ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

Firewall Policy Anomaly Detection and Resolution Using Rule Based Approach

B.Srikanth[1] , Smt.K.Venkata Ramana[2]

M.Tech Student, Dept. of CSE, R.V.R & J.C College of Engg,Chowdavaram, Guntur, Andhra Pradesh -522119, India[1]

Associate Professor, Dept. of CSE, R.V.R & J.C College of Engg,Chowdavaram, Guntur, Andhra Pradesh - 522119, India[2]

ABSTRACT: Security concerns are becoming increasingly critical innetworked systems. Firewalls provide important defense fornetwork security. Computer firewalls are widely used for security policy enforcement and access control. Current firewalls use various processing models and are configured using their own policy description languages. However, misconfigurations in firewallsare very common and significantly weaken the desired security. In this paper, a novel methodology called rule-based segmentation technique is proposed to identify policy anomalies, which is articulated with a grid-based representation. It derives effective solutions to avoid anomalies by providing anintuitive cognitive sense about policy anomaly. The experiments shown that, the proposed approachcan efficiently discover and resolve anomalies in firewall policies.

Keywords: firewall policy, security, rule segmentation, correlation.

I. INTRODUCTION

Firewall is a widely deployed mechanism for improving the security of enterprise networks. However, configuring a firewall is daunting and error-prone even for an experienced administrator. As a result, misconfigurations in firewalls are common and serious. In examining 37 firewalls in production enterprise networks in 2004, Wool found that all the firewalls were misconfigured and vulnerable, and that all but one firewall was misconfigured at multiple places [1]. As other evidence, Firewall Wizards Security Mailing List [2] has discussed many real firewallmisconfigurations. The wide and prolonged spread of worms, such as Blaster and Sapphire, demonstrated that many firewalls were misconfigured, because "well-configured firewalls could have easily blocked them" [1].

Correctly configuring firewall rules has never been an easy task. In 1992, Chapman [3] discussed many problems that make securely configuring packet filtering a daunting task. Some of them, e.g., omission of port numbers in filtering rules, have been addressed by firewall vendors. However, many others are yet to be addressed successfully. Since firewall rules are written in platform-specific, low-level languages, it is difficult to analyse whether these rules have implemented a network's high-level security policies accurately. Particularly, it is difficult to analyse the interactions among a large number of rules. Moreover, when large enterprises deploy firewalls on multiple network components, due to dynamic routing, a packet from the same source to the same destination may be examined by a different set of firewalls at different times. It is even more difficult to reason whether all these sets of firewalls satisfythe end-to-end security policies of the enterprise.

In this paper, we represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation (either conflicting or redundant) among those rules. We also introduce a flexibleconflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

definition. Besides, a more effective redundancy elimination mechanism is provided in our framework, and our experimental results show that our redundancy discovery mechanism can achieve approximately 70 per cent improvement compared to traditional redundancy detection approaches [4], [3]. Moreover, the outputs of prior policy analysis tools [4], [5] are mainly a list of possible anomalies, which does not give system administrators a clear view of the origination of policy anomalies.

II.RELATED WORK

Effective mechanisms and tools for policy management are crucial to the success of firewalls. Recently, policy anomaly detection has received a great deal of attention [4], [6], [7], [5]. Corresponding policy analysis tools, such as Firewall Policy Advisor [4] and FIREMAN [5], with the goal of detecting policy anomalies have been introduced. Firewall Policy Advisor only has the capability of detecting pairwise anomalies in firewall rules.

FIREMAN can detect anomalies among multiple rules by analysing the relationshipsbetween one rule and the collections of packet spaces derived from all preceding rules. However, FIREMAN alsohas limitations in detecting anomalies [6]. For each firewallrule, FIREMAN only examines all preceding rules butignores all subsequent rules when performing anomalyanalysis. In addition, each analysis result from FIREMANcan only show that there is a misconfiguration between onerule and its preceding rules, but cannot accurately indicate allrules involved in an anomaly

A first approach to addressing our problem domain is the use of refinement mechanisms. In this way, we can perform a top-down deployment of rules by unfolding a global set of security policies into the configurationsof several components and guaranteeing that those deployed configurations are free of anomalies. In [8], forexample, the authors present a refinement mechanism that uses a formal model for the generation of filteringrules by transforming general rules into specific configuration rules. Indeed, the authors propose the use of roles to better define network capabilities, and the use of an inheritance mechanism through a hierarchy of entities to automatically generate permissions and prohibitions.

