American Journal of Applied Sciences 10 (9): 979-985, 2013
ISSN: 1546-9239
© 2013 K. Ethala *et al*., This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license
doi:10.3844/ajassp.2013.979.985 Published Online 10 (9) 2013 (http://www.thescipub.com/ajas.toc)

A Role of Intrusion Detection System for Wireless Lan Using Various Schemes and Related Issues

[1]Kamalanaban Ethala, [2]R. Seshadri, [3]N.G. Renganathan and [4]M.S. Saravanan

[1]Department of CSE, Sri Venkateswara University, Tirupathi, India and
Vel Tech University, Avadi, Chennai, India
[2]SVU Computer Center, Sri Venkateswara University, Tirupathi, India
[3]Vel Tech Dr RR and Dr SR Technical University, Avadi, Chennai, India
[4]Department of IT, Vel Tech University, Avadi, Chennai, India

Received 2013-06-19, Revised 2013-07-20; Accepted 2013-07-27

ABSTRACT

The advancement in network based technology and augmented dependability of our everyday life on this technology. During recent years, number of attacks on networks has intensely increased. Hence interest in network intrusion detection has increased among the researchers. This study assesses different kinds of IDS and inclines preemptive procedures. An Intrusion Detection System (IDS) is used to automate the intrusion detection process. An Intrusion Deterrence System (IPS) is software which has complete competencies of an intrusion detection system and it can endeavor to stop probable events.

Keywords: Anomaly, Intruder, Intrusion, HIDS, IDS, NIDS

1. INTRODUCTION

Intrusion Detection Systems (IDS) can serve for three essential security functions. They are observation, identification and reaction to unauthorized activity. The determination of IDS is to identify and avoid electronic threat to computer system. In recent times every person is connected over networks and many services are provided over the internet. This global reach increases the threat of intrusion hazard from unknown sources. The IDS are predominantly absorbed on classifying possible incidents by observing both user and system, logging data about them, examining system arrangements and susceptibility, evaluating file and system integrity, identifying irregular activities and patterns distinctive of attacks and inform them to security administrator (Hu, 2009). Resulting terms give impression about probable extortions to security.

1.1. Risk

Fortuitous or impulsive exposure of information or destruction of operations reliability due to the interruption of hardware or unfinished or improper software design.

1.2. Vulnerability

A recognized or suspected fault in the hardware or software operation of a system that disclosures the system to penetrate or its information to unintentional revelation (Chou *et al*., 2011).

1.3. Attack

A specific formulation or implementation of a strategy to spread out a hazard.

1.4. Penetration

A positive attack--the capability to obtain illegitimate admittance to files and packages or the control state of a computer Machine. Intruders are two kinds the external intruders are illegal users of the system they attack and internal intruders, who have authorization to control the system, but not some part of it. Additional internal intruders are divided into invaders

Corresponding Author: Kamalanaban Ethala, Department of CSE, Sri Venkateswara University, Tirupathi, India and Vel Tech University, Avadi, Chennai, India

who masquerade as another user. Those with genuine access to complex data and the most hazardous type, the intruders those have the influence to turn off audit control for them (Uddin and Rehman, 2010). Different types of threats include.

1.5. Masquerading

Logging into system using illicit justification and password. So event has dissimilar login time, position or joining type than genuine user. They are penetration by reliable user that is user will perform dissimilar programs or activate more for deification violations (Dharmapurikar and Lockwood, 2006). The leakage by reliable user might route data to remote idle printer. The interference by authentic user might attempt to retrieve illegal data from database through combination and implication might recover more record than normal. The Trojan horse package established in system, its performance varies from genuine program in terms of CPU application or I/O activity. The Virus event causes growth in orderliness of executable files revised, loading used by executable files or specific program executed as the virus spread. The Denial of Service (DoS) is a kind of attack on a network that is intended to bring the network to its laps by flooding it with useless traffic (Yu *et al*., 2007). DoS attacks like the Ping of Death and Teardrop attacks, exploit boundaries in the TCP/IP protocols. Normally in DoS attacks, some of the software injects that system administrators can mount to limit the impairment produced by the occurrences. Just like viruses new DoS attacks are repetitively being visualized up by hackers.

