On using Constraints for Network Intrusion Detection

Pedro Salgueiro and Salvador Abreu

Departamento de Informática, Universidade de Évora
and CENTRIA FCT/UNL, Portugal
`{pds,spa}@di.uevora.pt`

Abstract. In this work we present a domain specific language for network intrusion detection that allows to describe network intrusions composed by several network packets, using a declarative approach to describe the desirable network situations, and based on that description, a set of parameterizations for network intrusion detection mechanisms based on Constraint Programming(CP) will execute to find those intrusions.

Keywords: Constraint Programming, Intrusion Detection Systems, Domain Specific Languages

Resumo Neste trabalho apresentamos uma linguagem específica de domínio para descrever intrusões de rede, capaz de descrever ataques compostos por vários pacotes de rede, e a partir de uma descrição declarativa da intrusão, criar um conjunto de ferramentas capaz de detectar a intrusão desejada, tendo como base a Programação por Restrições(CP).

Palavras Chave: Programação por restrições, Sistemas de detecção de Intrusões, Linguagens Específicas de Domínio

1 Introduction

Computer networks are composed of numerous complex and heterogeneous systems, hosts and services. Maintaining the security of the networks is crucial to keep the users data safe, which may be accomplished by an Intrusion Detection System (IDS) e.g. `Snort` [1,2]

To maintain the quality and integrity of the services provided by a computer network, some aspects must be verified in order to maintain the security of the users data. The description of those conditions, together with a verification that they are met can be seen as an Intrusion Detection task. These conditions, specified in terms of properties of parts of the (observed) network traffic, will amount to a specification of a desired or an unwanted state of the network, such as that brought about by a system intrusion or another form of malicious access.

Those conditions can naturally be described using a declarative programming approach, such as Constraint Programming [3] or Constraint Based Local Search Programming (CBLS) [4], enabling the description of these situations in a declarative and expressive way. To help the description of those network situations, we created NeMODe, a Domain Specific Language (DSL) [5], which enables an easy description of intrusion signatures that spread across several network packets, which will then translate the *program* into constraints that will be solved by more than one constraint solving techniques, including Constraint Based Local Search and Propagation-based systems such as Gecode [6]. It will also have the capabilities of running several solvers in parallel, in order to benefit from the earliest possible solution.

Throughout this paper, we mention technical terms pertaining to TCP/IP and UDP/IP network packets, such as *packet flags, ACK, SYN, RST, acknowledgment, source port, destination port, source address, destination address, payload*, which are described in [7].

1.1 Intrusion Detection Systems

Intrusion Detection Systems(IDS) play an important role in computer network security, which focus on traffic monitoring trying to inspect traffic to look for anomalies or undesirable communications in order to keep the network a safe place. There are two major methods to detect intrusions in computer networks; 1) based on the network intrusion signatures, and 2) based on the detection of anomalies on the network [8]. In this work, we adopted an approach based on signatures.

Snort is a widely used Intrusion Detection System that relies on pattern-matching techniques to detect the network attacks [9]. Snort is a very efficient Intrusion Detection System but is primarily designed to detect network attacks which have a signature that can be identified in a single network packet. Although it provides some basic mechanisms to write rules that spread across several network packets, the relations between those network packets are very simple and limited, such as the `Stream4` and `Flow` pre-processor.

Most of the recent work in intrusion detection systems has been focused on the performance [10], but there has been also some work [10,11] that focus on the method used to match the network packet signatures and the type of signatures that can be detected, using alternative search methods that allows the search of signatures that spreads across several packets, which is one of the limitations of Snort and most other intrusion detection systems.

1.2 Constraint Programming

Constraint Programming (CP) is a declarative programming paradigm which consists in the formulation of a solution to a problem as a *Constraint Satisfaction Problem* (CSP) [3], in which a number of variables are introduced, with well-specified domains and which describe the state of the system. A set of relations, called *constraints*, is then imposed on the variables which make up the problem. These constraints are understood to have to hold true for a particular set of bindings for the variables, resulting in a *solution* to the CSP.

