Title: SYSTEMS AND METHODS FOR SITUATION SEMANTICS BASED MANAGEMENT OF POLICY ENABLED COMMUNICATION SYSTEMS

Abstract: Communication nodes, systems and methods are described which manage and process management information using semantic variable entities governed by a formal logic and upon which computations can be performed. Such semantic variable entities include, for example, management Infos and or management situations which can be used, for example, to manage policy enforcement in communication networks.
Description

SYSTEMS AND METHODS FOR SITUATION SEMANTICS BASED MANAGEMENT OF POLICY ENABLED COMMUNICATION SYSTEMS

TECHNICAL FIELD

[1] The present invention generally relates to managing policies which control network resources in communications networks, and, more particularly, to situation semantics based management of such policies.

BACKGROUND

[2] Communication systems continue to grow and evolve. Convergence between different types of communication systems, e.g., Internet Protocol (IP), connection-based voice communications, and the like, is advancing rapidly. Recently the phrase "Next Generation Network" (NGN) has been used to describe various activities associated with this evolution. As defined by the International Telecommunications Union (ITU), an NGN is a packet-based network able to provide services (including telecommunication services) and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. NGNs will also likely offer unrestricted access by users to different service providers and will support generalized mobility, which in turn will provide for consistent service provision to end users.

[3] Various standardization groups are working on reaching a consensus regarding the technology considerations which will affect NGN design and implementation. For example, Telecommunications & Internet converged Services & Protocols for Advanced Networks (TISPAN) is an ETSI standardization group which focuses on convergence of technologies used in the Internet and other fixed networks. Among other things, TISPAN seeks to provide a modular, subsystem-oriented architecture which facilitates the addition of new subsystems over time to cover new demands and service classes. The TISPAN architecture attempts to ensure that network resources, applications, and user equipment are common to all of the various subsystems to provide for enhanced mobility across, for example, administrative boundaries.

[4] One of the TISPAN subsystems is referred to as the Network Attachment Sub System (NASS). The NASS is responsible for, among other things, handling configuration information, user authentication data, IP address allocation and registering associations between IP addresses allocated to user equipment (UE) and related network location information. These latter two NASS functions, i.e., allocating IP addresses and registering associations, are handled by the Network Access Con-
figuration Function (NACF) and the Connectivity Session Location and Repository Function (CLF), respectively, which are functional entities that are also specified by the NASS portion of the TISPAN standards.

[5] These NASS functional entities interact with another TISPAN subsystem known as the Resource Admission Control Subsystem (RACS) and, of particular interest for the present discussion, with the Access Resource and Admission Control Function (A-RACF) functional entity of the RACS. The A-RACF functional entity, among other things, receives information about the IP address allocated to a particular user and maps that IP allocation to physical resources in the access network. Each A-RACF is, in these exemplary embodiments, associated with a Session Border Controller (SBC). An SBC interacts directly with the network elements that provide communication services to an end user, e.g., Digital Subscriber Line Access Multiplexers (DSLAMs).

[6] Siloed management of communication systems has typically been based on a siloed structure which provides a dedicated management system for each network type as shown in Figure 1. The converged NGN networks described above (and other networks) are intended to be integrations of many different network types, each of which may itself include, for example, hundred of thousands of network elements, network diagnostics. Thus, management of such networks using, e.g., the siloed structure of Figure 1 becomes tremendously complex given that the network and its components are themselves highly self-configurable, dynamically adaptable to real-time conditions and highly autonomous. Moreover, the architectural evolution of these networks is characterized by the abandonment of so-called "stove-pipe" architectures in favor of service oriented architecture, in order to isolate changes and states from a service perspective and to hide operational specifics within a network domain.

