

# Denial of Service Prevention through Logical Fibering

Marvin Oliver Schneider and Jacques Calmet

University of Karlsruhe (TH),  
Institute IAKS, Am Fasanengarten 5  
76131 Karlsruhe, Germany  
{marvin, calmet}@ira.uka.de

**Abstract.** We propose a logic-based method to protect network nodes or web sites from Denial of Service (DoS) attacks. This method is based upon Logical Fibering. Queries to the node are stored inside the fiber and decisions whether a new query should be accepted or not are taken on an empirical basis. The respective base space consists of the incoming information whereas the fiber itself describes the universe of necessary values to treat the connection. At the end of the query processing a result of *true* or *false* for every request is reached. Apart from this specific process, a mediation scheme is initiated automatically by means of Data Mining methods. This enables to optimize the Logical Fibering structure and to assess possible similarities among attacks. The resulting information could be used by network or web managers to analyze the DoS threats to their system. This paper proposes an overview of the methodology being designed.

Keywords: *Denial of Service, Logical Fibering, Web Access Management, Data Mining, Firewalls*

## 1. Introduction

We propose a logic-based method to protect network nodes or web sites from Denial of Service (DoS) attacks and from distributed DoSs as well. This method is based upon Logical Fibering. Queries to the node are stored inside the fiber and decisions whether a new query should be processed or not are taken on an empirical basis.

The resulting system can be installed either on the incoming or the outgoing side of a network or on both. Its implementation will be performed first on a simple Personal Computer as a form of a personal firewall and will then be extended to servers and routing equipments as “attached logic”. Thus, the resulting top-down architecture is following a classic methodology whereas the treatment of information is highly different from those available in commercial firewalls (Cheswick et al, 2005).

A first motivation to use Logical Fibering lies in Günther’s philosophy (Pfalzgraf, 2004; Pfalzgraf and Edtmayr, 2004), which states that the world is made up of an infinite number of “*loci*” (*true / false* value) at different ontological places. All sorts of processes may thus be described with this method, which included the problem of DoS. Apart from this merely descriptive function, the principles of Logical Fibering, which evolves from Günther’s Polycontextural Logic (PCL) (Pfalzgraf, 2004 and references therein) provide a framework to analyze and reach decisions for a given problem. It provides thus a simple, yet powerful, tool against DoSs. Besides the PCL origin that was introduced as a philosophical tool, Logical Fibering is linked to the concepts of fiber, bundle and jet in mathematics. A fiber is a collection of vector spaces. This

collection is finitely enumerable, which is a crucial property for our purposes since the number of queries we may store is only limited by hardware characteristics such as memory capacity. In our model we consider a basic and unique sort of fiber where vector spaces are replaced by two-valued logics. Thus, the mathematical methodology is almost trivial.

## 2. Architecture

The logical fibering employed in the system consists of a base space  $B$  with a collection of incoming connections. These connections are typically labeled by their IP-address, but not fully since forged data might bring about many different forms of entries. In any case, this approach seeks to use an enumeration by labeling rather than by numbering as it is a more natural form to deal with incoming data and eases up programming. The space of all fibers  $E$  to which  $B$  is connected via the projection map  $\pi$  contains primarily the global *true* and *false* values, which will be interconnected by a mediation scheme. But, then each fiber is itself fibered and thus offers a second level subsystem with local logic (figure 1).