2. APPROACHES FOR INTRUSION DETECTION SYSTEMS

The various approaches used for intrusion detection systems they are Anomaly detection, Signature based misuse, Host based and Network based

2.1. Anomaly Detection

ABIDS has attracted many academic researchers due to its impending for lecturing novel attacks. Innovation detection is the documentation of new or unknown data which machine learning system is not conscious of during training (Wheeler, 2006). Anomaly detection IDS have two major benefits over signature based intrusion detection systems. The chief improvement is the capability to detect unidentified attacks as thriving as "zero day" attacks. This is for the reason that the ability of anomaly detection systems to typical the standard process of a system/network and detect eccentricities from them. A second improvement is that the above-mentioned outlines of normal activity are adapted for every system application and network and therefore making it very problematic for an attacker to know with inevitability what events it can carry out without getting noticed. There are two types of anomaly detection systems. They are Statistical based anomaly detection and Signature based approach (Scarfone and Mell, 2007).

2.2. Statistical Based Anomaly Detection (SABIDS)

Statistical modeling is one of the initial methods used for identifying intrusions in electronic information systems. Statistical based anomaly detection approaches practice statistical assets and statistical tests to control whether "Practical concert" deviates pointedly from the "predictable enactment". Statistical approaches used statistical properties (e.g., mean and variance) of usual activities to build a statistical based normal outline and service statistical tests to determine whether practical activities deviate pointedly from the normal outline. The IDS goes on transfer a score to an anomalous activity. As soon as this score becomes greater certain brink, it will produce an alarm (Ashoor and Gore, 2011). SABIDS is a two-step progression: first it launches behavior outlines for the usual activities and present activities. Then these profiles are matched based on various techniques to detect any kind of eccentricity from the usual behavior.

2.3. Dynamic Based Anomaly Detection (DABIDS)

To characterize usual and suitable performance, a base outline is created by Dynamic anomaly intrusion system. Building the Adequately correct base outline is the main struggle with the dynamic anomaly detection system (Narayana *et al*., 2011).

2.4. Signature Based Approach

Signature Based approach is also known as Misuse detection approach. Signature examination Systems are based off of modest pattern identical algorithms. In most cases, the IDS only Looks for a sub string within a stream of files passed by network packets. When it finds this sub string it recognizes those network Packets as vehicles of an occurrence (Montero-Melendez *et al*., 2013). The below **Fig. 1** shows the anamoly based detection and the **Fig. 2** shows the signature based detection agents and IDS.