Adaptive Search Adaptive Search (AS) [12] is a Constraint Based Local Search [4] algorithm, taking into account the structure of the problem and using variable-based information to design general heuristics which help solve the problem. AS has an adaptive memory similar to TabuSearch [13] in order to prevent stagnation while solving the problem. The solving method of AS relies on iterative repairs based on variable and constraint error information that seeks to reduce errors on the used variables, in order to reach a valid solution, i.e. a solution with error value of zero. Adaptive Search has recently been ported to Cell/BE, presented in [14].

Gecode Gecode [15] is a constraint solver library implemented in C++, designed to be interfaced with other systems or programming languages. Gecode is a Propagation-based [3] constraint solver system, involving variables ranging over some finite set of integers to solve the problems, being described by stating constraints over each variable of the problem, which states the allowed values for each variable , then, the constraint solver propagates all the constraints and reduce the domain of each network variables in order to satisfy all the constraints and instantiate the variables with valid values, thus reaching a solution to the initial problem.

2 Network Monitoring with Constraints

Our approach to intrusion detection relies on being able to describe the desired signatures through the use of constraints and then identify the set of packets that match the target network situation in the network traffic window, which is a log of the network traffic in a given time interval.

The problem needs to be modeled as a Constraint Satisfaction Problem (CSP) in order to use the constraint programming mechanisms. Such a CSP will be composed by a set of variables, V, representing the network packets, their associated domains, D, and a set of constraints, C that relates the variables in order to describe the network situation. On such a CSP, each network packet variable is a tuple of integer variables, 19 for TCP/IP [1] packets and 12 for UDP packets [2], which represent the significant fields of a network packet necessary to model the intrusion signatures that we have used in our experiments, such as the timestamp, source/destination addresses, source/destination ports and packet data, which are used in both TCP and UDP packets, the extra TCP flags and packet sequence number fields are used with TCP packets. The number of fields may increase over time with the evolution of the work and the use of more complex intrusions. The domain of the network packet variables, D, are the values actually seen on the network traffic window, which is a set of tuples of 19 integer values, each tuple representing a network packet actually observed on the traffic

[1] Here, we are only considering the "interesting" fields in TCP/IP packets, from an IDS point-of-view.

[2] Here, we are only considering the "interesting" fields in UDP packets, from an IDS point-of-view.

window and each integer value represents the fields that are relevant to network monitoring. The packets payload is stored separately in an array containing the payload of all packets seen on the traffic window. A solution to such a CSP, if it exists, is the set of packets that correspond to the network intrusion described by the CSP. Listing 1 shows a representation of such CSP, where P represents a set of network packet variables, D, a set of network packets representing the network traffic window, DP the payloads of all packets and $\forall P_i \in P \Rightarrow P_i \in D$ the associated domains of each variable. The payload of packet i would be $DP[i]$. Performing Network Monitoring with constraints is explained in more detail on the work presented in [16].

Listing 1 Representation of a network CSP

$$P = \{(P_{1,1}, \dots, P_{1,19}), \dots, (P_{n,1}, \dots, P_{n,19})\}$$
$$D = \{(V_{1,1}, \dots, V_{1,19}), \dots, (V_{m,1}, \dots, V_{m,19})\}$$
$$DP = \{DP_1, \dots, DP_m\}$$
$$\forall P_i \in P \Rightarrow P_i \in D$$

3 NeMODe - A DSL to describe network signatures

In this work we present a simple, declarative, intuitive domain-specific programming language for the Network Intrusion Detection [5] domain called NeMODe. NeMODe language talks about network entities, network entity properties and relations between network entities and network entity properties, which allows to describe network intrusion signatures, and with base on those description, generate Intrusion Detection mechanisms. A more complete description of this DSL as well as other examples are presented in [16], which is an extended description of the work described in this paper.

The key characteristic of NeMODe is to ease the way how network attack signatures are described using constraint programming, hiding from the user all the constraint programing aspects and complexity of modeling network signatures in a Constraint Satisfaction Problem(CSP), but still using the methodologies of CP to describe the problem at a much higher level, describing how the network entities should relate among each other and what properties they should verify. Maintaining the declaritivity and expressiveness of the CP allows an easy and intuitive way of describing the network attack signatures, by describing the properties that must or must not be seen on the individual network packets, as well as the relationships that should or should not exist between each of the network packets.

