Policy Management in Adhoc Networks

GantiNagaSatish[#1], Prof.P.Suresh Varma[*2]

[#1]*Research Scholar, Department of Computer Science, Adikavi Nannya University, Rajahmundry.A.P.INDIA*
[*2]*Professor, Department of Computer Science, Adikavi Nannya University, Rajahmundry, A.P., INDIA*

Abstract- Policy-based management is based on defining a set of global rules, according to which a network or distributed system must operate. In the last few years, policy-based management has begun to emerge as the dominant paradigm for developing network and systems management functions, primarily, since it can reduce complexity in management applications. Although attempts are underway to standardize policy-based management, significant research challenges remain. The paper outlines the research agenda and application of policy management to security management.

Index Terms- Policy Decision Point, Policy Enforcement Point, Policy Repository

I. INTRODUCTION

An adhoc network is a collection of wireless mobile hosts that creates a spontaneous network when they are enough close to each other. This network configuration is realized without any form of centralized management or standard support services that exists in wired networks. However, in such hosts, network interfaces have a limited transmission range. Consequently, in order to render possible communications between ad hoc terminals that are not directly reachable, multiple network hops are necessary. In fact, each terminal is a mobile node that can behave transparently as a host or as a router for other mobile nodes packets. Mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. To discover multi-hop routes, mobile nodes use an ad hoc routing protocol that is the same in principle as classical networks routing protocols but different in term of behaviour as ad hoc node are mobile necessitating to frequently discovering new routes or path loss due to QoS communication degradation when the distance between mobile nodes increases or when external factors affect negatively communications. In the commercial market, this type of network is gaining more and more acceptance due to the potential of applications, the facility to deploy as well as the cost economy in term of infrastructure and management (e.g. 802.11 technologies). Many indoor and outdoor applications in various areas can be envisaged in civil (e.g. students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting) and military domains (e.g. soldiers relaying information for situational awareness on the battlefield). However, this new technology introduces a lot of challenges in order to function properly. The main objective of this paper is not propose any solutions to these problems but rather how future mechanisms that are under study by a number of research groups will be managed in order to control utilization of network resources as well as access to end users. The main challenge is to introduce mechanisms that will permit the configuration of adhoc terminals so that any spontaneous network created inside the company area will follow a set of predefined enterprise management objectives. Thus, we propose naturally to use Policy-based Management (PBM) approach to control the adhoc networks [1]. However, because the specific behaviour of adhoc networks, it is necessary to rethink the way policy based management should be deployed in these networks. This approach can be a little bit in contradiction with the concept of self manageable and self configurable adhoc networks. A policy-based approach addresses most of the key requirements of an adhoc network management system, namely automation, self-organizing capability, robustness and efficiency. The fundamental challenge in extending the policy based approach to adhoc networks is to adapt this conceptually centralized approach to a distributed, infrastructure-independent environment [2]. The remaining of the paper is organized as follows: section II describes the Policy Based Management, Policy Decision Point and Policy Enforcement Point. Section III presents Background on Policy Technology. In Section IV, the Policy Based Traffic Management is presented. Section V presents Distributed Policy Management Architecture, Section VI presents Application of Policy Management to Security Management and finally a conclusion.

II. POLICY BASED MANAGEMENT

The policy based management [1] approach aims to defines high level objectives of network and system management based on a set of policies that can be enforced in the network. Policies are a set of predefined rules (defined actions to be triggered when a set of conditions are fulfilled) that govern network resources, including conditions and actions that are established by the network administrator with parameters that determine when the policies are to be implemented in the network. Policy provides a means of specifying and dynamically changing management strategy without coding policy into the implementation. Policy-based management has many benefits of delivering consistent, correct, and understandable network systems. The framework introduces a set of component to enable policy rules

definition, saving and enforcing. These components are the Policy enforcement Point (PEP) and the Policy Decision Point (PDP)[1]. The PEP component is a policy decision enforcer located at the network and system equipment's boundary. The PDP is the decision-making component which role is to perform the policy defined the manager. The PDP is responsible for the high level decision-making that consists of retrieving policy, interpreting policy, detecting policy conflicts, etc and enforcing the decision in the network through the PEP. It interacts with PEPs that are located in or near managed equipment to exchanging control information and/or decisions. Mainly, the PEP performs metering which consists of network monitoring and controlling for the purpose of detecting or performing any changes in the network in order to fulfill high level policies.