A second refinement approach based on the concept of roles is presented in [9]. However, and although the authors claim that their work is based on the Role Base Access Control (RBAC) model, their specification of network entities, roles, and permission assignments are not rigorous and does not fit any reality. Most of these limitations are solved in the approach presented in [11], where a global set of rules based on theOrganization Based Access Control (OrBAC) model [4] are further deployed into specific firewall configuration files through a transformation process. Generally, administrators are reluctant to set up from scratch a whole network security policy, and prefer recycling existing configurations.

A second manner to address our problem domain is through the use of automatic network support tools intended for the creation of configurations for security devices. Firewall Builder, for example, provides a common interface to specify a network access control policy and then this policy is automatically translated into various firewall configuration languages, such as net filter [10], ipfilter [9], or Cisco PIX [9]. Similarly, the Cisco Security Manager [13] is a commercial support tool designed to manage security policy deployments on heterogeneous networks based on Cisco devices. However, we consider that these two solutions do not offer a semantic model rich enough to express complete security policies; and, although they offer some routines for the discovery of conflicts between rules, such functionality requires the administrator's assistance and only simple redundancy that corresponds to trivial equality or inclusion between zones is detected.

The authors of [4–6] propose in their work an efficient set of algorithms to detect policy anomalies in both single- and multi-firewall configuration setups. Nonetheless, we also consider their approach as incomplete. First, their intra- and inter-component discovery approach is not complete since, given a single- or

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

multiple-component securitypolicy; their detection algorithms are based on the analysis of relationships between rules two by two. This way, errors due to the union of rules are not explicitly considered (as our approach does).

III.ANOMALYREPRESENTATIONBASEDONPACKET SPACE

A.PacketSpaceSegmentationandClassification

As per the discussion in Section 2, existing anomaly detection methods could not accurately point out the anomaly portions caused by a set of overlapping rules. In order to precisely identify policy anomalies and enable a more effective anomaly resolution, we introduce a rule-basedsegmentation technique, which adopts a binary decision diagram (BDD)-based data structure to represent rules and perform various set operations, to convert a list of rules into a set of disjoint network packet spaces. This technique has been recently introduced to deal with several research problems such as network traffic measurement [14], firewall testing [15] and optimization [16]. Inspired by those successful applications, we leverage this technique for the employ a two-dimensional geometric representation for each packet space derived from firewall rules. Note that a firewall rule typically utilizes five fields to define the rule condition; thus, a complete representation of packet space derived from the example policy shown in Table 1. We utilize colored rectangles to denote two kinds of packet spaces: allowed space (white color) and denied space (graycolor), respectively. In this example, there are two allowed spaces representing rules r3 and r5 three denied spaces and depicting rules r1, r2, and r4.

Table 1: An Example Firewall policy

Rule	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
R1	TCP	10.1.*.*	*	192.168.1.*	25	Allow
R2	TCP	10.1.*.*	*	192.168.1.*	25	Allow
R3	UDP	10.1.*.*	*	172.32.1.*	53	Deny
R4	UDP	10.1.*.*	*	172.32.1.*	53	Allow
R5	*	*	*	*	*	Deny

Two spaces overlap when the packets matching two corresponding rules intersect. For example, r5 overlaps with r2, r3 and r4, respectively. An overlapping relation may involve multiple rules. In order to clearly represent all identical packet spaces derived from a set of overlapping rules, we adopt the rule-based segmentation technique addressed in Algorithm 1 to divide an entire packet space into a set of pairwise disjoint segments. We classify the policy segments as follows: nonoverlapping segment and overlapping segment, which is further divided into conflicting overlapping segment and nonconflicting overlapping segment.