[7] Accordingly, siloed management of communication systems suffers from a number of limitations and problems including, for example: that exponential growth in management requirements (frequent network changes, dynamic routing, differentiated services, new types of services like service degradation) makes service management more difficult; a lack of control of self-deployment and self-configuration aspects in policy enabled systems; lack of a standard way to track what is happening in policy based system such as NGN networks; that the end service can span multiple technologies and multiple domains; increasing need for multiple technologies to interact and be provided as seamless services (e.g., voice and Internet); current management information content is typically not fine grained enough to enable end-to-end service management; a lack of automatic diagnostics for end-to-end network problems; a lack of an automatic audit trail of end-to-end automated network activities; a lack of automatic linking of service problems to network problems; a lack of sound drill down method from an end-to-end view (e.g., a call) to local views (e.g., multiple connections
that make the call); a lack of a method to capture generalized service path tracing; a lack of techniques for call path tracing without formal representation; a lack of a formal framework to manage policies; a lack of a formal method of managing policies related of aspects of Service Level Agreements (SLAs); and a lack of formal representation of attempted and unsuccessful configuration.

Accordingly, it would be desirable to provide systems and methods for managing policy enabled communications systems which address the afore-described problems and drawbacks.

SUMMARY

According to an exemplary embodiment, a method for managing policy enforcement in a communications network includes storing instances of policy enforcement in the communications network as management infons; and managing policy enforcement in the communications network using the management infons.

According to another exemplary embodiment, a network node includes a processor for transmitting and receiving information, and a memory for storing management infons associated with policy enforcements which have occurred.

According to still another exemplary embodiment, a computer-readable medium contains instructions which, when executed on a computer, perform the steps of: storing instances of policy enforcement in the communications network as management infons; and managing policy enforcement in the communications network using the management infons.

According to yet another exemplary embodiment, a management situation data structure includes a plurality of management infons linked together to form the management situation, wherein the plurality of management infons jointly model a service provided by a network.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate one or more embodiments and, together with the description, explain these embodiments. In the drawings:

Figure 1 illustrates a conventional, stovepipe type of management architecture;

Figure 2 illustrates a non-stovepipe type of management architecture;

Figure 3 illustrates a non-stovepipe type of management architecture which includes a situation engine according to an exemplary embodiment;

Figure 4 illustrates reference points associated with interfaces between a situation engine, a policy server and a policy enforcer according to an exemplary embodiment;

Figure 5 depicts a relationship between a service, policies, management infons and a management situation according to an exemplary embodiment according to an
exemplary embodiment;
[19] Figure 6 is an exemplary embodiment illustrating a correspondence between aggregation points in a broadband network and management infons;
[20] Figure 7 illustrates an NGN network including a management infon repository according to an exemplary embodiment;
[21] Figure 8 is a flowchart illustrating a method for managing policy enforcement according to an exemplary embodiment; and
[22] Figure 9 illustrates a network node for generating and/or storing management infons according to an exemplary embodiment.

DETAILED DESCRIPTION

[23] The following description of the exemplary embodiments of the present invention refers to the accompanying drawings. The same reference numbers in different drawings identify the same or similar elements. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims.

[24] These exemplary embodiments provide methods and systems for managing information, e.g., policies that control network resources in, for example, a large communication network (e.g., cellular networks, etc.). As will be described below, these exemplary embodiments are based on the application of situation semantics theory in the area of information management, generally, and, more specifically, according to one exemplary embodiment, in the area of policy based network management and control to enable service semantics aware management and generalized service path tracing. For example, some embodiments describe a management paradigm which is applicable to any self-managing system through policy rules, such as NGN networks.

[25] Taking this more specific example first, NGN networks are designed to be policy enabled in order to provide easier operations and maintenance. For example, IMS and TISPAN network reference models include policy frameworks. According to exemplary embodiments, by using the policy management paradigm for communication systems, it becomes possible to overcome stove pipe architecture boundaries and enable unified management and control for converged networks as illustrated conceptually in Figure 2. Therein, Policy Decision Points (PDPs), which can be implemented as policy servers 200, are described in TISPAN networks as, for example, the Network Attachment Subsystems Architecture (NASS), the Access Resource and Admission Control Function (A-RACF) and the Service-based Policy Decision Function (SPDF). The RACS provides generic policy-based transport control services to applications as well as admission and gate control functionality. Policy Enforcement Points (PEPs) 210 are switching and routing transport components which can, for
example, include TISPAN components such as the Resource Control Enforcement Function (RCEF).