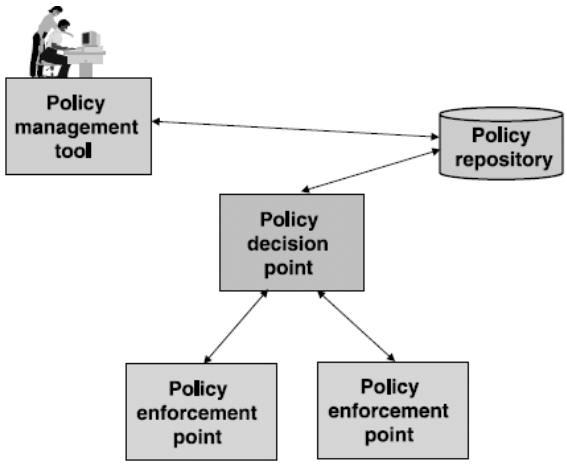

Fig 1. Policy Based Management Architecture

A. Policy Decision Point (PDP)

The PDP [1] or policy server is a logical component responsible for the high level decision-making. The PDP decision is based on policies retrieved from the policy repository as well as on level network information collected from network management entities. The policy server generally retrieves policy from the policy repository, interprets and translates them into a format that can be used to enforce decision in the network through Policy Enforcement Points.

B. Policy Enforcement Point (PEP):

PEP [1] is a network device (a router, a switch, an end-host) which requests and applies policy-based decisions from one or more PDP. PEP is also responsible for collecting the necessary information about the current network state, the traffic situation, transmission errors as well as any relevant information and reporting them to the PDP.

III. Background on Policy Technology

There is no standard way of defining policy but there are some definitions put forward by academic researchers. Policy is predetermined action statement for such action patterns that are repeated by entities involved in a network under certain systems conditions when they are met. More concisely, policy is set of rules to administer, manage and control the access to network resources and services. Each policy is a rule containing four components, namely conditions, actions, priority and role. The conditions associated with a policy rule specify if the policy is applicable. We say a policy is applicable when the conditions associated with the rule evaluate to true. If a policy is applicable, then the set of actions associated with the policy gets executed. The priority is a non-negative integer that indicates the relative importance of the associated policy. The priority value determines which policy must be applied when there are multiple applicable policies with potentially conflicting actions (e.g., one policy may allow access to data, while another blocks it). Finally, the role defines the context in which the policy will be relevant. The policies are stored in a policy repository.

IV. Policy Enforcement in a Wireless Adhoc Network

Policy enforcement is always dependent on the ability of the various devices in the network to implement the policies, which may include permitting or blocking traffic from specific hosts or applications, permitting or blocking traffic of specific type, and so on. Network management policies in traditional enterprise wire-line networks are typically enforced by the routers in the network or other network devices therefore advantageous for each node to act as a policy enforcement point (PEP) and have the ability to accept requests from the policy management system and enforce the various policies based on those requests.

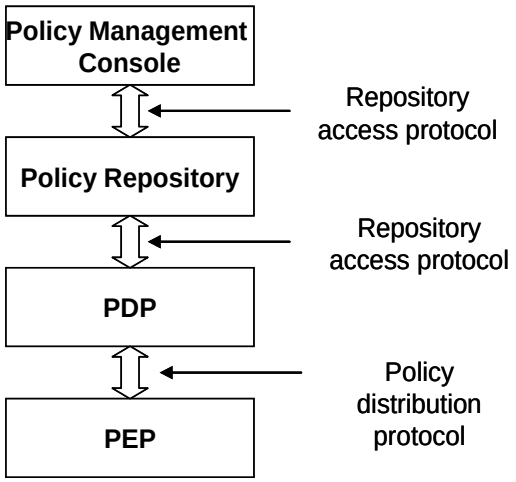

Fig2: Policy Based Architecture Components

The policy repository can be seen as a database that contains policy information. Several possibilities exist to store policy information (e.g. text files, database), however they must, necessarily, obey to a specific data model used to represent policy information.