NeMODe is a front-end to several back-ends, one to each intrusion detection mechanism, allowing to generate several detection mechanisms from a single description. Having a single specification to several constraint solvers allows the search of a solution using different methods of search, allowing to run each of those methods in parallel, which allows to obtain different results from each solver. Depending on the characteristics of the problem, some solvers could produce a better and faster solution that others, allowing to choose the first solution to be produced.

NeMODe presents five groups of *statements*: (1) the primitives of the language, (2) the connectives, (3) definitions, (4) the use of such definitions and (5) macro statements. The primitives are the basic statements of the language, which state simple properties that each network variable should verify. The connectives are statements that relate two or more network variables, forcing them to verify some relations. The definition is a simple way of storing primitives or connectives under a variable to be used later. The *use* of definitions, forces a previous definition to used. Finally, the macro statements, are helpers that avoid unnecessary code repetition and ease the description of the signature.

The following list presents the set of primitives (*predicates*) available in the current implementation of NeMODe which allows to state properties of network packets that should be verified.

– Force a variable to be a network packet.
– Force a variable to be a TCP or UDP packet.
– Force a packet to have specific a TCP flag set.
– Force a packet not to acknowledge any packet.
– Force a packet to contain a string.

Follows a list of the *connective* statements, which are used to relate several network entities.

– Force a packet to acknowledge other packet.
– Restrict the temporal distance between packets.
– Force two packets to be related.
– Force the source/destination port of a packet.
– Force the source/destination address of a packet.
– Force two packet to contain the same piece of data in a given position and size on their payload.

NeMODe provides a special type of statements to help users specify network signatures with minimum work, the ***definition*** statements. These statements allows to store a set of properties over a set of network entities and give it a name and using them later on the program. Listing 2 shows an example of a simple ***definition*** where some properties over two network packets are stated, in this particular case, the variable `A` should be a TCP/IP packet, and have its `syn` flag set. These set of properties are *stored* in variable `C`, which can later be used. Those definitions by them self don't have any effect, they are only applied when used or referred. In order to use those definitions, simply refer the variable to which the set of properties was assigned or use it in a `macro` statement, explained next.

The `macro` statements provide mechanisms to help the user describe the situation, by avoiding unnecessary code repetition. This `macro` statements can

Listing 2 Example of a definition

```
C = { packet(A),
      tcp(A), syn(A) }
```

Listing 3 Example of `macro function`

```
C = { packet(A), syn(A) },
R:=repeat(3,C),
max_duration(R) < secs(60)
```

be used to repeat a set of properties assigned to a variable, and give a name to that repetition, allowing future references to each property of each instance of the repetition i.e. `R:=repeat(3,C)`. Other type of `macro` statements are the ones that are applied to the repetitions *stored* in a variable, such as state the maximum or minimum allowable time interval between each instance of the repetition, i.e. `max_duration(R) < secs(60)` or the maximum/minimum overall interval time that a repetition can take, i.e. `max_interval(R) < secs(60)`. Listing 3 illustrates a simple use of this macro functions.

Listing 4 Accessing a variable

```
1:     C = { packet(A), syn(A)},
2:     R := repeat(3,C),
3:     nak(R[1]:A)
```

When using the `repeat` statement, as in line 2 of Listing 4, each instance of the repetition as well as its variables keeps accessible, referring it as the *nth* instance and then referring the variables name, i.e. `R[1]:A`. Listing 4 shows an example, where the statement `nak` is applied to variable `A` of the first instance of the repetition `R`.

3.1 Available back-ends

NeMODe provides two back-end detection mechanisms; (1) based on the Gecode constraint solver and (2) based on the Adaptive Search algorithm.

Each of these detection mechanisms are based on Constraint Programming techniques, but they are completely different in the way they perform the detection, and also the way the signatures are described. In Sec. 1.2 each of these approaches are explained.

3.2 Examples

So far, we have worked with some simple network intrusion signatures: (1) a DHCP spoofing, (2) a DNS spoofing and (3) a SYN flood attack. All of these intrusion patterns can be described using NeMODe and the generated code was successful in finding the desired situations in the network traffic logs. A Portscan attack and an SSH Password brute-force attack are further explained in [16].