To provide some context, policy-based management is an enabling technology for dynamic and global control of large scale distributed system through rule-based policies. Policy-based management has, for example, been introduced in the Internet Engineering Task Force (IETF) to automate the network configuration process. The IETF management architecture introduces new elements in the network, some of which are shown in Figure 2: the policy server 200 (also referred to as a Policy Decision Point (PDP)), the policy client 210 (also referred to as a Policy Enforcement Point (PEP)) and the policy repository (not shown in Figure 2) where the policies are stored.

A policy transport protocol called the Common Open Policy Service (COPS) has been defined in RFC 2748 to support the interaction between the PDP 200 and its controlled PEPs 210. This management framework has been also adopted by, for example, standards bodies such as 3GPP, 3GPP2 and ETSI TISPAN with various differences regarding the interface between the PDP and the PEP.

In, for example, networks employing the "stove pipe" architecture of Figure 1 for network policy management and enforcement, it has been common to employ syntactical approaches toward managing the resulting information, e.g., using rule-based, action-based, case-based, model-based or probability based reasoning techniques. Such syntactical approaches, which focus on the form of the information rather than its meaning, are limited by, for example, the capability of the underlying syntax to capture the complexity of the information being managed and to, in effect, anticipate the types of management computations which may be desirable in the future to appropriately manage highly complex communication systems, such as NGN networks.

By way of contrast, these exemplary embodiments take a semantical approach toward managing information, e.g., relating to policy enforcement in communication networks. Using such a semantical approach, the meaning of the information being managed becomes part of what is captured and used to perform computations. For example, a data point's context and relationships can be captured and manipulated. For example, these exemplary embodiments exploit a semantical approach referred to as situational semantics to manage information. To better understand such situational semantical approaches, a brief discussion of information theory and situational semantics follows.

The theory of information as developed by Shannon is purely syntactical, see Shannon, CE., "A Mathematical Theory of Communication", The Bell System Technical Journal, Vol. 27, pp.379-423, 623-656, July, Oct. 1948. Various semantical approaches have been developed, such as the approach proposed by Carnap in "Meaning and Necessity", University of Chicago Press, 1947, which was based on a
version of possible words semantics to explain the system of intension and extensions. Hintikka explored the logic of knowledge and belief within a version of the possible worlds framework in Hintikka, J., "Knowledge and belief: an introduction to the logic of two notions", New York: Cornell University Press, 1962. More recent works introduced situation semantics in the early 1980s, for example, Barwise, Jon and Perry, John, " Situations and Attitudes", Cambridge, MA 1983, and Barwise, Jon, "The Situation in Logic", Stanford, 1988, which describe situation semantics as a mathematical theory of linguistic meaning. Development of situation semantics into a formal mathematical model of information flow through complex systems has been described by, for example, Jon Barwise and Jerry Seligman in "Information Flow. The Logic of Distributed Systems", Journal of Logic, Language and Information Volume 8, Number 3 / July, 1999.

A significant feature of the situation semantics model is the notion of an information channel which is capable of preserving information as it is transmitted through a complex, causally interacting system. The basic ontology includes:

- individuals, denoted by a, b, c…
- relations, denoted by P, Q, R…
- spatial locations, denoted by i, V, \( V \)…
- temporal locations, denoted by t, t', t''
- situations, denoted by s, s', s''…
- truth values: 1 (true) and 0 (false)

An "infon", or state-of-affair, as used in the situation semantic model and the exemplary embodiments described below is a computationally viable unit of semantic information content, i.e., a mathematical object used in situation semantics. An exemplary infon includes, for example, a relation, individuals, location, time and a polarity (i.e., a truth value) and can be expressed as:

(1) \( \langle R, \ a, \ b, \ c, \ d, \ e \rangle \)

For example, a simple infon can convey that certain objects stand in some relation or, alternatively, do not stand in that relation. Various examples of infons used, for example, to express relations between managed objects associated with policy enforcement in communications networks are provided below.