V. Policy Based Traffic Management

Policy-based traffic management (PBTM) [3], a sub-domain of policy-based network management (PBNM), is management paradigm in networking that separates administration operations from other basic network operations. It provides a flexible and robust mechanism to allocate network resources and services like bandwidth allocation, quality of service, access rights, traffic prioritization and security to different network elements. It results in increasing quality of work, efficiency, adaptability, coherent network behaviour, flexibility and reduced maintenance cost regarding to network management. Policy as a goal or course of action to guide present and future network decisions. More concisely, policy is set of rules to administer, manage and control the access to network resources and services. There are mainly two types of network operations: Core network operations, management operations. Network management can be further broken into three major types of management tasks: Network QoS Management, Network Security Management, and Network Configuration Management. QoS and security, both requires configuration management and are dependent on it. However network policies can be classified generally into the following six broad categories

- Performance Management Policies
- Security/Access Control Policies
- Quality of Service Policies
- Administrative/Configuration Management Policies
- Fault Management Policies
- Customized/Event Condition Action Policies

A. Distinct Characteristics of Policy based Network Management:

- Classification of network Traffic
- Degrees of control
- Stateful Traffic Inspection
- User Identification
- Application Identification
- Policy Enforcement

B. Service and Controls of Policy Based Network management:

- Scalability
- Scope of Control
- User Specific Privileges
- Traffic priority
- Search restrictions
- Alert Notifications

VI. Distributed Policy Management Architecture

Management of large networks is not usually possible from a single network management system because a single system will need to maintain a large quantity of data[2]. Further, the number of functions that the single system will need to perform may require a very large amount of CPU processing. Traditional network management systems distribute the management functions to several systems and usually multiple layers of management. Unique characteristics of wireless ad hoc networks also make it necessary to distribute the network management functions. Depending on the specific application that the wireless ad hoc network is used for, additional requirements may exist that mandate a distributed architecture and potentially drive the implementation of a specific distributed architecture. Designing an effective distributed architecture for the specific application that is supported by the network is a challenging problem that involves many trade-offs. There are two general approaches that have been proposed for distributing the network management functions.

In the peer-to-peer architecture, the network is divided into domains and each domain is managed by a single network management system that is fully independent from the network management systems in the other network domains. Coordination among network management systems in different domains may not be possible or may not be allowed because the different domains may belong to different administrative entities. Coordination among the network management systems in each domain may only be allowed if it benefits both domains.

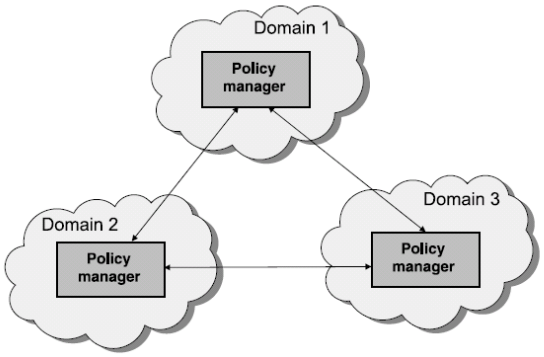

Fig 3: Peer to Peer policy management architecture

The alternative distributed policy management architecture is the hierarchical architecture. In the

hierarchical architecture each policy manager is responsible for managing a network domain which may contain one or more network devices. The difference in the hierarchical architecture is that the different domains are not independent administratively. There is a relationship among the policy managers of each domain reflected in the hierarchy. This hierarchy affects how the various policy managers coordinate. The network is also divided into domains and each domain has its own management system but each system is not independent of the others. In the hierarchical architecture there is a management system that is at the top of the hierarchy and all other systems are subordinate to that system. Distribution of the network management functions is driven from the top of the hierarchy such that policy enforcement is accomplished across the whole network and is implemented such that it benefits the entire network.

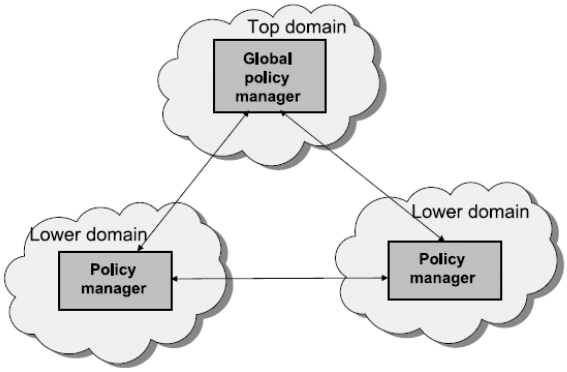

Fig 4 Hierarchical Policy management architecture

VII. Application Of Policy Management To Security Management

Policy management applies in general to various aspects of network management including security management. For example, policy management has been applied to managing access control (e.g. based on the level of trust of each node), which is a key security management area. One of the approaches for applying policy management to managing access control has been the use of policies for defining access control for users based on their roles rather than defining access control manually for each user which is called role-based access control. Some of the security management schemes explained below