DHCP spoofing DHCP Spoofing is a Man in The Middle(MITM) attack, where the attacker tries to reply to a DHCP request faster than the legit DHCP server of the local network, allowing the attacker to provide false network configurations to the target host, such as the default gateway, forcing all traffic from/to the target to pass though an attacker controlled machine, allowing it to capture or modify the important data. This kind of intrusion can be detected by looking for several answers to a single DHCP request, originated in different machines. If this situation is found in the traffic of some network, there is a great probability that someone is performing this kind of attack. A NeMODe program to model a DHCP spoofing is shown in Listing 5. Lines 2 and 3 describes the packet that initiates a requests a DHCP, lines 5 and 6 the first reply to the request and lines 8 and 9 the second reply the DHCP request. Finally, on line 11 is stated that packets `B` and `C`(the first and second reply) should have different source addresses.

Listing 5 A DHCP Spoofing attack programmed in NeMODe

```
1:  dhcp_spoofing {
2:      packet(A), udp(A),
3:      dst_port(A)==67,
4:
5:      packet(B), udp(B),
6:      dst_port(B)==68,
7:
8:      packet(C), udp(C),
9       dst_port(C)==68,
10:
11:     src(B) != src(C)
12: } => {
13:     alert('DHCP Spoofing attempt')
14: };
```

DNS spoofing DNS Spoofing is also a Man in The Middle (MITM) attack. In this attack, the attacker tries to provide a false DNS query posted by the victim, if succeeded the victim could access a machine under the control of the attacker, thinking that it is accessing the legit machine, allowing the attacker to obtain crucial data from the victim. In order to arrange this attack, the attacker tries to respond with a false DNS query faster than the legit DNS server, providing a false IP address to the name that the victim was looking for. This kind of attacks is possible to detect by looking for several replies to the same DNS query. Listing 6 shows how this attack can be programmed using NeMODe. Line 2 and 3 describes the packet that makes the DNS request. Lines 5-8, describes a first reply to the DNS request and lines 10-13 describes the second reply. Lines 15-17 states that packets `B` and `C` should be different and that the *DNS id* of the replies should be the equal to the DNS request, which is the first two bytes of the packets data.

Listing 6 A DNS Spoofing attack programmed in NeMODe

```
dns_spoofing {
    packet(A), udp(A),
    dst_port(A)==53,

    packet(B), udp(B),
    dst(B)==src(A),
    src_port(B)==53,
    dst_port(B)==src_port(A),

    packet(C), udp(C),
    dst(C) == src(A),
    src_port(C) == 53,
    dst_port(C) == src_port(A),

    B != C,
    data(B,0,2) == data(A,0,2),
    data(C,0,2) == data(A,0,2)
} => {
  alert('DNS Spoofing attempt')
};
```

SYN flood attack A SYN flood attack happens when the attacker initiates more TCP/IP connections than the server can handle and then ignoring the replies from the server, forcing the server to have a large number of half open connections in standby, which leads the service to stop when this number reach the limit of number of connections. This attack can be detected if a large number of connections is made from a single machine to other in a very short time interval. Listing 7 shows how a SYN flood attack can be described using NeMODe. Line 2-5 describes a TCP/IP packet with the SYN flag and assigns those properties to variable `C`. In line 7, the *macro* statement *repeat* is used to repeat the properties of definition `C` 30 times, and assign it to variable `R`. Line 8 states that the time interval between each repetition of C should be less than to 500 micro-seconds.

Listing 7 A SYN flood attack programmed with NeMODe

```
1:  syn_flood {
2:    C = {
3:          packet(A), tcp(A),
4:          syn(A), nak(A)
5:    },
6:
7:    R := repeat(30,C),
8:    max_interval(R) < usecs(500)
9: } => {
10:   alert('SYN flood attack attempt')
11: };
```

3.3 Code Generation

The current implementation of NeMODe is able to generate code for the Gecode solver and for the Adaptive Search algorithm. These two approaches to constraint solving are completely different as well as the description of the problems, forcing us to have several code generators for each of back-end available. We were able to minimize this difference by creating custom libraries for each constraint solver so that the code generation process is not completely different for each back-end.

Generating an A.S. program The task of generating Adaptive Search resumes to create the proper error functions so that Adaptive Search be able to solve the problem; the `cost_of_solution` and `cost_on_variable`. To ease the generation of this functions, a small library was created which implements small error functions, specific to the network intrusion detection domain, which are then used to generate the code for the error functions.

