HYBRID ARCHITECTURE FOR DISTRIBUTED INTRUSION DETECTION SYSTEM IN WIRELESS NETWORK

Seyedeh Yasaman Rashida

1Department of Computer Engineering, Shirgah Branch, Islamic Azad University
Shirgah, Mazandaran, Iran

s.y.rashida@gmail.com

ABSTRACT

In order to the rapid growth of the network application, new kinds of network attacks are emerging endlessly. So it is critical to protect the networks from attackers and the Intrusion detection technology becomes popular. Therefore, it is necessary that this security concern must be articulate right from the beginning of the network design and deployment. The intrusion detection technology is the process of identifying network activity that can lead to a compromise of security policy. Lot of work has been done in detection of intruders. But the solutions are not satisfactory. In this paper, we propose a novel Distributed Intrusion Detection System using Multi Agent In order to decrease false alarms and manage misuse and anomaly detects.

KEYWORD

Intrusion Detection, Agent, Architecture, Misuse detection, Signature-based

1. INTRODUCTION

With the evolution of computer networks, computer security has also revolted from securing giant mainframes in the past to securing large scale unbounded computer networks. The need for computer security has become even critical with the proliferation of information technology in everyday life. The nature of threat has changed from physical infiltration and password breaking to computer viruses, self-propagating and self-replicating worms, backdoor software, Trojan horses, script kiddies, computer criminals, terrorists and the list is long.

The increase in dependability on computer systems and the corresponding risks and threats has revolutionized computer security technologies. New concepts and paradigms are being adopted, new tools are being invented and security conscious practices and policies are being implemented. There is a clear need for novel mechanisms to deal with this new level of complexity.

Network intrusion-detection systems (NIDSs) are considered an effective second line of defence against network-based attacks directed to computer systems [4, 3], and – due to the increasing severity and likelihood of such attacks – are employed in almost all large-scale IT infrastructures [2]. Intrusion Detection System (IDS) must analyse and correlate a large volume of data collected from different critical network access points. This task requires IDS to be able to characterize distributed patterns and to detect situations where a sequence of intrusion events occurs in multiple hosts. . In this paper, we propose a novel Distributed Intrusion Detection System using Multi Agent In order to decrease false alarms and manage misuse and anomaly detects.

DOI : 10.5121/ijnsa.2013.5305

The rest of this paper is organized as follows: in Section 2 reviews literature of related works. Section 3 presents an architecture of our hybrid IDS; While section 4 and 5 present unique characteristics and disadvantages of our hybrid IDS. In section 6, we have evaluated the performance of proposed scheme. And Section 7 and 8 concludes the paper with future research directions and challenges in IDS.

2. RELATED WORKS

Generally, the deployment of WSN in an unattended environment and the use of wireless signals as the media for communication make it easy for eavesdroppers to get the signals. Moreover, the limitations in processing, storage and battery lifetime make the security issues of these networks difficult. Different types of attacks against WSN have been explored in the literature like, attacks on sensed data, selective forwarding attacks, sinkhole attacks, hello flood attack and many more[5]. In the following we provide a review of some relevant prior work. In [6], the mobile agent based intrusion detection system were developed which uses the trace gray technique to detect the intrusions. A proposed efficient anomaly intrusion detection system in Ad-hoc by mobile agents[7] which uses the data mining algorithm to detect the attacks exploited by the intruders. Mobile agent based intrusion detection system for MANET [9] proposed by yinan Li which uses the clustering and joint detection technique to identify the intruders. In [21], Focus of the paper is on the clustering WSNs, designing and deploying Cluster-based Intrusion Detection System (CIDS) on cluster-heads and Wireless Sensor Network wide level Intrusion Detection System (WSNIDS) on the central server. In [8], intrusion detection in distributed networks is studied. They consider agent and data mining independently and their mutual benefits. M. Saiful Islam Mamun and A.F.M. Sultanul Kabir propose a hierarchical architectural design based intrusion detection system that fits the current demands and restrictions of wireless ad hoc sensor network. In the proposed intrusion detection system architecture they followed clustering mechanism to build a four level hierarchical network which enhances network scalability to large geographical area and use both anomaly and misuse detection techniques for intrusion detection. They introduce policy based detection mechanism as well as intrusion response together with GSM cell concept for intrusion detection architecture [22]. The paper [10] presents the preliminary architecture of a network level IDS. The proposed system monitors information in network packets and learning normal patterns and announcing anomalies. Another approach is presented in [13], in which Cooperative Security Managers (CSM) are employed to perform distributed intrusion detection that does not need a hierarchical organization or a central coordinator. Each CSM performs as local IDS for the host in which it is running, but can additionally exchange information with other CSMs. The architecture also allows for CSMs to take reactive actions when an intrusion is detected. Unclear aspects are the mechanisms through which CSMs can be updated or reconfigured, and the intrusion detection mechanisms that are used locally by each CSM.