A. Role-Based Access Control (RBAC)

Role-based access control (RBAC)[2] is a widely used security scheme for providing access control. Although it is not really a policy management system, it can be considered as a vehicle for implementing access control policies, which is one of the most important aspects of security policies. RBAC assigns access privileges not to specific users but to specific roles. For example, a security administrator may have access privileges to significant services that other users may not. Tying access privileges to roles rather than individual users simplifies the management of access control because permissions only need to be entered once for the role and then each user with the same role receives the same permission, avoiding a repetitious and error-prone task. Also, changes in the security policies of the organization can be easily implemented by modifying permissions to roles and not to every individual user. It is also possible in RBAC systems to allow users to inherit permission from another role and then expand on the permissions for that role. For example, a security administrator may inherit all of the privileges that a regular user has and then obtain additional privileges that are unique to the administrator role. This further simplifies managing changes to security policies and provides the ability to consistently manage access control.

B. Trust Management and the KeyNote System

Trust management is a common framework for representing and managing security policies, security credentials, and trust relationships. A key advantage of this concept[4][5] is that it allows applications to treat these three key security functions consistently and in a unified manner reducing overall complexity and risk of security flaws. KeyNote trust management system that has been developed for implementing the trust management concept and is representative of the concept. In the KeyNote system security policies are defined as small programming units that authorize specific users to perform specific actions under certain conditions.

The KeyNote system has the following concepts:

- Principals are entities that can be authorized to perform certain functions. They may be users, objects, programs, etc.
- Policies and credentials are specified using a concept called assertion. Assertions are the basic programming units that define the conditions under which a principal authorizes actions requested by other principals. Policies are authorized by a principal called “Policy” who is the root of the trust hierarchy.
- Actions are a collection of attribute-value pairs. Applications make queries to the KeyNote system requesting whether a particular set of actions is authorized or not. The KeyNote system determines compliance based on the security policies and returns a policy compliance value (e.g. authorized, unauthorized).

The KeyNote architecture which has been extended in what is called the STRONGMAN [6]. The STRONGMAN (scalable trust of next generation management) approach assumes that high-level policies are specific to applications and therefore policy languages specific to the application are used

for specifying high-level policies. All the high-level policies are then translated into a common low-level policy language. The low-level policy language hides the implementation complexities from the high-level policy engines. The low-level policies are defined using the KeyNote system. The STRONGMAN architecture relies on the KeyNote system. KeyNote is a simple trust management system that provides compliance checking. In other words, it supports checking whether a proposed action complies with the local policies. Policies can be broken into smaller pieces which are signed assertions called credentials. Credentials can be distributed over the network and then local nodes can make decisions based on those credentials. Credentials signed by multiple parties can be considered when making a specific decision. Each service that needs to determine whether to permit or decline specific requests can utilize the local compliance checker.

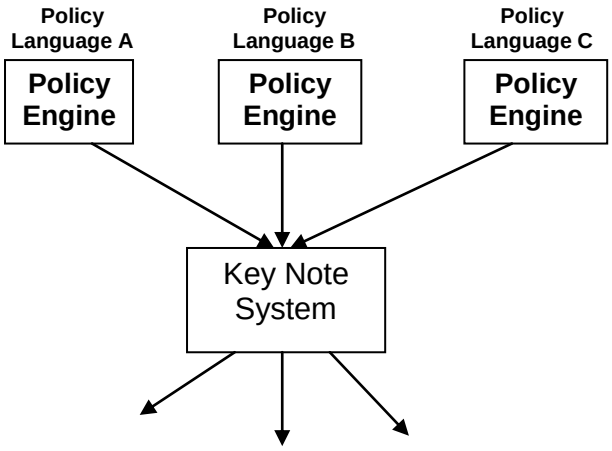

Fig 5: STRONG MAN Architecture

Since policy is expressed as credentials issued to users, it is not necessary to distribute policies throughout the network to all policy enforcement points. Users are required to provide credentials to prove that they are allowed to perform specific functions. With time, policy enforcement points learn the various policies that need to be enforced. Credentials may age with time to allow revocation of credentials.