Generating a Gecode program This goal is achieved by generating code based on Gecode constraint propagators that describe the desired network signatures. We created a custom library that defines functions that combine several stock Gecode constraints to define custom, network related "macro" constraints. The same library includes definitions for a few network-related constraint propagators, useful to implement some of the constraints needed to describe and solve IDS problems.

4 Experimental Results

While developing this work, several experiments were done. We have tested the examples of Sect. 3.2, a DHCP Spoofing attack, a DNS Spoofing attack and a SYN flood attack. All these network intrusions were successfully described using NeMODe and valid Gecode and Adaptive Search code were produced for all network signatures. The code generated by NeMODe was then executed in order to validate the code and ensure that it could indeed find the desired network intrusions.

The code generated for Gecode was run on a dedicated computer, an HP Proliant DL380 G4 with two Intel(R) Xeon(TM) CPU 3.40GHz and with 4 GB of memory, running Debian GNU/Linux 4.0 with Linux kernel version 2.6.18-5. As for the Adaptive Search code, it run on an IBM BladeCenter H equipped with QS21 dual-Cell/BE blades, each with two 3.2 GHz processors, 2GB of RAM, running RHEL Server release 5.2.

The reason to run both detection mechanisms in different machines with a completely different architecture is because Adaptive Search has recently been ported to Cell/BE, and we choose this version of Adaptive Search to run our experiments, forcing us to use the QS21 dual-Cell/BE blades, which is incompatible with the implementation of Gecode, forcing us to use a machine with x86 architecture to run Gecode.

Table 1. Average time(in seconds) necessary to detect the intrusions using Gecode and Adaptive Search

Intrusion to detect	Gecode (seconds)	A.S (seconds)
DHCP Spoofing	0.0082	0.3924
DNS Spoofing	0.0069	0.3512
SYN flood	0.0566	0.0466

In all the experiments we used log files representing network traffic which contains the desired signatures to be detected. These log files were created with the help of `tcpdump` [17], which is a packet sniffer, during an actual attack to a computer, which was induced to simulate the real attacks described in this work.

DHCP spoofing and DNS spoofing attacks For the DHCP spoofing and DNS spoofing attack, we used tcpdump to capture a log file, composed of 400 network packets, while a computer was under an actual attack. We used Ettercap to perform the DHCP spoofing and DNS spoofing attacks. The attack was programmed in NeMODe, which successfully generated code for Adaptive Search as well as for Gecode and successfully detected the intrusions.

SYN flood attack In the SYN flood attack a log file of 100 network packets was created with the help of tcpdump while a computer was under a SYN flood attack. The attack was programmed in NeMODe which in turn generated code for Adaptive Search and Gecode. This code was then used to successfully detect the intrusion.

4.1 Results

Table 1 presents the time(user time, in seconds) required to find the desired network situation for each of the attacks presented in the present work, using both detection mechanisms, Gecode and Adaptive Search. The execution times presented in Table 1 are the average times of 128 runs.

5 Evaluation

The performance of the prototypes described in Sec. 4 shows a multitude of performance numbers relative to the intrusion detection mechanisms used for each network signature. Looking closely at the results in Table 1, it is possible to see that Gecode usually performs better than Adaptive Search, except in the SYN flood attack. This difference is explained by the fact that Adaptive Search needs a very good heuristic functions to improve its performance. We created some heuristics based on the network situations we are studying which improved the performance of Adaptive Search, but still can't reach the performance of Gecode. The SYN flood attack performed better in Adaptive Search due to the fact that the network packets of the attack are close together and there aren't almost any other packets between the packets of the attack.

Even without a perfect heuristic of Adaptive Search, the results obtained are quite encouraging. As for Gecode, the results obtained are quite good. With these results, we are now ready to start the detection of intrusions in real network traffic instead of log files.

As for NeMODe, it turns out to be a success, since it was possible to easily describe all the three network intrusions and generate valid code that could detect the desired network situation. Although other intrusion detection systems like Snort could detect the attacks presented in this work, they can not describe the problems with the expressiveness used by NeMODe or even relate the several packets that make part of the attack.