Another feature of situation semantic models is the "situation". A situation is another unit of information which is defined in such models to be a set or chain of infons. A characteristic of situation semantics theory is that the meaning (or semantics) is contextual, i.e., the meaning of an infon depends on a situation. The following proposition indicates that \( s \) supports \( \phi \):

(2) \( s \models \phi \)
this means that s is the real situation that makes the infon φ factual. In the context of situation semantic models or semantic methods for processing information, information relates to a situation, i.e., the context of the data. Situations are partial, in contrast with possible worlds which are total—this means they capture a part of the universe or a scene involving some individuals, relations, location and time. As with infons, various examples of situations as they can be applied to managing information, generally, and policy enforcement, more specifically, are provided below.

The objects of the situation semantic theory can be typed thereby allowing the building of complex entities. Examples of types are geographic locations (LOC), temporal locations (TIM), individuals (IND), situation (SIT) and n-place relations (REL). The following example provides a new type by type abstraction using parameter absorption:

\[
(3) \lambda x \, I_s \equiv 1
\]

Thus, equation (3) represents the type of x for which situation s supports the infons in the set of infons I. Parameter absorption in situation semantics theory is analogue of λ-abstraction (i.e., anonymous function of λ-calculus). From a computational perspective, situation semantics provides an informational approach to formal semantics where soundness and completeness are mathematically proven, see, e.g., Juan Barba Escriba, "Two Formal Systems for Situation Semantics", Notre Dame Journal of Formal Logic, Vol. 33 Number 1 1992.

Exemplary embodiments apply such situation semantics to the management and processing of information outside of the context of linguistics. Some exemplary embodiments will first be described with respect to the management and processing of information associated with communication networks, e.g., policy enforcement information. However, it will be appreciated that the present invention is not limited thereto. At a conceptual level, the application of situation semantics in the context of policy based network management can be illustrated as shown in Figure 3. Therein, a situation engine 300 provides a framework and mechanism for representing states-of-affairs using situation semantics for both successful policy enforcements in the illustrated network and, also, attempted but unsuccessful policy enforcements. The management situation semantics reference model according to this exemplary embodiment provides an extension of the afore-described policy based management model as shown in Figure 4. Therein, S_a is the reference point that defines the interface between the policy server(s) 200 and the policy enforcer(s) 210. Reference point Sa can, for example, be implemented as COPS (3GPP R5 - Gq/Go), Diameter (3GPP R7 Rx/Gx, 3GPP2 Tx/Ty, ITU-T Rs/Rw) or H.248 (TISPAN Gq/V1a). Similarly, S_b is the reference point that defines the interface between the policy enforcer(s) 210 and the situation engine 300 and S_c is the reference point that defines the interface between the
policy server(s) 200 and the situation engine 300. Both the Sb and Sc interfaces provide policy enforcement information in the format of management infons according to these exemplary embodiments. In some exemplary architectures a policy server 200 may control many policy en-forcement results. In such exemplary embodiments, the policy server 200 can inform the situation engine 300 by providing it with management infons reflecting the policy enforcement results. According to other exemplary embodiments, the policy server 200 may, for example, be a PEP for another policy server in the case of a network which is controlled with hierarchical policies.