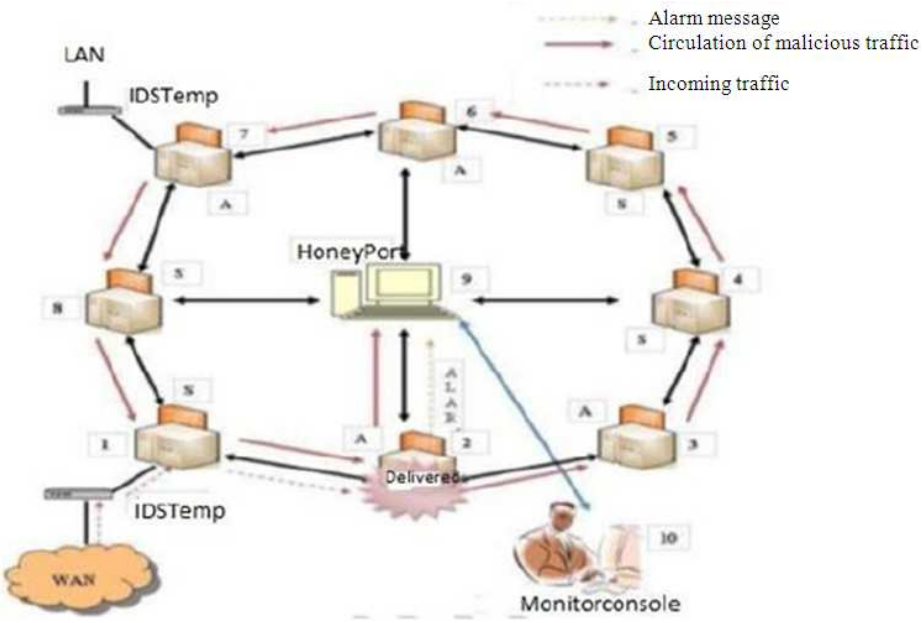

Fig. 1. Anomaly based detection

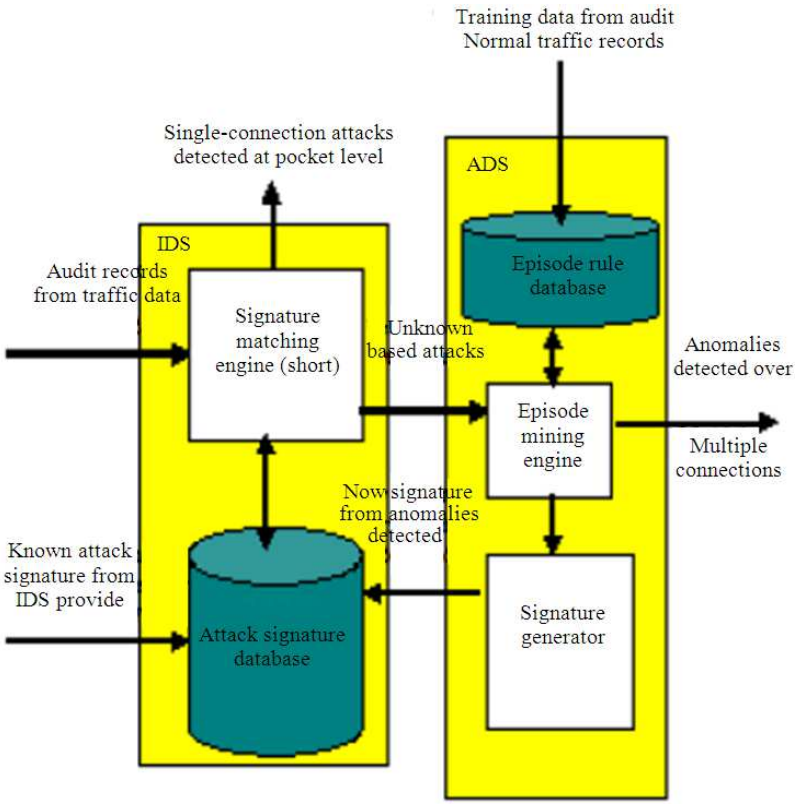

Fig. 2. Signature based detection agents and IDS

3. OUR PROPOSAL USING SIGNATURE BASED INTRUSION DETECTION SYSTEM

The sense of a word agent is an arrangement to act on one's behalf. In software rapports, agent is a program that performed for the user or some other program in association of agency. Thus an agent is accredited to sovereignty, authority and reactivity. The concept of an agent provides a suitable and influential way to describe a multifarious software entity that is proficient of acting with a certain degree of independence in order to accomplish tasks on behalf of its host (Pei *et al*., 2004). Components of Agent Figure depict the different modules of agent. Agent consists of two modules.

Frequent Attack Signature Database: In signature based intrusion detection method, we have a massive record of signatures. In order to check whether the received packet is an intruder or not, we have to match the signature of received packet against all the signatures in the database (Chandola *et al*., 2009). However it is a time unbearable process, as the database is large. To overcome this condition, we are using cache mechanism. We are going to maintain a cache of regularly happening intruder signature database. Balancing database clamps all the signatures.

Detection Module: Detection Module is main element of agent. Its main assignment is to detect intrusion. It works as follows. The detection Module grosses packet as input and removes its signature. This removed signature is then associated with all the signatures in cached database first, to check for intrusion. If any match arises then packet is marked as intruder packet. Resultant detection in short time. However if no match occurs then the removed signature is then related with all the signatures in balancing database. If match occurs then packet is intruder packet else packet is considered to be a usual packet. This module includes multi threading logic as above-mentioned.

4. IDS TECHNOLOGIES

There are many types of intrusion detection systems (William and Brown, 2013). They are separated into the following four groups founded on the type of proceedings that they observed and the ways in which they are positioned.

