Review Form: 1st International Workshop on
Services and Infrastructure for the Ubiquitous and Mobile Internet (SIUMI'05)

SIUMI 2005

WEB MINDS

Columbus, Ohio, USA, June 6th, 2005

In conjunction with the 25th Int. Conference on Distributed Computing Systems (**ICDCS'05**)

Paper Number: 2
Paper Title: A wawelet based ID model
Authors: Liu Lan

Reviewer1:

Familiarity Rate your familiarity with the topic	1 Novice	**2X** Some knowledge	3 **Familiar**	4 Expert	
Significance Technical relevance and practicality of ideas in the paper	1 Not significant	**2X** **Somewhat significant**	3 Highly significant		
Novelty How original the problem and/or solution method is	1 Not novel	**2X** **Somewhat novel**	3 Highly novel		
Quality of Presentation Writing and presentation style/accuracy	1 **Poorly written**	**2X** Could be improved	3 Well written		
Overall Recommendation	1 Strong reject	2 **Weak reject**	**3X** Weak accept	4 Accept	5 Strong accept

Contributions

First of all I must say I am not an expert neither in (distributed) Intrusion Detection System nor in wavelet transforms, so that I might not be able to identify the degree of originality and novelty of the approach.
However, for what I understood from the paper, the proposed approach appears to be well motivated and reasonable to tackle the problem. To a non-expert like myself the proposed approach appears to be interesting and worthwhile studying.

Strengths and weaknesses

The major strengths seems to be the good performance of wavelet transforms in identifying abnormal behaviour out of large logs.

A possible weakness that came to my mind (as I am not an expert in the field) is the difficulty of making sure that what is supposed to be the "normal" behavior against which the current behavior is compared in order to detect anomalies, is really "normal". Is it possible to make sure that a log of a complex situation does not contain security attacks? If not, the presence of the attack would be considered normal, and that type of attack would never be noticed.

Detailed public comments
First of all, the English must be improved in order to guarantee a higher level of readability. In the current draft the presence of many typos and syntactical mistakes seriously affects the readability.

For what concerns the technique proposed in the paper, I must say that I am not an expert neither on ID nor on wavelets, so that I could fully evaluate and appreciate the novelty of the approach and the quality of the results shown. However the results look sufficiently interesting to me to possibly warrant publication.

The only doubt I have is related to the use of large log files as a prototype for "normal behavior". Is it possible to make sure that a huge log of a complex situation does not contain security attacks? If not, the presence of the attack would be considered normal, and that type of attack would never be noticed, even by the proposed wavelet approach. I would suggest that the authors commented on this point in the final version, as I think this is a crucial point for practical application of the proposed technique.

Reviewer2:

Familiarity Rate your familiarity with the topic	1	2	**3X**	4	
	Novice	Some knowledge	**Familiar**	Expert	
Significance Technical relevance and practicality of ideas in the paper	1	**2X**	3		
	Not significant	**Somewhat significant**	Highly significant		
Novelty How original the problem and/or solution method is	1	**2X**	3		
	Not novel	**Somewhat novel**	Highly novel		
Quality of Presentation Writing and presentation style/accuracy	**1X**	2	3		
	Poorly written	Could be improved	Well written		
Overall Recommendation	1	**2X**	3	4	5
	Strong reject	**Weak reject**	Weak accept	Accept	Strong accept

Contributions
This paper proposes a distributed model for analyzing network traffic and finding DOS attacks. The model is based on wavelet techniques.
The topic is important, but the novelty is limited because other researchers have previously proposed the use of these techniques for analyzing network traffic. The authors claim that their proposal improves previous techniques, but no demonstration is provided in the paper.

Strengths and weaknesses
The experimental part with real data is appreciable, but there is no comparison with other techniques, hence it is impossible to appreciate the real quality of the proposal. Moreover, this paper does not consider the major issue of network traffic analyses that is, the huge amount of data that should be evaluated in real-time.
The subject of this paper is far from the topics of the SIUMI workshop.

Detailed public comments
The topic is important, but not related with the topics of the workshop.

The use of wavelet techniques is appreciable but not so new. There is no evaluation about the computational and storage complexity. It seems that the solution to address these issues is to choose a five minutes interval, that is typically considered too large for detecting network attacks in time.

The last part of the experiment is rather unclear. From the text, it seems that a flash crowd is considered similar to an attack. It is generally true that at the beginning a DoS attack resembles a flash crowd, but the quality of the traffic analyzers is evaluated on the capacity of distinguishing the origin of the sudden peaks.
For major details, see “Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites”, Jung and Krishnamurthy and Rabinovich, Proceedings of WWW 2002.

The presentation should be improved. There are many typos and grammar errors. The initial part contains a too long survey that prevents a detailed description about the pros and cons of the proposed technique and comparisons with at least another method.