The application of situation semantics to the management and processing of information according to these exemplary embodiment results in, among other things, the generation of, storing of and operations on, management infons. A management infon is a state-of-thing in network management. In some examples provided below, management infons are described which correspond to policy enforcements. The management infon states or conveys that a plurality of management objects in a network element (e.g., 3GPP MOs, TISPAN MOs, etc.) either stand in a particular relation or do not stand in that particular relation. The management objects (MOs) represent any network resources (e.g., network nodes, service nodes, time, etc.) and can, for example, include elements of the Network Resource Model (e.g., 3GPP/3GPP2 NRM) or the Management Information Base (e.g., IETF MIB). Additionally, management infons according to these exemplary embodiments may represent positive or negative states-of-affairs. This means that management infons can represent attempted and unsuccessful policy actions, i.e., actions that were not enforced for various reasons such as network conditions, e.g., congestion, etc., as well as successful policy enforcements.

Consider the following example of a management infon according to an exemplary embodiment. In this example, a management infon includes a relation, a plurality of MOs associated with a network which are related by the relation, and a polarity, and can be represented as:

(4) « streaming, Said, MusicServer; yes »
(5) « streaming, Said, Yassir, MusicServer; yes »

Management infon (4) states that two managed objects (i.e., a user (Said) and a Music Server) are related by a relation called streaming. Similarly, management infon (5) states that three managed objects are related by the streaming relation.

Management infons according to these exemplary embodiments can take various forms. For example, arguments of a management infon may be parameterized, as shown in (6):

(6) « streaming, x, MusicServer; yes »
Parameterized roles can be associated to individuals or managed objects. For example, management infon (6) becomes similar to management infon (4) if x is associated with Said. Likewise, parameterized infons can be restricted by other parameterized infons, as in management infon (7), where the subject role for the property of streaming is restricted to individuals who are subscribers:

\[(7) \langle \text{streaming}, x \in \text{subscriber}.x, \text{yes}\rangle; \text{yes} \rangle\]

Moreover, properties and relations can be produced from parameterized infons by absorbing parameters as illustrated below:

\[(8) \langle x \text{ streaming}, x, \text{MusicServer}; \text{yes} \rangle ]\]

where management infon (8) corresponds to the property of streaming music.

A management situation according to these exemplary embodiments is an infon chain which describes, e.g., policy events, in which the infons in the chain are anchored to, or associated with, a particular end-to-end (e2e) service. Note that the meaning of e2e is contextual and can, for example, refer to the end-user of the service or an "end" with respect to any network service or a component of the network service (e.g., a transport network service). Each particular context is determined by a set of infons that set a particular view of the service. Thus, a plurality of management infons linked together form a management situation data structure, wherein the plurality of management infons jointly model a service provided by a network. For example, if the service spans two domains within a network, a corresponding management situation can be generated by management infons from nodes within the two domains upon provisioning of the service. The management situation data structure can be stored in a computer-readable medium, as described below.

An exemplary relationship between a service, policies and a management situation according to an exemplary embodiment is shown in Figure 5. Therein, it can be seen that a particular service 500 has policies and actions associated therewith. When these policies are enforced, they result in the generation of corresponding infons which are associated with the management situation 502 that corresponds to service 500. The generation of infons within block 502 can be performed by the situation engine (which can also be called an infon engine) 300. For example, as shown in Figure 5, Policy 1 triggers one action (action1) which, in turn, generates a corresponding management infon (infon1). Policy2 triggers two actions (action21 and action22) which, in turn, generate a composite management infon (infon2) which is made of two infons (infon21 and infon22). Similarly, in this example, Policy3 triggers one action (action3) and then one infon (infon3) and Policy4 triggers one action (action4) and then one infon (infon4).

To further understand the usage of management infons and management situations to this exemplary embodiment of policy management in a communication network,
consider the following example of a policy-enabled broadband optical communication network which includes many different nodes with different capabilities. These nodes provide, for example, fiber switching capability (FSC), e.g., nodes such as fiber cross-connects, lambda switching capability (LSC), e.g., nodes such as optical cross-connects, time-division-multiplex capability (TDMC), e.g., nodes such as SONET cross-connects, Layer 2 packet switching capability (PSC), e.g., MPLS routers or ATM switches, and Layer 3 packet switching capability (PSC) e.g., IP routers. In this exemplary network a service is offered which is called "Set up a Packet LSP", wherein the acronym LSP refers to Label Switched Path, i.e., a path defined in the context of MPLS or GMPLS technologies. An instance of this service will be associated with a management situation called packetLSP. Note that in this example the overlap between the GMPLS Control Plane and the Management Plane is not considered to provide simplicity to this example.