4.1. Host Intrusion Detection

Host intrusion detection references to the session of intrusion detection systems that occur on and observed an individual host machine (Gupta and Mamtora, 2012). More number of system features that a Host Intrusion Detection System (HIDS) used in assembling data including:

- File System-Variations to a host's file system can be revealing of the activities that are showed on that host. In particular, changes to delicate or seldom modified portions of the file system and unbalanced patterns of file system access can provide evidences in realizing attacks
- The **Fig. 3** shows the various components of agents, in this the attack in signature database is shown. The **Fig. 4** shows the distributed IDS
- Network Events-IDS can seize all network communications after they have been managed by the network stack before they are recognized on to user-level procedures. This methodology has the benefit of scrutinizing the information precisely as it will be understood by the expiration process, but it is significant to note that it will be useless in detecting attacks that are propelled by a user with admittance or attacks on the network heap itself
- System Calls-through some alteration of the host's kernel. IDS can be located in such a way as to observe all of the system calls that are made. This can deliver the IDS with very amusing data representative in the behavior of a program

A perilous decision in any HIDS is consequently selecting the suitable system features to observe. This conclusion includes an amount of trades containing the content of the data that is observed, the capacity of information that is netted and the possibility to which the IDS may adapt the operating system of the host machine.

4.2. Network Intrusion Detection

A Network Intrusion Detection System (NIDS) observed the packets that traverse a given network link. Such a system functions by insert the network interface into promiscuous mode. Affording the benefit of existence capable to observe a whole network although not revealing its presence to possible enemies. Since the packets that a NIDS is observing are not essentially addressed to the host NIDS exist on, the system is also in vulnerable to an complete class of attacks such as the "ping-of-death" attack that can inactivate a host deprived of ever generating a HIDS (More *et al*., 2012). A NIDS is perceptibly of slight charge in noticing attacks that are propelled on a host through a border other than the network. Network information has a diversity of features that are obtainable for a NIDS to observe.