6 Conclusions and Future Work

The work presented in this paper presents NeMODe, a Domain Specific Language to describe network intrusion signatures that generates intrusion detection recognizers based on Constraint Programming, more specifically, using Gecode and Adaptive Search.

The results obtained in this work show that it's possible to transform the description of a network situation using several intrusion detection mechanisms, based on Constraint Programming, from a single description and then use those recognizers detect the desired intrusion using the generated code, demonstrating the viability of using Constraint Programming in network monitoring tasks.

Also, we showed that we can easily describe network signature attacks that spread across several network packets, which is somewhat tricky or even impossible to make using systems like Snort. Although the intrusion mentioned in this work can be detected with other intrusion detection systems, they are modeled/described with out relating the several network packets of the intrusion, much of the times using a single network packet to describe the intrusion, which could in some situations produce a large number of false positives.

This work is still at an early stage of development, we expect there to be plenty of room for improvement: we have reached an efficiency level that may be suitable to start performing network monitoring tasks on live network traffic link, meaning that and important step will be to apply this method in a real network to assess its performance.

A very important future work is to model more network situations as a CSP in order to evaluate the performance of the system while working with a larger diversity of problems.

NeMODe will be extended to be more flexible, allowing to describe other network properties and a broader range of attack signatures and also include more back-ends, allowing the detection of intrusions using several methods using a single description.

Acknowledgments

Pedro Salgueiro acknowledges FCT –Fundação para a Ciência e a Tecnologia– for supporting him with scholarship SFRH/BD/35581/2007. The IBM QS21 dual-Cell/BE blades used in this work were donated by IBM Corporation, in the context of a SUR (Shared University Research) grant awarded to Universidade de Évora and CENTRIA.

References

1. Martin Roesch. Snort - lightweight intrusion detection for networks. In *LISA '99: Proceedings of the 13th USENIX conference on System administration*, pages 229–238, Berkeley, CA, USA, 1999. USENIX Association.
2. Jay Beale. *Snort 2.1 Intrusion Detection, Second Edition.* Syngress Publishing, 2004.
3. F. Rossi, P. Van Beek, and T. Walsh. *Handbook of constraint programming.* Elsevier Science, 2006.
4. P. Van Hentenryck and L. Michel. *Constraint-based local search.* MIT Press, 2005.
5. A. Van Deursen and J. Visser. Domain-specific languages: An annotated bibliography. *ACM Sigplan Notices*, 35(6):26–36, 2000.
6. Gecode Team. Gecode: Generic constraint development environment, 2008. Available from http://www.gecode.org.
7. Douglas Comer. *Internetworking With TCP/IP Volume 1: Principles Protocols, and Architecture, 5th edition.* Prentice Hall, 2006.
8. Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, page 283. ACM, 2000.
9. H. Song and J.W. Lockwood. Efficient packet classification for network intrusion detection using FPGA. In *Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays*, pages 238–245. ACM New York, NY, USA, 2005.
10. K.S.P. Arun. Flow-aware cross packet inspection using bloom filters for high speed data-path content matching. In *Advance Computing Conference, 2009. IACC 2009. IEEE International*, pages 1230 –1234, 6-7 2009.
11. S. Kumar and E.H. Spafford. A software architecture to support misuse intrusion detection. In *Proceedings of the 18th national information security conference*, pages 194–204, 1995.
12. P. Codognet and D. Diaz. Yet another local search method for constraint solving. *Lecture Notes in Computer Science*, 2264:73–90, 2001.
13. F. Glover, M. Laguna, et al. *Tabu search.* Springer, 1997.
14. Salvador Abreu, Daniel Diaz, and Philippe Codognet. Parallel local search for solving constraint problems on the cell broadband engine (preliminary results). *CoRR*, abs/0910.1264, 2009.
15. C. Schulte and P.J. Stuckey. Speeding up constraint propagation. *Lecture Notes in Computer Science*, 3258:619–633, 2004.
16. Pedro Salgueiro and Salvador Abreu. A DSL for Intrusion Detection based on Constraint Programming. In *SIN 2010: Proceedings of the 3rd International Conference on Security of Information and Networks*, New York, NY, USA, 2010. ACM.
17. tcpdump web page at http://www.tcpdump.org/, April, 2009.