As shown in Figure 6, this exemplary network has a plurality of different aggregation points. Suppose that the first aggregation point 600 is implemented as an ATM cross connect that enforces an aggregation policy of music streaming flows on a dedicated LSP. The corresponding management infon can be expressed as:

\[
(9) \ i_1 = \text{aggregation, LSP1, ATM_MOC; MusicUsersVIOC } \ \ \ i_{\text{core}} \ \ \ \text{MuxServer, yes} \]

where MusicUsers_MOC is the managed object that represents flows of music streaming users. At the second aggregation point 602, there is, for example, a first photonic switch which enforces an aggregation policy on LSC LSP. The corresponding management infon can be expressed as:

\[
(10) \ i_2 = \text{aggregation, LSP2, Lambda_IOC, yes} \]

The third aggregation point is associated with a second photonic switch which enforces an aggregation policy on FSC LSP. The corresponding management infon for this aggregation point can be expressed as:

\[
(11) \ i_3 = \text{aggregation, LSP3, Fiber_IOC, yes} \]

The corresponding management situation packetLSP is the chain of the three management infons (9)-(11), i.e.:

packetLSP = \text{ `I}_1, \text{ I}_2, \text{ I}_3` \]

This management situation provides the service trace path of all users that are streaming music in this optical broadband network. An impairment in either an LSC LSP or in an FSC LSP can be traced back to the impacted users by the situation engine 300 (sometimes also referred to herein as the infon engine). A similar set of management infons and corresponding management situation can be generated for the splitting points 606, 608 and 610 in the network of Figure 6.

To provide another example of the usage of management infons and management
situations according to these exemplary embodiments, consider an access and a core network which are operated with an adaptive QoS provisioning system based on a model called DiffServ. Applications which provide service on this access and core network will have different quality levels. The policy server 200 may decide upon congestion and business rules to downgrade certain application traffic classes from a higher class to a lower class. Since the DiffServ model provides only a statistical guarantee of QoS, if there is no reservation of resources in the network, the deployment of situation semantics based management according to these exemplary embodiments will facilitate analysis of the end-to-end QoS status of certain critical services from local policy enforcements using management infons such as the following:

(12) « voip, user1, DSCPMarker(EF), Routerl;tl, yes »
(13) «voip, user2, DSCPMarker(EF), Routerl, tl, no»
(14) «voip, user2, DSCPMarker(AF32), Routerl, tl, yes»
(15) «voip, user1, DSCPMarker(AF42), Routerl, t2, yes»

Management infon (12) is an infon that corresponds to the set up of a per-hop-behavior (PHB) configuration for a voice-over-IP (VoIP) service. The Expedited Forwarding PHB (EF) provides the user with a guaranteed minimum percentage of the link that will be allocated to his or her VoIP connection, which is a useful quality control feature for real time applications that require a guarantee on the delay and jitter, like telephony service. Management infon (13) states that user2 was not able to obtain a PHB configuration with Expedited Forwarding value. This latter infon provides an example of how management infons according to these exemplary embodiments provide a computationally viable mechanism for capturing negative relations as well as positive relations. Negative relations are desired but not realized while position relations are realized.

Management infon (14) states that another policy triggered the PHB configuration to Assured Forwarding (AF). The Assured Forwarding PHB (AF) specifies four classes of traffic, and each of those classes is guaranteed a minimum amount of bandwidth and buffering, which guaranteed amount is better than the common best-effort service, providing low packet loss within a given traffic rate, but making minimal guarantees about latency of the packets. Within each AF class, there are three drop precedences. Management infon (14) conveys the information that user2 gets AF32 (i.e., which indicates AF class 3 with a medium drop precedence). Management infon (15) states that, at a later point of time t2, a policy has been activated, e.g., following a network congestion, which has downgraded user1 to AF42 (AF class 4 with medium drop precedence).