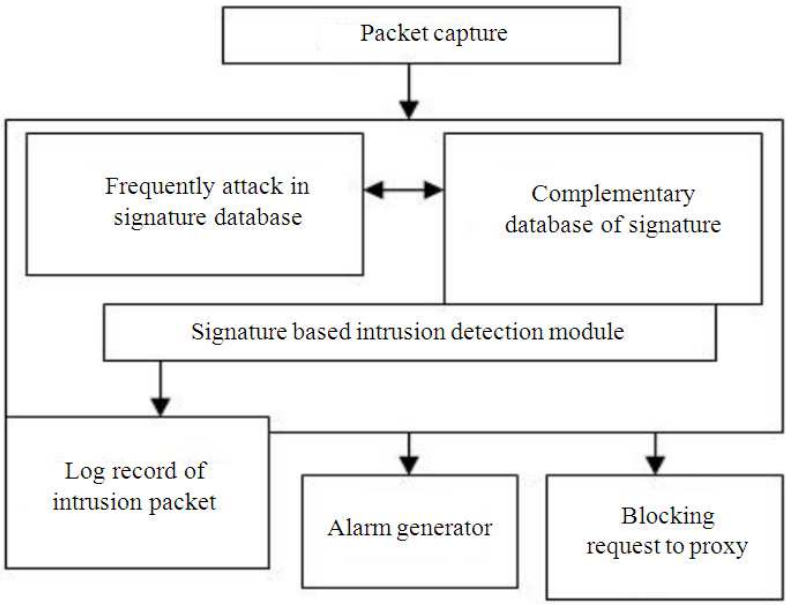

Fig. 3. Components of agents

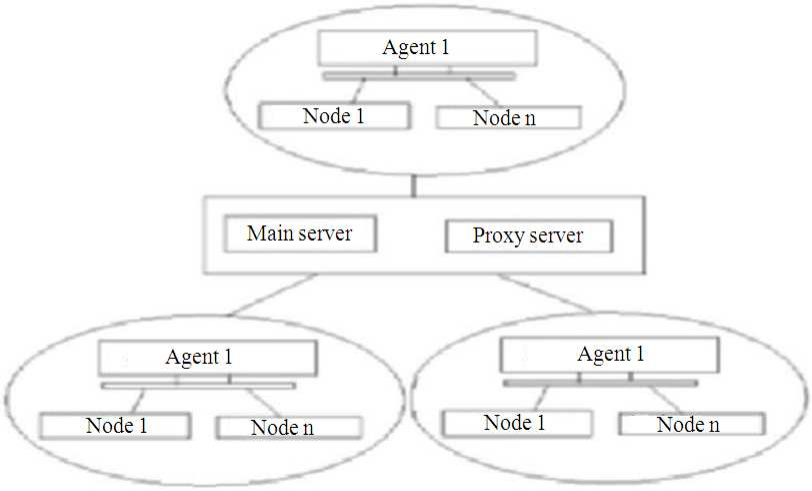

Fig. 4. Distributed IDS

Most operate by inspecting the IP and transport layer headers of specific packets, at ease of these packets, or certain mixture thereof. Regardless of which features a system selects to observe, however, the standing of a NIDS fundamentally offering amount of encounters to its accurate operation. Preceding a heterogeneous network, a NIDS generally does not retain familiar information of all of the hosts on the network and is incompetent of responsible how a host may construe packets with uncertain characteristics. Deprived of unambiguous information of a host system's protocol operation, a NIDS is powerless in influential how arrangement of packets will affect that host if different implementations understand the same order of packets in different ways. A knowledge assailant can feat this stuff by sending packets that are intended to complicate a NIDS. Such bouts are referred to as supplement (Handley *et al*., 2001). A delusion attack based on whether they insert

further information into a packet stream that a NIDS will see and the objective host will ignore or if they find by falsifying information in such a way that a NIDS cannot totally examine a packet stream. Protocol uncertainties can also present a difficulty to a NIDS in the procedure of crud. Crud appears in a network brook from a diversity of bases within accurate network implementations, faulty network links and network pathologies that have no connection to intrusion attempts. If a NIDS achieves inadequate analysis on a stream comprising crud, it can make false positives by erroneously recognizing this crud as being invasive. Although a NIDS therefore is in a very suitable position whereby it has complete admittance to all packets negotiating a network link. Its perceptiveness is challenged due to obscurities in network information and its limited standpoint of host system applications and network topology.

4.3. Wireless IDS

It observes wireless network traffic and examines its wireless networking protocols to recognize suspicious movement concerning the protocols themselves. It cannot recognize doubtful action in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is shifting. It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be positioned to where abouts where illegal wireless networking could be occurring (Nitin *et al*., 2012).

4.4. Network Behavior Analysis (NBA)

It surveys network traffic to recognize threats that produce infrequent traffic flows, such as Distributed Denial of Service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors) and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often installed to observed flows on an organization's interior networks and are also sometimes organized where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners networks).

5. FUTURE RESEARCH

The learning of intrusion detection systems is fairly new practical to many other areas of systems research and it stands to reason that this topic offers a number of occasions for future exploration. In discussing some of the problematic issues that oppose IDS designers, this study has touched upon a number of open questions related to intrusion detection including:

- Can anomaly detection systems be recycled to produce attack rules for misuse detection systems
- In what ways can differences of known attacks be detected by a misuse system without revealing the IDS to resource consuming attacks
- Can an anomaly system that adaptively adjusts its model of usual behavior over time be protected from being training by attackers to accept intrusions as usual behavior
- Is it possible for triage appliances to provide an IDS with the ability to shed load without diminishing its efficacy or its coverage
- How can the completeness, correctness and performance of intrusion detection systems are measured in order to facilitate relative comparison and absolute evaluation of these systems

In addition to these issues, there are a number of un-answered issues regarding the scope of analysis that a IDS performs and the interoperability of intrusion detection systems. Most intrusion detection efforts today focus on providing analysis for a relatively localized target: either a single host or a collection of hosts joined by a network. A system that operates with a more global scope may be capable of detecting distributed attacks or those that affect an entire enclave. Development of such a system would be a valuable contribution to the study of intrusion detection.