The idea of employing widely distributed elements to perform intrusion detection, by emulating to some extent the biological immune systems, and by giving the system a sense of "self", has also been explored [12].

Intrusion detection is the process of monitoring and analyzing the data and events occurring in a computer and/or network system in order to detect attacks, vulnerabilities and other security problems [16]. IDS can be classified according to data sources into host-based detection and network-based detection. In host-based detection, data files and OS processes of the host are directly monitored to determine exactly which host resources

are the targets of a particular attack. In contrast, network-based detection systems monitor network traffic data using a set of sensors attached to the network to capture any malicious activities.

Networks security problems can vary widely and can affect different security requirements including authentication, integrity, authorization, and availability. Intruders can cause different types of attacks such as Denial of Services (DoS), scan, compromises, and worms and viruses [17, 18]. The approach for using Agents in ID that was the foundation for our work was proposed in [4, 3]. These papers introduced the idea of lightweight, independent entities operating in concert for detecting anomalous activity, prior to most of the approaches mentioned previously.

3. SYSTEM ARCHITECTURE

We propose new architecture for building IDSs that uses agents as their lowest-level element for data collection and analysis and employs a structure to allow for scalability. In general, there are mainly two techniques for intrusion detections: i) misuse (signature-based) detection and ii) anomaly (behavior-based) detection [20]. In the paper, we apply both techniques. Purpose of applying both techniques is in attempting to detect any attacks or intrusions in a system. As shown in the Fig. 1, the proposed IDS architecture consists of seven modules – Tracker, Anomaly Detection Module, Misuse Detection Module, Monitor, Signature Generator, Inference Detection Module and Countermeasure Module combining the results of the three detection modules.

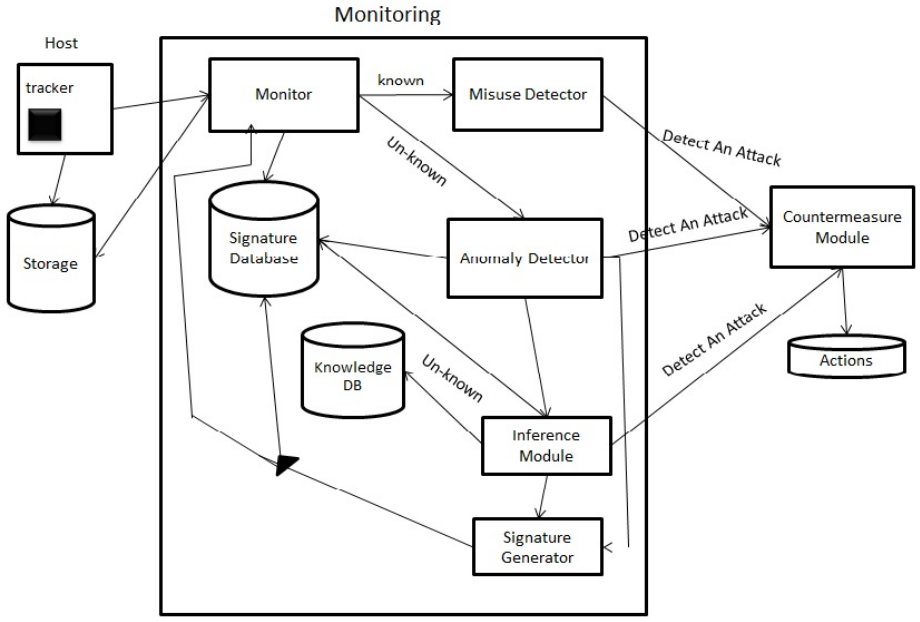

Figure1. The proposed Architecture for Intrusion Detection System

In the following sections, each module is explained in more detail.