Having provided some specific examples of management infons and management
situations according to exemplary embodiments, the focus now returns to higher level aspects of these exemplary embodiments. NGN architecture enables policy control as shown in, for example, Figure 7. Therein, multiple instances of RACFs 700, 702 and 704 may exist since the access network 706 and/or the core network 708 may be made of multiple domains, each having their own RACF. A consumer premises equipment (CPE) 710 is provided with various services by one or more application functions 712. According to exemplary embodiments, the NGN Operations Support System (OSS) 714 can be enriched by the situation semantics engine described above to manage the policies enforced in the network by the RACF (Resource and Admission Control Functionality). For that purpose the TISPAN Management Information Model (MIM), which models all relevant TISPAN NGN management entities, can be evolved to include the aforementioned management situation semantics model. In such context, management situations could, for example, each comprise a set of management infons issued by the PEPs of the access transport network and the PEPs of the core transport network, which describe an end-to-end service behavior in the network. The management infons could, for example, be stored in an infon repository 716.

Thus, a method for managing policy enforcement in a communications network according to an exemplary embodiment can include the steps illustrated in the flowchart of Figure 8. Therein, at step 800, instances of policy enforcement in the communications network are stored as management infons, e.g., in an infon repository 716. Next, at step 802, policy enforcement in the communications network is managed using the management infons. Various types of calculations can be performed on the management infons to generate data for managing policy enforcement. For example, infons associated with a significant user (customer) or a significant node can be monitored to monitor, e.g., using the truth flag value in management infons, the negative policy enforcements which occur with respect thereto.

Management infons can be stored and manipulated in one or more nodes of a system, e.g., a communication system. An exemplary node 900 will now be described with respect to Figure 9. Node 900 can include a processor 902 (or multiple processor cores), memory 904, one or more secondary storage devices 906 and an interface unit 908 to facilitate communications between network node 900 and the rest of the network. Additionally, the node 900 can also include protocols allowing communications over the potentially different available interfaces through which it may communicate. The memory 904 (or the secondary storage device) can be used for storage of management infons and/or management situations, either in a database or in another manner.

Systems and methods for processing data according to exemplary embodiments of the present invention can be performed by one or more processors executing sequences
of instructions contained in a memory device. Such instructions may be read into the memory device from other computer-readable mediums such as secondary data storage device(s). Execution of the sequences of instructions contained in the memory device causes the processor to operate, for example, as described above. In alternative embodiments, hard-wire circuitry may be used in place of or in combination with software instructions to implement the present invention.

[48] As mentioned above, exemplary embodiments relate to policy-based network management which includes, among other things, the use of delineated policies to control access to, and priorities for the use of, network resources and services including, for example, active QoS (Quality of Service) and network service-level-agreement provisioning.

[49] The foregoing description of exemplary embodiments provides illustration and description, but it is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. The following claims and their equivalents define the scope of the invention.
Claims

1. A method for managing policy enforcement in a communications network comprising:
   - storing instances of policy enforcement in said communications network as management infons; and
   - managing policy enforcement in said communications network using said management infons.

2. The method of claim 1, wherein each of said management infons is a mathematical object containing semantic information content.

3. The method of claim 2, wherein said semantic information content of each management infon is partially determined by each management infon's relationship to other management infons within a management situation.

4. The method of claim 1, wherein each of said management infons includes a relation and a plurality of managed objects.

5. The method of claim 4, wherein at least some of said management infons include a truth value.

6. The method of claim 5, wherein at least some of said management infons include a location and a time value.

7. The method of claim 1, wherein storing of instances further comprises:
   - storing said management infons in an infon repository database.