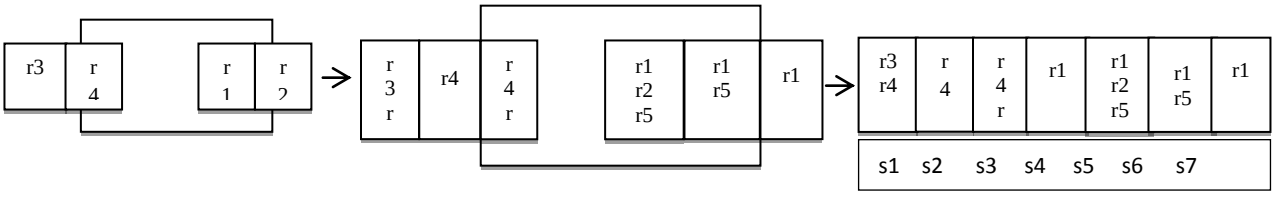

Figure 1 : Packet space segmentation

The second step in figure1 demonstrates the segments of packet spaces derived from the example policy. Since the size of segment representation does not give any specific benefits in resolving policy

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

anomalies, we further present a uniform representation of space segments in Fig. 1c. We can noticethat seven unique disjoint segments are generated. Three policy segments s2,s4, and s7 are nonoverlapping segments. Other policy segments are overlapping segments, including two conflicting overlapping segments s7 and s3, and two nonconflicting overlapping segments s1and s6.

B. Grid RepresentationofPolicyAnomaly

To enable an effective anomaly resolution, complete and accurate anomaly diagnosis information should be represented in an intuitive way. When a set of rules interacts, one overlapping relation may be associated with several rules. Meanwhile, one rule may overlap with multiple other rules and can be involved in a couple of overlapping relations (overlapping segments). Different kinds of segments and associated rules can be viewed in the uniform representation of anomalies (Fig. 1). However, it is still difficult for an administrator to figure out how many segments one rule is involved in. To address the need of a more precise anomaly representation, we additionally introduce a grid representation that is a matrix-based visualization of policy anomalies, in which space segments are displayed along the horizontal axis of the matrix, rules are shown along the vertical axis, and the intersection of a segment and a rule is a grid that displays a rule's subspace covered by the segment.

Table 2: Grid representation of policy anomaly

	s1	s2	s3	s4	s5	s6	s7
r1	r3						
r2	r4	r4	r4				
r3					r1	r1	r1
r4					r2		
r5				r5	r5	r5	r5

Figure 2 shows a grid representation of policy anomalies for our example policy. We can easily determine which rules are covered by a segment, and which segments are associated with a rule. For example, as shown in Fig. 2, we can notice that a conflicting segment (CS) s5, which points out a conflict, is related to a rule set consisting of three conflicting rules r3,r4, and r5 (highlighted with a horizontal red rectangle), and a rule r3 is involved in three segments s5,s6, and s7 (highlighted with a vertical red rectangle). Our grid representation provides a better understanding of policy anomalies to system administrators with an overall view of related segments and rules.

IV. ANOMALYMANAGEMENTFRAMEWORK

Our policy anomaly management is composed of two core functionalities: conflict detection and resolution, and redundancy discovery and removal, as depicted in Fig. 3. Both functionalities are based on the rule-based segmentation technique. For conflict detection and resolution, conflicting segments are identified in the first step. Each conflicting segment associates with a policy conflict and a set of conflicting rules.

Also, the correlation relationships among conflicting segments are identified and conflict correlation groups (CG) are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately; thus, the searching space for resolving conflicts is reduced by the correlation process. The second step generates an action constraint for each conflicting segment by examining the characteristics of each conflicting segment.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