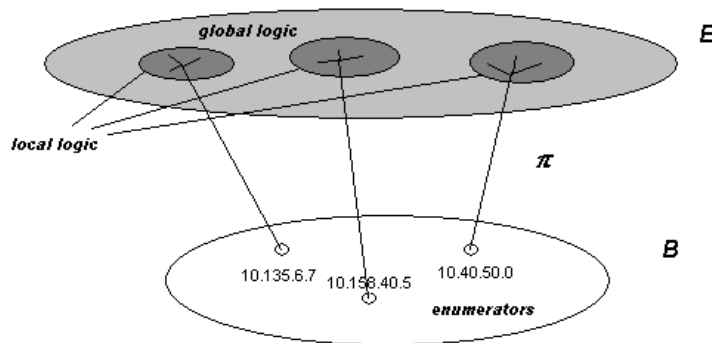


Figure 1: Logical Fibering structure

As soon as a new connection is monitored, the received data is stored in a newly created fiber. At first, this fiber does not show any logical connection with the others fibers nor does it itself have anything but any relevant data that the system can access during the initial processing of the queries. Over time, more characteristics can be observed. This can be done in a simple way, e.g. trying to link bandwidth consumption with a specific fiber or in a more complex way e.g. reporting that a number of connections in a certain order over a period of time have a specific impact on the available memory and which action is to be taken to optimize the processing. The fibering must thus be optimized through intelligent learning algorithms. In an ideal case, little or no manual interference is given, i.e., the system is fully automated. The outcome of all this logic is simple: it is to decide, whether and when to block a connection. It is thus not mandatory in case of attacks to block the whole system. Most of the time the queries will be accepted but not immediately processed. As a result, the effects of fake IP-addresses will be mitigated as someone actually using an address appearing in previous attacks might be able to get through, depending on the access char-

acteristics. The main benefit and goal is to prevent the collapse of the system in case it is flooded with numerous queries, a characteristic of many DoSs.

The management of the system's information is performed through a relational database (see the architecture overview in figure 2) with basic SQL-like commands, thus enabling users to easily browse data and – if necessary – make adjustments. This system architecture was also chosen because it enables administrators to visualize graphically reports on the status of the processing.

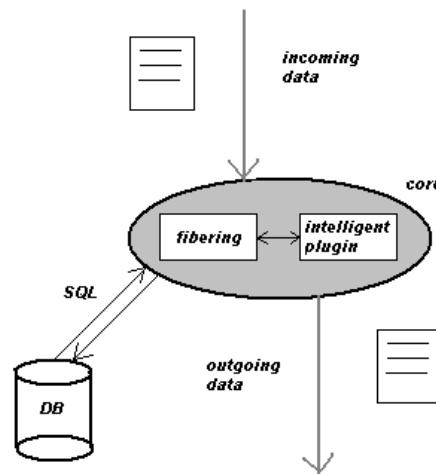


Figure 2: System architecture overview

### 3. Special Features

Due to the fibered fibering (one fibering encapsulated in the other) local and global conclusions can be made about threats. This is a special feature that approaches threats in suitable and practical manner, e.g. a SYN-attack (Ferguson and Senie, 1998) is isolated and concentrated on one IP address, which the system can easily find and block. On the other hand DDoS attacks require global thinking and conclusions as the most varied IP-information will arrive at once and will urge for quick global action in order to eliminate the problems (McClure, 2003; Lau et al, 2000).

Our main goal is to prevent DoS threats. A second one is to identify the sources of such attacks. In this respect Data Mining is an adequate tool to be used. A possibly feasible approach is to implement a classification rule engine among several possibilities (Witten and Frank, 2000). Logical Fibering enables to design a mediation scheme from which to extract relevant information on attackers.

An example of a mediation scheme between three *loci* ( $i=3$ ) is demonstrated in figure 3. The scheme of the left side of figure 3 shows the interconnection of *true* / *false* values and the right side depicts the orderings. Transitions from one system to the other occur in a vertical axis while corresponding pairs in one system are given in a horizontal axis. The symbol  $\supset\text{---}\subset$  expresses the transition from a *true* to a *false* value or vice versa.

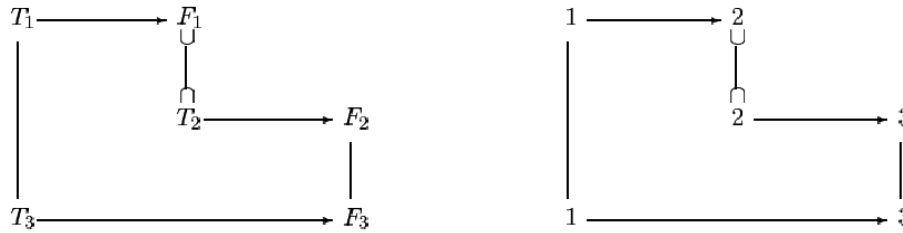


Figure 3: Example of a mediation scheme

The above scheme may be also expressed in the form of equivalences:

$$T_1 \equiv T_3 \quad F_1 \equiv T_2 \quad F_2 \equiv F_3$$

#### 4. Examples of Processing

In case of a SYN-attack an example may be processed as follows: From a given IP a connection shall be established. The fiber does not yet exist (neither examining the IP-address, nor the characteristics), therefore a new fiber is created and stored in the fibering. It shall contain the IP-address (enumerator) as well as several other characteristics (fiber) in order to define the scope of the connection in the most complete possible way. A flag is maintained to define whether the connection is “established”, “to be established” or “inactive”. In the case of a first connection, it shall be marked as “in process”. Now, after a very short period of time, a new SYN packet might be sent by the attacker. The incoming information is compared with the stored fibers. The previous fiber is found not only because of its known IP-address, but also because of its general characteristics. Now the system may take action, firstly dropping the two faulty connect attempts and secondly marking the fiber as a “SYN-attack” fiber, so that anything from the same source is dropped directly. This is similar to spasm filtering at first sight. However, since we store more than an IP address we ought to be able to refine the filtering algorithm. Supposing that a connect attempt is made from a machine with the same IP-address as the one used in the attack, but with different overall characteristics, the system may treat this request in a different manner, actually modifying the logical system of the fiber to store the legal access as well and differentiate between the two.

In case of a DDoS attack, packets will come in from many different sources at the same time. IP-addresses will be clearly different. For simplicity’s sake a DDoS attack of only three agents (IPs: 10.135.152.12, 254.122.156.523, 52.251.128.161) is assumed. The first agent (10.135.152.12) attacks. The information is stored in a new fiber – just as in the case above. The second agent (254.122.156.523) sends a packet, the information is also stored. It is now assumed, that a serious bandwidth problem occurred after the connection of the third agent (52.251.128.161). The system detects this sudden problem situation and executes an analysis on the data of all active connections and how they were established over time. Furthermore, this analysis will not work only upon IP, but also on similar general characteristics. In this way a global scope of DoS-attack may be detected and the respective links dropped. All concluded information is stored in the logical structure of the fibering, so that future attempts may be detected faster.

## 5. Conclusions

The format of the paper does not allow to survey the various methods and techniques that are used to prevent DoS or DDoS threats. The logical fiberings based method that we propose aims at replacing all of them. A first result of the paper is to propose a theoretical model where only empirical models do exist. The current state of development of this project does demonstrate that we have a promising approach to the problem of Denial of Service prevention.

The two main features of the overall methodology are that we have a logical content and a Data Mining content. The latter is in fact tightly linked to the former. The fiberings system will be indeed combined with Data Mining routines and other intelligent algorithms. A standard database shall ensure the readability of results and the possibility of the development of additional reports. An advantage arising from combining Data Mining to Logical Fiberings is to gather information on how attacks do work and how they should be prevented (Witten and Frank, 2000; Lee and Stolfo, 1998).

As for any system involving AI methods, it is to be expected that performance will be one of the main problem issues to be treated. Our approach is not in line with the rather simple techniques that are currently on the market, but offers a relatively complete framework to deal with the problem of DoS as a whole. Also, since we work with trivial fiberings we may expect to be able to control the complexity of the approach.

## 6. References

- Cheswick, W.R., Bellovin, S.M., Rubin, A.D. (2005); *Firewalls and Internet Security: Repelling the Wily Hacker*; 2<sup>nd</sup> ed., Pearson Education
- Ferguson, P., Senie, D. (1998); *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*; <http://rfc2267.x42.com/>, Natick/USA
- Lau, F., Rubin, S.H., Smith, M.H., Trajovic, L. (2000); *Distributed denial of service attacks*; IEEE International Conference on Systems, Man, and Cybernetics, Nashville/USA (pp. 2275-2280)
- Lee, W., Stolfo, S.J. (1998); *Data mining approaches for intrusion detection*; Proceedings of the 7th USENIX Security Symposium
- McClure, S., Scambray, J., Kurtz, G. (2005); *Hackers Exposed – Network Security Secrets & Solutions*; 5<sup>th</sup> ed., McGraw-Hill
- Pfalzgraf, J. (2004); *On Logical Fiberings and Automated Deduction in Many-valued Logics Using Gröbner Bases*; *Revista Real Academia de Ciencias, Serie A de Matemáticas (RACSAM)*, Vol. 98 (1)
- Pfalzgraf, J., Edtmayr, J. (2004); *The concept of Logical Fiberings: distributed logics for multi-agent systems*; Proceedings 17th European Meeting on Cybernetics and Systems Research (EMCSR'2004), Vienna
- Witten, I.H., Frank, E. (2001); *Data Mining – Practical Machine Learning Tools and Techniques with Java Implementations*; Morgan Kaufmann Publishers