a. Tracker: Tracker is an independently running entity that monitors certain aspects of a host. The agent would then generate a report that is sent to the appropriate Monitor and also is stored in Storage. The agent does not have the authority to directly generate an alarm. Usually, Countermeasure Module will generate an alarm based on information received from one or more agents/ detectors. By combining the reports from different agents, Monitor builds a picture of the status of their host.

b. Monitor: Analyse an on-going process to find out whether it behaves according expectation. On the other hand, the Monitor compares the received packets it observes with the signatures or rules of normal patterns of behavior stored in Signature database by using pattern matching algorithm. If Monitor finds any match then sends appropriate message for known attack to the Misuse Detector Module. Also it enters entry in log file about the event that caused the alert. If Monitor does not find any match then sends data to Anomaly detector for finding anomaly using pattern mining technique.

c. Misuse Detector: The misuse detection agent is worked like Monitor but the difference between them is on detail. In fact, each monitor acts as independent IDS and detects attacks for itself only without sharing any information with another IDS node of the system, even does not cooperate with other systems. So, all intrusion detection decisions are based on information available to the individual node. Its effect is too limited. However, each node runs its own misuse detector and finally they collaborate to form a global misuse detector. The agent is used to analyse the data captured by the Monitor agent globally. It detects the known attacks in network by using the pattern matching algorithm. If there is a similarity between the received reports and attack signatures in the database, then it reports to Countermeasure Module for deciding on solutions.

d. Anomaly Detector: The anomaly detection agent is used to detect the new or unknown attacks by using the classification techniques. Classification is concerned with establishing the correct class (or category) for an object. The classification is based on characteristics of the object [15]. The anomaly detection agent collects the data from the monitor to analyse the data to detect the unknown attacks. Then it classifies to detect the new attack. The specification of the classification model is shown in Fig. 3. The first *While* loop generates the set of candidate solutions. The second *While* loop prunes this set by obtaining new information. The method finishes if one of the following three conditions is true.

Fig. 2 shows the corresponding inference structure. Three inferences are used in the method plus a transfer function for obtaining the attribute value:

- Generate candidate: In the simplest case, this step is just a look-up in the knowledge base of the potential candidate solutions.
- Specify attribute: There are several ways of realizing this inference. The simplest way is to just do a random selection. This can work well, especially if the "cost" of obtaining information is low. Often however, a more knowledge-intensive attribute specification is required. One possibility is to define an explicit attribute ordering as is the case in a decision tree. This requires domain knowledge of the form "if attribute *a* has value *x* then ask about attribute *b*". Often, experts can provide this type of attribute-ordering information. The specification knowledge then takes the form of a decision tree. A more comprehensive approach is to compute the attribute that has the highest information potential. Several algorithms for this exist. This last approach can be very efficient but may lead to system behavior that is alien to users and experts.

- Obtain feature: Usually, one should allow the user to enter an "unknown" value. Also, sometimes there is domain knowledge that suggests that certain attributes should always be obtained together.
- Match: This inference is executed for every candidate, and produces a truth value indicating whether the candidate class is consistent with the information collected so far. The inference should be able to handle an "unknown" value for certain attributes. The normal approach is that every candidate is consistent with an "unknown" value.

After classification, if anomaly detector finds any anomaly then send appropriate message to Inference Module to more investigation. Otherwise, it sends the report to Countermeasure Module to decide on solution and confront with the attack.

e. Inference Module: Inference is important component of Knowledge models. Inference acts as the building blocks of reasoning process. In the inference knowledge we describe how these static structures can be used to carry out a reasoning process. The module is the highest-level entities in the architecture. They also have control and data processing roles that are similar to those of the anomaly detectors. The main difference between inference module and anomaly detector is that an inference module can control entities that are running in several different hosts whereas anomaly detectors only control local agents. This part decides by knowledge and rules in KB and Signature Base. A knowledge base contains instances of those knowledge types which are related to user's actions. This module uses the naïve bayes classifier to detect the new attack. It classifies the data based on the dataset available in the knowledge database. If the incoming data is detected as attack means then it reports to Signature Generator, which in turn reports to alert agent about the attack. It updates the detected attack in the database.