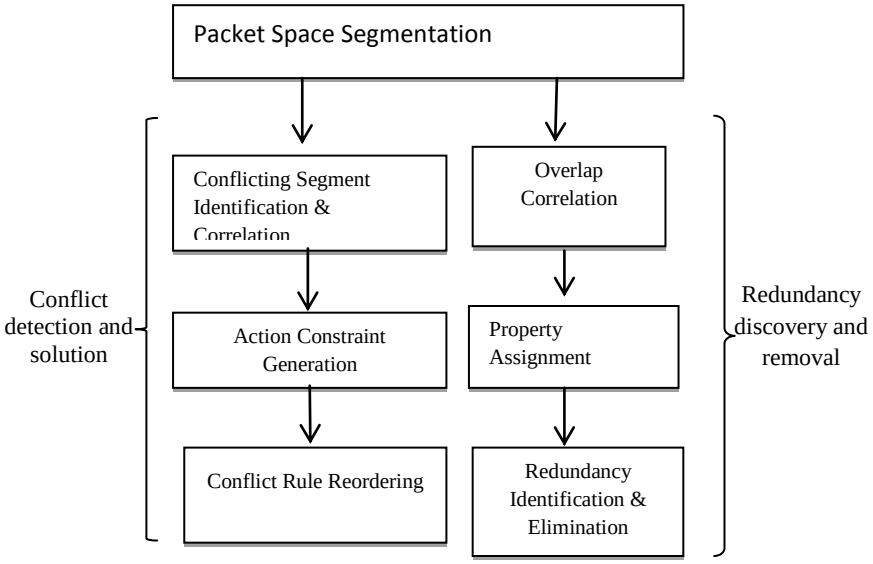

Figure 2 : Policy anomaly management framework

A strategy-based method is introduced for generating action constraints. The third step utilizes a reordering algorithm, which is a combination of a permutation algorithm and a greedy algorithm, to discover a near-optimal conflict resolution solution for policy conflicts. Regarding redundancy discovery and removal, segment correlation groups are first identified. Then, the process of property assignment is performed to each rule's subspaces. Consequently, redundant rules are identified and eliminated.

A.ConflictResolution

Each conflicting segment indicates a policy conflict as well as a set of conflicting rules involved in the conflict. Once conflicts are identified, a possible way for a system administrator to resolve conflicts is to manually change the conflicting rules. However, as we addressed in Section 1, resolving all conflicts manually is a tedious task and even impractical due to the complicated nature of policy conflicts. Thus, a practical and effective method to resolve a policy conflict is to determine which rule should take precedence when a network packet is matched by a set of rules involved in the conflict. In order to utilize the existing first-match conflict resolution mechanism implemented in common firewalls, the rule expected to take precedence needs to be moved to the first-match rule.

Table 3 : Generating Constraint from Conflict Resolution Strategy

Strategy	Action Constraint
Deny-overrides	Action = "deny"
Allow-overrides	Action = "allow"
Recency-overrides	Action of the newest rule
Specificity-	Action of the most specific rule
High-majority-overrides	Action of the rules with greater number than the
First-match-	Action of the first-matched rule
High-authority-overrides	Action of the rule with the highest

Our conflict resolution mechanism introduces that an action constraint is assigned to each conflicting segment. An action constraint for a conflicting segment defines a desired action (either Allow or Deny) that the

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

firewall policy should take when any packet within the conflicting segment comes to the firewall. Then, to resolve a conflict, we only assure that the action taken for each packet within the conflicting segment can satisfy the corresponding action constraint.

A key feature of this solution is that we do not need to move a rule expected to take precedence to the first match rule at all times. Any rule associated with the conflict on the same action (as a rule with the precedence) can be moved to the first-match rule, guaranteeing the same effect with respect to the conflict resolution. Thus, it is doable to obtain an optimal solution for conflict resolution.

V. RESULTS AND ANALYSIS

A. Evaluation of Conflicting SegmentGenerationandCorrelation

Table 4 shows the evaluation results generated by the segmentation and correlation engine of FAME. The number of conflicting segments, the number of conflict correlation groups, the number of large conflict correlation groups (the rule number is greater than six)and the number of conflicting rules in the largest correlation group are given in this table, which also contains the execution time required by the segmentation module of FAME for identifying conflicting segments (i.e., detecting conflicts), as well as the one required by the correlation module of FAME for identifying correlation groups among conflicting segments. Note that all measurements were based on the system time stamps in our experiments.

In Table 4, the number of large conflict correlation groups and the number of conflicting rules in the largest correlation group give us the evidences that manual conflict resolution for a large size of firewall policies is almost impossible. Also, we can observe that the segmentation and correlation processes are efficient enough to handle a larger size of firewall policies, such as policy G and policy H in the table.