8. The method of claim 1, wherein said managing policy enforcement further comprises:
   - performing calculations on said management infons.

9. The method of claim 8, wherein said performing of calculations further comprises:
   - identifying, for a particular user or node within said communication network, each negative policy enforcement associated therewith.

10. The method of claim 1, further comprising:
    - generating management situations as chains of said management infons, each of said situations being associated with a service provided within said communication network.

11. A network node comprising:
    - a processor for transmitting and receiving information; and
    - a memory for storing management infons associated with policy enforcements which have occurred.

12. The network node of claim 11, wherein each of said management infons is a computationally viable unit of semantic information content.
13. The network node of claim 12, wherein said semantic information content of each management infon is partially determined by each management infon's relationship to other management infons within a management situation.

14. The network node of claim 11, wherein each of said management infons includes a relation and a plurality of managed objects.

15. The network node of claim 14, wherein at least some of said management infons include a truth value.

16. The network node of claim 15, wherein at least some of said management infons include a location and a time value.

17. The network node of claim 11, wherein said memory stores said management infons in an infon repository database.

18. The network node of claim 11, wherein said processor performs calculations on said management infons.

19. The network node of claim 18, wherein said performing of calculations further comprises:
   - identifying, for a particular user or node within a communication network, each negative policy enforcement associated therewith.

20. The network node of claim 11, wherein said processor generates management situations as chains of said management infons, each of said situations being associated with a service provided within said communication network.

21. A computer-readable medium containing instructions which, when executed on a computer, perform the steps of:
   - storing instances of policy enforcement in said communications network as management infons; and
   - managing policy enforcement in said communications network using said management infons.

22. The computer-readable medium of claim 21, wherein each of said management infons is a computationally viable unit of semantic information content.

23. The computer-readable medium of claim 22, wherein said semantic information content of each management infon is partially determined by each management infons relationship to other management infons within a management situation.

24. The computer-readable medium of claim 21, wherein each of said management infons includes a relation and a plurality of managed objects.

25. The computer-readable medium of claim 24, wherein at least some of said management infons include a truth value.

26. A management situation comprising:
- a plurality of management infons linked together to form said management situation, wherein said plurality of management infons jointly model a service provided by a network.

[27] 27. The management situation of claim 26, wherein said service spans multiple domains and technologies within said network and said management situation is generated upon provisioning said service by linking together management infons from nodes within said multiple domains and technologies.

[28] 28. The management situation of claim 26, wherein each of said management infons is a computationally viable unit of semantic information content.

[29] 29. The management situation of claim 28, wherein said semantic information content of each management infon is partially determined by each management infon's relationship to other management infons within said management situation.
START

STORE INSTANCES OF POLICY ENFORCEMENT AS MANAGEMENT INFONS

MANAGE POLICY ENFORCEMENT USING THE MANAGEMENT INFONS

END
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

INV. H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC.

**B. RELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched.

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, IBM-TDB, INSPEC, COMPENDEX

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No</th>
</tr>
</thead>
</table>

* Further documents are listed in the continuation of Box C

* See patent family annex

**Date of the actual completion of the international search**

24 March 2009

**Date of mailing of the international search report**

06/04/2009

**Name and mailing address of the ISA/**

European Patent Office, P B 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Fax (+31-70) 340-3016

**Authorized officer**

Cichra, Michael
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3GPP: &quot;Policy and charging control architecture&quot; 3GPP TECHNICAL SPECIFICATIONS, no. TS23.203V7.5.0, 1 December 2007 (2007-12-01), pages 1-72, XP002520821 paragraph [6.2.1] paragraph [6.2.2]</td>
<td>1-29</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>US 2002101826 A1</td>
<td>01-08-2002</td>
<td>NONE</td>
</tr>
<tr>
<td>US 2003005034 A1</td>
<td>02-01-2003</td>
<td>NONE</td>
</tr>
</tbody>
</table>