6. CONCLUSION

Since the study of intrusion detection began to gain momentum in the security community roughly ten years ago, a number of varied ideas have emerged for provoking this problem. Intrusion detection systems vary in the sources they use to obtain data and in the specific techniques they employ to analyze this data. Most systems today classify data either by misuse detection or anomaly detection: each approach has its relative merits and is accompanied by a set of limitations. It is likely not accurate to expect that an intrusion detection system be capable of correctly classifying every event that occurs on a given system. Seamless detection, like flawless security, is simply not an achievable goal, given the complexity and rapid evolution of modern systems. IDS can, however, strive to raise the bar for attackers by reducing the efficacy of large classes of attacks and increasing the work factor required to achieve a system compromise. The coordinated deployment of multiple intrusion detection systems promises to allow greater

confidence in the results of and to improve the coverage of intrusion detection, making this a critical component of any comprehensive security architecture. In future the random forest methodology is useful for identifying the intruders in WLAN and in the domain of cyber terrorism the intrusion detection planning major role to identify the malicious attacks and in the field of wireless sensor network can also have a scope to identify the malicious attacks.

7. REFERENCES

Ashoor, A.S. and S. Gore, 2011. Importance of Intrusion Detection System (IDS). Int. J. Sci. Eng. Res., 2: 1-4.

Chandola, V., A. Banerjee and V. Kumar, 2009. Anomaly detection: A survey. ACM Comput. Surveys. DOI: 10.1145/1541880.1541882

Chou, T.S., 2011. Development of an intrusion detection and prevention course project using virtualization technology. Int. J. Educ. Dev. Inform. Commun. Technol., 7: 46-55.

Dharmapurikar, S. and J.W. Lockwood, 2006. Fast and scalable pattern matching for network intrusion detection systems. IEEE J. Selected Areas Commun., 24: 1781-1792. DOI: 10.1109/JSAC.2006.877131

Gupta, S. and R. Mamtora, 2012. Intrusion detection system using wireshark. Int. J. Adv. Res. Comput. Sci. Soft. Eng., 2: 34-36.

Handley, M., V. Paxson and C. Kreibich, 2001. Network intrusion detection: Evasion, traffic normalization and end-to-end protocol semantics. Proceedings of the 10th Conference on USENIX Security Symposium, (USS' 01), USENIX Association Berkeley, CA, USA., pp: 9-9.

Hu, Z., 2009. Design of intrusion detection system based on a new pattern matching algorithm. Proceedings of the International Conference on Computer Engineering and Technology, Jan. 22-24, IEEE Xplore Press, Singapore, pp: 545-548. DOI: 10.1109/ICCET.2009.244

Montero-Melendez, T, J. Dalli and M. Perretti, 2013. Gene expression signature-based approach identifies a pro-resolving mechanism of action for histone deacetylase inhibitors. Cell Death Different, 20: 567-575. DOI: 10.1038/cdd.2012.154

More, S., M.L. Mathews, A. Joshi and T. Finin, 2012. A semantic approach to situational awareness for intrusion detection. Proceedings of the National Symposium on Moving Target Research, (MTR' 12), UMBC.

Narayana, M.S., B.V.V.S. Prasad, A. Srividhya and K.P.R. Reddy, 2011. Data mining machine learning techniques-a study on abnormal anomaly detection system. Int. J. Comput. Sci. Telecommun., 2: 8-14.

Nitin, T., S.R. Singh and P.G. Singh, 2012. Intrusion Detection and Prevention System (IDPS) Technology- Network Behavior Analysis System. ISCA J. Eng. Sci., 1: 51-56.

Pei, J., S.J. Upadhyaya, F. Farooq and V. Govindaraju, 2004. Data mining for intrusion detection: Techniques, applications and systems. Proceedings of the 20th International Conference on Data Engineering, Mar. 30-Apr. 2, IEEE Xplore Press, pp: 877-877. DOI: 10.1109/ICDE.2004.1320103

Scarfone, K.A. and P.M. Mell, 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology.

Uddin, M. and A.A. Rehman, 2010. Dynamic multi layer signature based intrusion detection system using mobile agents. Int. J. Netwo. Security Appli.

Wheeler, P.S., 2006. Techniques for improving the performance of signature-based network intrusion detection systems. MSc Thesis, University of California.

William, S. and L. Brown, 2011. Computer Security: Principles and Practice. 2st Edn., Pearson Education, Boston, ISBN-10: 0132775069, pp: 788.

Yu, Z., J.J.P. Tsai and T. Weigert, 2007. An automatically tuning intrusion detection system. IEEE Trans. Syst. Cybernetics-Part B: Cybernetics, 37: 373-384. DOI: 10.1109/TSMCB.2006.885306