Table 4 : Segmentation and Correlation Evaluation

Policy	Rules(#)	Segmentation		Correlation		First Match		Proposed	
		CS(#)	Time(s)	CG(#)	Time(s)	RC	Time(s)	RC	Time(s)
1(A)	12	4	0.134	2	0.056	3	0.358	4	0.563
2(B)	18	5	0.186	3	0.073	3	0.689	4	0.689
3(C)	25	8	0.233	3	0.081	6	0.748	7	0.769
4(D)	52	14	0.377	7	0.094	9	1.132	11	1.764
5(E)	83	20	0.427	9	0.118	15	1.438	17	2.547
6(F)	132	36	0.518	10	0.143	24	6.567	31	9.239
7(G)	354	67	0.854	10	0.189	57	33.879	60	94.756
8(H)	926	107	2.386	13	0.437	86	104.407	93	251.76

B. Evaluationof ConflictingRuleReordering Algorithm

We have addressed that permutation and greedy algorithms can be used for reordering conflicting rules, and our conflict resolution mechanism utilizes a combination algorithm incorporating the features of both permutation and greedy algorithms to achieve a more effective and efficient conflict resolution. In order to evaluate our proposed method, we measured the effectiveness and efficiency of three algorithms implemented in the rule reordering module of FAME using two metrics, resolved conflicts (RC) and resolving time.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

The permutation algorithm can always achieve an optimal conflict resolution for all policies except policy H. We were unable to resolve the conflicts in policy H using the permutation algorithm, because there exist a larger size of conflicting rules in some correlation groups. From Table 3, we can notice that the number of the largest group member of policy H is eighteen. Also, it shows that the resolving time required by the permutation algorithm increases exponentially as the number of conflicting segments increases. Hence, the permutation algorithm is infeasible to the policies with a large size of conflicting rules, although it can achieve an optimal solution.

Regarding the greedy algorithm, Table 4 shows that it can only achieve a near-optimal conflict resolution for all firewall policies. However, as the size of conflicting rules increases, the time taken by the greedy algorithm increases almost linearly as opposed to an exponential increase in case of using the permutation algorithm.

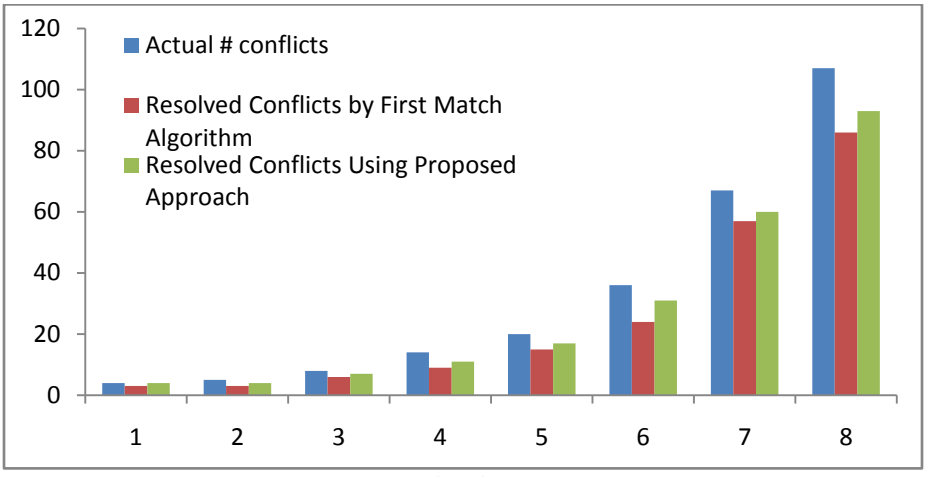

Figure 3 : Evaluation of conflict resolution

For the combination algorithm with the default threshold (N=6), the results in Table 4 show that the number of resolved conflicts by the combination algorithm is greater than the greedy algorithm and almost equal to the optimal solution achieved by the permutation algorithm. The computation time is acceptable for all policies as well. Therefore, it represents higher efficiency and effectiveness in conflict resolution.

VI.CONCLUSION

The range of network security is very broad. Firewall security, like any other technology, requires proper management in order to provide proper security services. Thus, just having firewalls on the network boundaries or between sub-domains may not necessarily make the network any secure. One reason of this is the complexity of managing firewallrules and the resulting network vulnerability due to rule anomalies. A firewall is a network element that controls the traversal of packets across the boundaries of a secured network based on a specific security policy.