f. Signature generator: Signature generator creates rule or signature and makes new entry in Signature database. Then it sends appropriate message to Monitor to reanalyse the attack.

g. The Signature database records enable the IDS to have a set of signature, criteria or rules against which they can be used to compare packets as they pass through the host. The signatures database needs to be installed along with the IDS software and hardware itself.

h. Countermeasure module: When Countermeasure module receives the alert message of known attack from Detectors, it notifies the administrator in one of several ways that the administrator has configured beforehand. The module might display a pop-up window or sends an e-mail message to the designated individual, for example. Besides the automated response sent to the administrator, this module can be configured to take action at the same time that an alert message is received. Typical actions are: i) Alarm, in which an alarm is sent to the administrator, ii) Drop, in which the packet is dropped without an error message being sent to the originating computer; and iii) Reset, which instructs the IDS to stop and restart network traffic and thus stop especially severe attacks. This module is also used by network administrator to evaluate the alert message and to take proper actions such as dropping a packet or closing a connection. The administrator can anticipate having to fine-tune the signature database to account for situations that seem to the IDS to be intrusions but that are actually legitimate traffic. For example, an adjustment might be made to enable traffic that might otherwise be seen by the firewall as suspicious, such as a vulnerability scan performed by a scanning device located at a particular IP address. The IDS could be configured to add a rule that changes the action performed by the IDS in response to traffic from that IP address from Alarm to Drop.

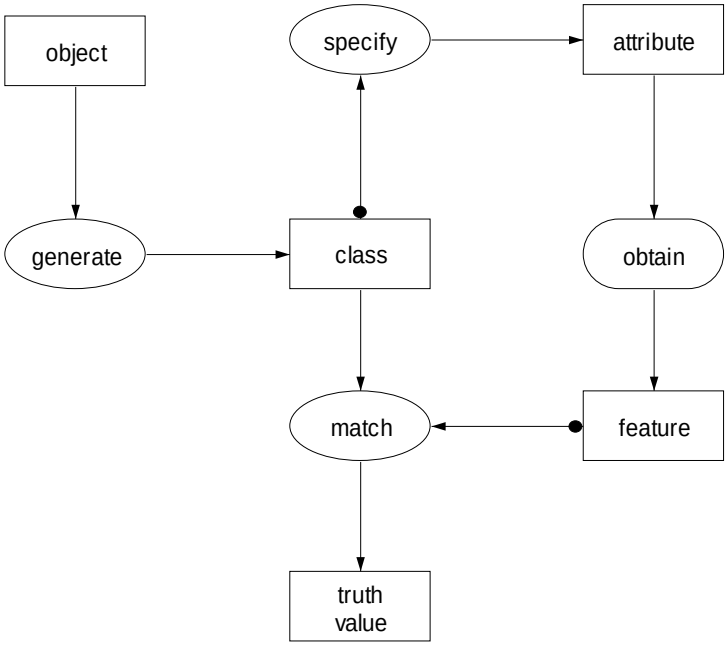

Figure2. The classification Structure

While new-solution generate (object→candidate) **do**

Candidate-classes:=candidate Union candidate-classes;

While new-solution specify(candidate-classes→attribute)

And length candidate-classes > 1 **do**

Obtain(attribute→new-feature);

Current-feature-set:=new-feature union current-feature-set

For each candidate in candidate-classes **do**

Match(candidate+current-feature-set→truth-value);

If truth-value = false **then**

Candidate-classes:= candidate-classes subtract candidate;

Figure3. Method Control of classification Model

\

4. ADVANTAGES OF THE PROPOSED ARCHITECTURE

The following are the list of unique characteristics of our IDS.

- It will run constantly with minimal human supervision. It will create signatures of new attacks.
- It will be applied as Distributed IDSs.
- It will be adaptive in nature and adapts the changes in user and system behavior.
- It will provide information to tracking attackers.
- Design of our IDS makes it fault tolerant, so that it will be able to recover from crashes. It will be able to get its prior state and resume its operation without any adverse effect.
- It will be able to monitor itself and detect attacks on it.
- It will be accurate and thereby there will be less number of false positives and false negatives.