C. Firewall Management

In Firewalls are probably the key devices for securing enterprises from outside threats. Firewalls are usually positioned at the boundaries of enterprises with external networks and limit the traffic that is allowed to enter the enterprise. The main idea behind firewalls is the belief that the fewer the traffic types that are allowed to enter the enterprise network the smaller the risk from a malicious outside user. Firewalls are often even placed inside the enterprise to provide additional layers of protection in case the external perimeter is penetrated. This also helps limit access to portions of the network that host critical servers with even stricter traffic filters. Thus, it results in enhanced protection against outsiders as well as against potential malicious insiders (i.e. users operating within the enterprise network). Ensuring that firewalls in an enterprise are configured correctly is a challenging problem, to a large extent configuration of firewalls today is done manually. Firewalls as they exist in enterprise networks today are not directly applicable to wireless ad hoc networks. This is because in the adhoc environment, it is not possible to identify traffic concentration points where a firewall can be placed to filter most of the traffic.

D. Policy Enforcement in a wireless Adhoc Network

Policy enforcement is always dependent on the ability of the various devices in the network to implement the policies, which may include permitting or blocking traffic from specific hosts or applications, permitting or blocking traffic of specific type, and so on. Network management policies in traditional enterprise wire-line networks are typically enforced by the routers in the network or other network devices. In wireless adhoc networks every node is typically involved in the networking functions such as routing. It is therefore advantageous for each node to act as a policy enforcement point (PEP) and have the ability to accept requests from the policy management system and enforce the various policies based on those requests. In wireless ad hoc networks there are usually no traffic concentration points where most traffic from the outside can be inspected and filtered. In these networks, as nodes move around, the boundaries of the network change and therefore every node or at least most nodes may become the boundary of the network with other external networks. Since every node may become part of the network boundary in order to provide effective protection from the outside every node in a wireless ad hoc network should have some policy enforcement capabilities. In wireless ad hoc networks there is also a significant threat from malicious or misbehaving insiders. In many applications envisioned for such networks, nodes are allowed to join the network dynamically. Such nodes can provide networking services, thereby becoming part of the critical infrastructure of the network. It is therefore important in such an environment for the network to be able to limit the access of all the nodes to the network and services provided over the network. This also leads to the requirement that policy enforcement points in wireless ad hoc networks must have the ability to protect each node from all other nodes. Therefore, a fully distributed solution where each node has policy enforcement capabilities is imperative for securing a wireless ad hoc networking environment. One potential approach for providing distributed policy enforcement capability is utilizing a fully distributed implementation of a firewall. The distributed firewall in was originally proposed for protecting the hosts and the network from insiders in a

large enterprise environment. Since insiders may be anywhere in the enterprise, the traditional approach of placing a few firewalls at the network boundaries is not a viable solution for protecting the network from malicious insiders. Protecting the network from insiders in an enterprise environment also requires a fully distributed solution. This leads us to believe that a solution such as the one described can be adapted to the wireless ad hoc networking environment. The key concept proposed [7] is the use of a Network Interface Card (NIC) at each host, which is a hardened tamper-resistant device that incorporates firewall capabilities. The NIC is a non by passable interface to the network that has its own processor and memory that is not accessible from the host operating system or the applications running on the host the NIC is protecting. Therefore, the NIC cannot be easily compromised by malicious users. The NIC is controlled only by a policy server that distributes new packet filtering firewall rules (i.e. access control policies) during start up and whenever new or updated policies need to be enforced. In the policy server is a centralized well-protected entity in the enterprise environment that can be used to define the security policies to be enforced by the distributed firewall implementation. The policy server needs to be well protected, because a compromised policy server can be used to open up the defenses of all nodes by implementing policies that would allow any traffic to go through the NIC.

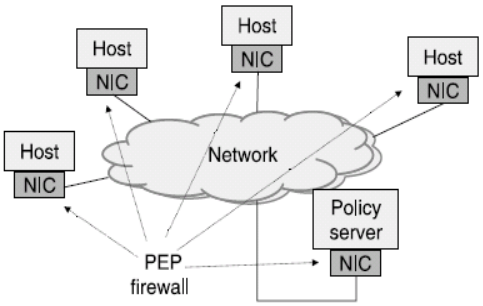

Fig 6: Distributed Firewall Architecture

One of the challenges is that the interface from a host to the network in a typical enterprise environment is based on Ethernet. In a wireless ad hoc network the network interface is not usually Ethernet-based but most likely some type of a radio interface. The other challenge with the architecture is the applicability of the centralized policy server in a wireless ad hoc networking environment. It is very difficult to ensure that a centralized policy server will be able to communicate with all NIC at all times. In a wireless adhoc network environment, connectivity to nodes is intermittent and it is impossible to ensure connectivity between the policy server and all NIC.

