Singh *et al.*, "The earlybird system for the real-time detection of unknown worms," Tech. Rep. CS2003-0761, UCSD, Department of Computer Science, Aug. 2003.
[14] V. H. Berk, R. S. Gray, and G. Bakos, "Using sensor networks and data fusion for early detection of active worms," in *Proc. AiroSense*, 23 Sept. 2003, pp. 92–104.
[15] V. Vlachos, S. Androutsellis-Theotokis, and D. Spinellis, "Security applications of peer-to-peer networks," *Comput. Netw.*, vol. 45, no. 2, pp. 195–205, 2004.
[16] V. Vlachos and D. Spinellis, "A PROactive malware identification system based on the computer hygiene principles," *Inform. Management Comput. Security*, vol. 15, no. 4, pp. 295–312, 2007.
[17] "Symantec deepsight early warning services." [Online]. Available: http://tms.symantec.com/
[18] "Cisco IronPort reputation filters." [Online]. Available: http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/ironport_reputation_filters.pdf
[19] "Dshield." [Online]. Available: http://www.dshield.org/
[20] E. Biersack *et al.*, "Visual analytics for BGP monitoring and prefix hijacking identification," *IEEE Network*, vol. 26, no. 6, pp. 33–39, 2012.
[21] G. Caruana, M. Li, and H. Qi, "SpamCloud: A MapReduce based antispam architecture," in *Proc. FSKD*, vol. 6, Aug. 2010, pp. 3003–3006.
[22] C. Leita and M. Cova, "HARMUR: Storing and analyzing historic data on malicious domains," in *Proc. EuroSys BADGERS*, Apr. 2011, pp. 44–51.
[23] C. Leita and M. Dacier, "SGNET: A worldwide deployable framework to support the analysis of malware threat models," in *Proc. EDCC*, May 2008, pp. 99–109.
[24] L. Mokdad and J. Ben-Othman, "Performance evaluation of security routing strategies to avoid DoS attacks in WSN," in *Proc. IEEE GLOBECOM*, Dec. 2012, pp. 2859–2863.
[25] J. Ben-Othman and Y. I. Saavedra Benitez, "IBC-HWMP: A novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s," *Concurrency Comput.: Practice Experience*, vol. 25, no. 5, pp. 686–700, 2013.
[26] Y. I. Saavedra Benitez, J. Ben-Othman, and J.-P. Claudé, "Performance comparison between IBE-HWMP and ECDSA-HWMP," *Security Commun. Netw.*, vol. 6, no. 4, pp. 437–449, 2013.
[27] V. Vlachos, *Security Applications of Peer to Peer Networks*. Ph.D. dissertation, DMST, AUEB, July 2007.
[28] V. Vlachos, A. Raptis, and D. Spinellis, "PROMISing steps towards computer hygiene," in *Proc. INC*, July 2006, pp. 229–236.
[29] G. Moritz, F. Golatowski, and D. Timmermann, "A lightweight SOAP over CoAP transport binding for resource constraint networks," in *Proc. MASS*, 2011, pp. 861–866.
[30] C. Neuman *et al.*, "The Kerberos network authentication service (v5)," RFC 4120, IETF–Network Working Group, July 2005.

Spyridon Kollias is a Ph.D. candidate in the field of Computer Security, regarding forecasting methodology of security data and research associate of Forecasting & Strategy Unit, School of Electrical and Computer Engineering of the National Technical University of Athens (NTUA), Greece. He received his B.Sc. in Computer Science & Telecommunications from the Technological Educational Institute (TEI) of Larissa, Greece and an M.Sc. in Financial Software Engineering from the Centre for Computational Finance and Economic Agents (CCFEA) of the University of Essex, UK. He is an Official Translator of the Greek Chapter of OWASP.org and a Leading Software Engineer in a Greek software company. His major interests are software engineering, software sensor systems (agents), and computer security measurement and forecasting.

Vasileios Vlachos is a Lecturer at the Department of Computer Science and Engineering of the Technological Educational Institute (TEI) of Thessaly, Larissa, Greece. He is a Senior R&D Engineer at the Research Academic Computer Technology Institute (R.A.C.T.I.) of Patras, Greece. He was a Member of the Digital Awareness and Response to Threats (DART) team of the Special Secretariat for Digital Planning of the Hellenic Ministry of Economy and Finance. He holds a B.Eng. in Electronic&Computer Engineering from Technical University of Crete, Greece, an M.Sc. in Integrated Hardware and Software Systems from the Department of Computer Engineering and Informatics of the University of Patras, Greece, and a Ph.D. in Information Systems Security from the Department of Management Science and Technology of the Athens University of Economics and Business. He has taught courses at several Greek Universities, including the University of Thessaly, the University of Central Greece and the University of Piraeus. He is Co-Founder and Coordinator of DART-NGO (Non Governmental Organisation).

Alexandros Papanikolaou is an Adjunct Lecturer at the Department of Computer Science and Engineering of the Technological Educational Institute (TEI) of Thessaly, Larissa, Greece. He holds a B.Sc. in Computer Science and a Ph.D. in Cryptography and Information Security, both from Aston University (Birmingham, UK). His research interests include the evolution of cryptographic techniques and their applications, wireless sensor networks security, and cybercrime and intrusion detection systems.

Periklis Chatzimisios (SMIEEE) serves as an Associate Professor with the Computing Systems, Security and Networks (CSSN) Research Lab of the Department of Informatics at the Alexander TEI of Thessaloniki (ATEITHE), Greece. He received a B.Sc. in Informatics from ATEITHE, continued his studies with scholarship in Bournemouth University (UK) and received a Ph.D. in 2005. He holds Editorial Board positions for several IEEE/non-IEEE journals such as IEEE Wireless Communication Magazine, IEEE Communications Letters, IEEE Communications Surveys & Tutorials, Wiley Transactions on Emerging Telecommunications Technologies, IET Wireless Sensor Systems, Springer Wireless Networks. He has organized more than 20 Special Issues in prestigious journals and he is acting as a Director for the IEEE MMTC E-letter. Moreover, he has served in the Organizing/TPC Committee for more than 100 conferences. He is the author of 8 books and more than 80 peer-reviewed papers and book chapters in the areas of wireless mobile communications, multimedia communications and security. His published research work has received more than 1300 citations by other researchers.

Christos Ilioudis obtained his B.Sc. degree in Computer Science from the University of Crete and his Ph.D. on Internet Security from the Aristotle University of Thessaloniki, Greece. Since 2007, he is an Associate Professor of Informatics Department, Alexander TEI of Thessaloniki, Greece. He has taught information systems security and Internet technology and services. His research interests include the areas of Internet technology and security, cloud and big data security. He has been working on several EU research projects on security area and he has been author of several research articles in international journals and conferences.

Kostas Metaxiotis is an Associate Professor at the Department of Informatics of the University of Piraeus. He is Member of the Executive Board of Directors of World Capital Institute (WCI). He has wide experience in knowledge management, knowledge-based development, artificial intelligence, enterprise information systems, and ERPs. He is an Associate Editor (and Editor-in-Chief 2011-2013) of the International Journal of Knowledge Based Development. He has served as Guest Editor in many journals, including the Journal of Knowledge Management for the Special Issue "Knowledge-Based Development 2010". Since 1996, he has been participating in various European Commission (EC)-funded projects within Tacis, Phare, MEDA and IST Programmes as Senior ICT Consultant and Manager. Since 2007, he has been serving as External Evaluator of EC-funded ICT projects in Balkans.