5. DISADVANTAGES OF THE PROPOSED ARCHITECTURE

We have identified several shortcomings in the proposed architecture. Detection of intrusions at the Inference Module is delayed until all the necessary information gets there from the agents. This is a problem common to distributed IDSs. The architecture does not specify access control mechanisms to allow for different users to have different levels of access to the IDS. This is an issue that will need to be addressed.

In their control role, Inference Module is single points of failure. If an inference module stops working, all the anomaly detector that it controls stop producing useful information. This can be solved through a hierarchical structure where the failure of an Inference Module would be noticed by higher level monitors, and measures would be taken to start a new inference and examine the situation that caused the original one to fail. Another possibility is to establish redundant monitors that look over the same set of anomaly detector so that if one of them fails, the other can take over without interrupting its operation. If duplicated Inference modules are used to provide redundancy, mechanisms have to be used to ensure that redundant inference modules will keep the same information, will obtain the same results, and will not interfere with the normal operation of the IDS.

6. IMPLEMENTATION

We have performed the analytical performance comparison of our proposed scheme with existing schemes. We analysed their performance on two major factors i.e. Security and Efficiency. The security factor is divided further into three parameters i.e. internal external and novel threats. Internal threats are those attacks that are initiated or injected by the intruder residing inside the network. External threats are from outside attackers. Novel threats are the unusual or unrecognized form of the intrusions which have not occurred previously. Three types of possible values used by these intrusions are low, high and medium that indicates how clearly the proposed scheme identifies these intrusions.

We have given the low value to all those schemes that doesn't provide defence against the compromised node, under attack nodes, inside attackers, master or secret key is captured or the node activity is dependent on the neighbourhood node information, trust relationship on nodes etc. the medium value to the all those proposed scheme that identify the intrusion but does not provide any defensive measurement how to handle them, generate false negative in large amount. The high value to all those schemes that clearly identify the intrusion as well as provide

the counter measure against that intrusion, compromise of one node will not make the whole security of the system vulnerable.

We divide the efficiency factor into three parameters i.e. computation costs, network bandwidth, node resource utilization and number of messages. Two types of values are used high and medium in computation cost, network bandwidth and node resource utilization. We have given high value to all those schemes that increases burden on network resource i.e. cryptographic algorithms are resource hungry in nature that require extra computation and memory overhead, communication steps between nodes increases, simultaneous transmission increases the rate of collision that effect the bandwidth issues, large amount of false negative dissipate the energy resources etc. The medium value is given to the scheme that uses victim resources in order to discover an intrusion by using minimum network resources. The number of messages which contains the integer value i.e. additional steps used by the proposed schemes in order to identify the intrusion. Table 1 shows that our proposed scheme is efficient in several aspects as compare to the existing schemes.

Table 1: Performance comparison between different existing schemes

No.	Scheme Name	Security			Efficiency			
		Internal Threat	External Threat	Novel Threat	Comp. Cost	Net. Bandwidth	Node Resource	No. of Message
1	An IDS for WSN	Medium	Medium	High	--	High	High	--
2	Security Protocol for Sensor Network [1]	Low	High	Low	High	High	High	7
3	Mobile Agent for WSN [9]	Low	High	Low	High	High	High	2
4	Mobile agents for mobile Ad-hoc network [7]	Medium	High	low	--	High	High	--
5	Proposed scheme	High	High	Medium	High	Medium	Medium	--

7. FUTURE WORK

These are some of the specific points we have identified as relevant for future work:

- Developing agents.
- Communication mechanisms.
- Developing Inference Module.
- Semantics of the communication.
- Porting to other platforms.
- Deployment and testing.
- Global administration and configuration.
- Reliability and fault tolerance.