A firewall security policy is a list of ordered filtering rules that define the actions performed on packets that satisfy specific conditions. A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effective and efficient anomaly analysis. In addition, it is demonstrated that our proposed anomaly analysis methodology is practical and helpful for system administrators to enable an assurable network management. Our future work includes to extend our anomaly analysis approach to handle distributed firewalls.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

REFERENCES

[1] A. Wool. A quantitative study of firewall configuration errors. IEEE Computer, 37(6), 2004.
[2] Firewall wizards security mailing list.http://honor.icsalabs.com/mailman/listinfo/firewall-wizards.
[3] D. B. Chapman. Network (in)security through IP packet filtering.In Proceedings of the Third Usenix Unix SecuritySymposium, pages 63–76, Baltimore, MD, September 1992.
[4] E. Al-Shaer and H. Hamed, "Discovery of Policy Anomalies inDistributed Firewalls," IEEE INFOCOM '04, vol. 4, pp. 2605-2616,2004.
[5] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C.Davis, "Fireman: A Toolkit for Firewall Modeling and Analysis,"Proc. IEEE Symp. Security and Privacy, p. 15, 2006.
[6] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "CompleteAnalysis of Configuration Rules to Guarantee Reliable NetworkSecurity Policies," Int'l J. Information Security, vol. 7, no. 2, pp. 103122,2008.
[7] F. Baboescu and G. Varghese, "Fast and Scalable ConflictDetection for Packet Classifiers," Computer Networks, vol. 42,no. 6, pp. 717-735, 2003.
[8]Bartal, Y., Mayer, A., Nissim, K., and Wool, A. Firmato: A novel firewall management toolkit. In IEEE Symposiumon Security and Privacy, pp. 17–31, Oakland, California, May, 1999.
[9] Reed, D. IP Filter. [Online]. Available from:http://www.ja.net/CERT/Software/ipfilter/ip-filter.html
[10]Welte, H., Kadlecsik, J., Josefsson, M., McHardy, P., andet al. The netfilter project: firewalling, nat and packetmangling for linux 2.4x and 2.6.x. [Online]. Availablefrom: http://www.netfilter.org/
[11]Hassan, A. and Hudec, L. Role Based Network Security Model: A Forward Step towards Firewall Management.In Workshop On Security of Information Technologies, Algiers, December, 2003.
[12] Open Security Foundation. Open Source Vulnerability Database. [Online]. Available from: http://osvdb.org/
[13]Cuppens, F., Cuppens-Boulahia, N., Sans, T., and Miege, A. A formal approach to specify and deploy anetwork security policy. In Second Workshop on Formal Aspects in Security and Trust, pp. 203–218, Toulouse,France, August, 2004.
[14] L. Yuan, C. Chuah, and P. Mohapatra, "ProgME: TowardsProgrammable Network Measurement," ACM SIGCOMM ComputerComm. Rev., vol. 37, no. 4, p. 108, 2007.
[15] A. El-Atawy, K. Ibrahim, H. Hamed, and E. Al-Shaer, "PolicySegmentation for Intelligent Firewall Testing," Proc. First WorkshopSecure Network Protocols (NPSec '05), 2005.
[16] G. Misherghi, L. Yuan, Z. Su, C.-N.Chuah, and H. Chen, "AGeneral Framework for Benchmarking Firewall OptimizationTechniques," IEEE Trans. Network and Service Management, vol. 5,
no. 4, pp. 227-238, Dec. 2008.

BIOGRAPHY

Ms.K.VenkataRamana obtained her B. Tech in Computer Science and Engineering from R.V.R. & J.C. College of Engineering, Guntur. She received her M.Tech. in Computer Science and Engineering at R.V.R. & J.C. College of Engineering, Guntur. She is pursuing Ph.D. in Computer Science and Engineering at AcharayaNagarjuna University, Guntur. She is currently working as Associate Professor at R.V.R. & J.C. College of Engineering, Guntur. She has 11 years of teaching experience. Her research areas of interest include Information Security, Cryptography&Network Security and Computer Networks.

B.Srikanth received B.Tech in Information Technology from Jawaharlal Nehru Technological University, Kakinada in the year 2010 and He is currently pursuing M.Tech in Computer Science and Engineering at R.V.R. & J.C. College of Engineering, Guntur. His research areas include Network security and cryptography, Information security and computer networks.