VIII CONCLUSION

In this paper we have presented the policy based management architecture, Traffic management and applications of policy for security management. We identified policy-based management as a promising approach for managing in adhoc networks. Policy-Based Network Management (PBNM) provides a logically centralized, simplified and automated control of the network as a whole, making management of complex network operational characteristics such as access control, and network security easier. Even though policy management is a well-developed technology for network management, there are many areas that need further investigation. Such areas include approaches for negotiating policies in a distributed policy management implementation, synchronizing policies across multiple distributed policy management systems, and resolving policy conflicts in such an environment. Each adhoc terminal includes PDP and PEP functionalities. The management of the adhoc network is based on a distributed and hierarchal schema where delegation of management can be realized between various ad hoc network managers. Each manager can define its own policies that is constrained by the policies of the authoritative network manager. Managing access of users to the network and other systems is typically a slow and manual process. This is a challenging problem in particular because of the increased volatility due to node movements, connectivity changes, networks joining, and splitting, which necessitates frequent changes.

Policy-based network management allows administrators to define high-level security requirements, therefore allowing tools to automate the security management process.

REFERENCES

[1] Mouna Ayari, Farouk Kamoun, Davor Males “Towards a Policy-Based
Management for Ad Hoc Networks”
[2] Farooq Anjum and Petros Mouchtaris “Security For Wireless Ad Hoc Networks”
[3] Annie Ibrahim Rana Micheal O Foghlu Policy-based Traffic Management in Home Area Network –An Elementary Testbed Model
[4] M. Blaze, J. Feigenbaum, and J. Lacy, “Decentralized Trust Management,” Proceedings of the 17th IEEE Symposium on Security and Privacy, IEEE Computer Society, New York, 1996, pp. 164–173,
[5] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, “The KeyNote Trust-Management System Version 2,” IETF RFC 2704, September 1999.
[6] A. D. Keromytis, S. Ioannidis, M. Greenwald, and J. Smith, “The STRONGMAN Architecture,”DISCEX 20003, Washington, DC, April 2003.
[7] T. Markham and C. Payne, “Security at the Network Edge: A Distributed Firewall Architecture,”DISCEX 20001, California, June 2001.
[8] A.Lindfors, “Policy Based Management in Ad-hoc Networks”http://www.tml.hut.fi/Opinnot/Tik110.551/2000/papers/policy_management/internetworking.html
[9] J.Moffet,M.Sloman, “ Policy Hierarchies for distributed Systems Management” IEEE December 1993
[10] M.Solman, “ Policy Driven Management for Distributed Systems” Journal of Network and Systems Manegement, DEC1994
[11] Jorge Pena Cotarelo “Policy Based Management of overlay Networks” Sep 2010
[12] J. Wong, R. Hunt, “Policy Based Network Management”, Department of Computer Science, University of Canterbury, NewZealand, February 2003.

[13] J. Wong, R. Hunt, "Policy Based Network Management", Department of Computer Science, University of Canterbury, NewZealand, February 2003.
[14] K. S. Phanse, "Policy-Based Quality of Service Management in Wireless Ad Hoc Networks", Virginia Polytechnic Institute and State University, October 2002.
[15] A. Munaretto, N. Agoulmine, M. Fonseca, "Policy-based Management of Ad Hoc Entreprise Networks", 2001.
[16]D. Verma, "Policy-Based Networking: Architecture and Algorithms", Chapter 3, published November 2000.
[17]S. L. Keoh, E. Lupu, and M. Sloman, "Peace: A policy-based establishment of ad-hoc communities," in the Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC), September 2004, pp. 386–395.
[18] R. Boutaba and I. Aib. Policy-based management: A historical perspective. ACM Journal of Network and Systems Management, 15(4):447–480, December 2007.
[19] S. Boros. Policy-based network management with snmp. In Proceedings of EUNICE, pages 13–15. University of Twente, Netherlands, September 2000.
[20] R. Chadha et al, "Policy Based Mobile Ad hoc Network Management" 5th IEEE Intl. Work. on Policies for Distributed Systems and Networks
[21] M.Sloman, E. Lupu, "Policy Specification for Programmable Networks", Proceedings of First International Working Conference on Active Networks (IWAN'99), Berlin, June 1999