8. CONCLUSION

The main characteristic of misuse (signature-based) intrusion detection technique is in comparing incoming threats against a predefined knowledge base in order to decide whether the threat is considered an attack or intrusion whilst anomaly detection technique involves looking for any unexpected changes in behavior of a system against what is considered normal behavior. Both misuse and anomaly detection techniques have their own advantages and disadvantages. We have used features of both the intrusion detection techniques in our IDS Architecture. This paper presents research from an ongoing study on the use of features of both the intrusion detection techniques to design a novel and efficient hybrid IDS. The proposed design of IDS, however, aims to be more accurate and it does not require more processing resources, thus offering both speed and accuracy to detect the intrusions.

REFERENCE

[1] M. Eid. (2004) A New Mobile Agent-Based Intrusion detection System Using distributed Sensors, In proceeding of FEASC.

[2] Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner, (2000) ‘‘State of the Practice of Intrusion Detection Technologies”, Technical Report CMU/SEI-99TR-028, Carnegie-Mellon University – Software Engineering Institute.

[3] Debar, H., M. Dacier, and A. Wespi, (2000) ‘‘A Revised Taxonomy of Intrusion-Detection Systems,’’ Annales des Telecommunications, Vol. 55, N.7, pp. 361-378.

[4] R. Bace, (2000) Intrusion detection, Macmillan Publishing Co., Inc.

[5] C. Karlof, D. Wagner, (2003) Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, IEEE Xplore Press, pp.113-127.

[6] Ani Taggu, Amar Taggu, (2011) “TraceGray: An Application layer scheme for intrusion detection in MANET using Mobile agents” in Third International Conference on Communication Systems and Networks, pp.1-4.

[7] Yinan Li, Zhihong Qian, (2010) “Mobile agents based intrusion detection system for mobile Ad-hoc network” in International Conference on Innovative Computing and Communication, pp.145-148.

[8] O. Oriola, (2012). Distributed Intrusion Detection System Using P2P Agent Mining Scheme”, African Journal of Computing & ICT, Vol 5. No. 2, pp. 3-10.

[9] N.Jaisankar, R. Saravanan, K. Duraisamy, (2009) “Intelligent intrusion detection system framework using mobile agents”, in International Journal of Network Security and its Applications, Vol. 1, No 2,.

[10] R. Heady, G. Luger, A. Maccabe, “The Architecture of a network level Intrusion Detection System”, 1990.

[11] Damiano Bolzoni, Bruno Crispo, Sandro Etalle, “ATLANTIDES: An Architecture for Alert Verification in Network Intrusion Detection Systems”, 21st Large Installation System Administration Conference (LISA ’07), pp. 141-152.

[12] S. Forrest, S. A. Hofmeyr, and A. Somayaji. (1997) Computer Immunology, Communications of the ACM, Vol. 40, No. 10, pp. 88–96.

[13] G. B. White, E. A. Fisch, and U. W. Pooch, (1996) Cooperating security managers: A peer-based intrusion detection system. IEEE Network, pp. 20–23.

[14] Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, (2005) An intelligent intrusion detection system for anomaly and misuse detection in computer networks, Expert Systems with Applications, Vol. 29, pp. 713–722.

[15] Schrieber, G., H. Akkermans, A. Anjewierden, R.D. Hoog, N. Shadbolt, W.V. Velde and B. Wielinga, (2000) Knowledge engineering and management. The MIT Press.

[16] Jiawei Han and. Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kufmann, 2nd edition, 3rd edition 2011.

[17] S.J. Stolfo, W. Lee. P. Chan, W. Fan and E. Eskin, "Data Mining – based Intrusion Detector: An overview of the Columbia IDS Project" ACM SIGMOD Records vol. 30, Issue 4, 2001.

[18] W. Lee and S.J. Stolfo, (1998) "Data Mining Approaches for Intrusion Detection", 7th USENIX Security Symposium, Texas.

[19] S. Khanum, M. Usman and A. Alwabel, (2012) Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks, IJCSI International Journal of Computer Science Issues, Vol. 9, No 3.

[20] Axelsson, S, (2000) Intrusion-detection systems: A taxonomy and survey, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden.

[21] H. Jadidoleslamy A Hierarchical Intrusion Detection Architecture for Wireless Sensor Networks, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[22] Mohammad Saiful Islam Mamun, HIERARCHICAL DESIGN BASED INTRUSION DETECTION SYSTEM FOR WIRELESS AD HOC SENSOR NETWORK, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.