ENM: A Service Oriented Architecture for Ontology-Driven Network Management in Heterogeneous Network Infrastructures

Saber Zrelli *, Atsushi Ishida †, Nobuo Okabe * and Fumio Teraoka †

* Yokogawa Electric Corporation
Musashino, Tokyo, 180-8750, Japan
Email: Saber.Zrelli,Nobuo.Okabe@jp.yokogawa.com

† Graduate School of Science and Technology, Keio University
Yokohama, Kanagawa, 223-8522, Japan
Email: dolin,tera@tera.ics.keio.ac.jp

***Abstract*—Heterogeneous network infrastructures have always been part of the public Internet as well as production systems in enterprise and industrial environments. The coexistence of multiple communication technologies and systems from multiple vendors still represents management cost and reliability challenges mainly due to the lack of interoperability at the network management plane. In this paper, we outline the main challenges that organizations face in managing large scale multi-technology and multi-vendor heterogeneous network infrastructures. We then propose the ENM (Extended Network Management) framework, a scalable and extensible service oriented architecture for deploying ontology-driven network management services adapted for large scale heterogeneous infrastructures. The ENM framework defines the different entities involved in deploying ontology-driven network management services and specifies a scalable and flexible communication protocol, based on Diameter (RFC3588), between these entities. To demonstrate the feasibility of the proposed framework, a proof of concept was implemented and deployed on a small scale test-bed.**

***Index Terms*—Network Management, Ontology, Distributed Middleware, SOA.**

I. Introduction

Network management is a fundamental activity which enables network operators and managers to plan, organize, supervise, control and account for the use of the networking infrastructure and services. Such activities allow network managers to ensure predictable communication behaviors, and allow them to respond to changing requirements [1]. The increasing size of network infrastructures and the increasing adoption of new communication technologies brings new challenges that traditional network management paradigms may not be able to address.

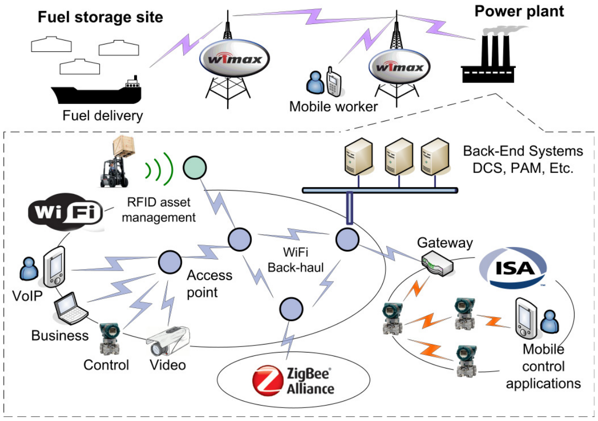

Fig. 1. Heterogeneous Network Infrastructures in Industrial Automation

Recently, established and emerging industries started to leverage wireless communication technologies in various applications. The International Society for Automation (ISA) recently released the ISA100.11a [2] specification, a technology based on IEEE 802.15.4 [3] for wireless communications in industrial applications. Besides ISA100.11a, several wireless technologies such as WirelessHART [4], IEEE 802.11 [5] and IEEE 802.16 [6] are being gradually introduced in industrial plants resulting in heterogeneous wireless infrastructures such as the one illustrated in Figure 1. Each of these technologies, as shown in Figure 2, has different characteristics (e.g., range and data rate) and serves a different need. As shown in Figure 1, WiFi plays an essential role in industrial plants. Besides acting as an access network for various applications such as voice over IP (VoIP) and video surveillance, WiFi is used as a back-haul connecting other wireless systems to the infrastructure (as shown in Figure 1, ISA100.11a gateways equipped with WiFi interfaces can be used to connect an ISA100.11a network to the WiFi back-haul). IEEE 802.15.4 based technologies with reliable and power efficient radio interfaces such as ISA100.11a and WirelessHART, on the other hand, are used for connecting sensors and actuators to field gateways.

978-1-4673-0269-2/12/$31.00 © 2012 IEEE

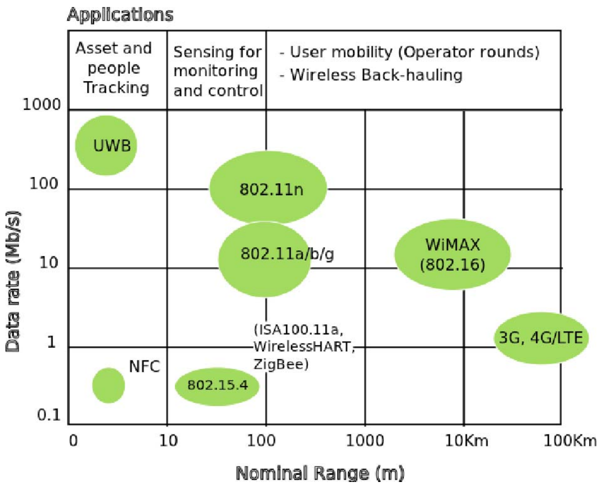

Fig. 2. Wireless Technologies used in Industrial Automation

The use of multiple communication technologies for fulfilling different needs in such application domains results in large scale heterogeneous network infrastructures where different technologies from different vendors need to coexist. This paper is concerned about the costs and reliability of traditional management paradigms in such heterogeneous network infrastructures.

The ontology-driven network management paradigm [7] [8] which leverages adaptive and autonomic techniques on top of semantic ontologies is suitable for addressing management issues in heterogeneous network infrastructures. However, there is lack of research regarding deployment aspects of ontology-driven network management techniques in real life situations.

The goal of this paper is to provide a scalable and secure framework for deploying ontology-driven network management services. The framework specifies methods and protocols for exchanging network management information between different entities involved in network management operations including network management applications, a network management knowledge base and the managed infrastructure nodes.

In the remaining of this paper, we discuss costs and reliability issues related to the management of heterogeneous network infrastructures in section II. In section III, where the ENM (Extended Network Management) framework is presented, we start by describing the role of the ENM framework in enabling the deployment of ontology-driven network management services. We then describe the different entities specified by the ENM framework. In section IV, we describe the service oriented communication architecture used in the ENM framework which leverages the Diameter protocol [9] for its scalability and inter-domain capabilities. In section V, we present a proof-of-concept prototype of the ENM architecture described in this paper. Finally, in the conclusion, we provide a summary of the paper and outline our future research items.

II. Problem Statement: Managing Issues in Large Scale Heterogeneous Network Infrastructures

Heterogeneous network infrastructures that include different networking technologies from different vendors are complex systems to manage. The root cause of the complexity is the diversity in network management technologies and the scale of the infrastructure. Both of these aspects lead to cost and reliability issues.

Diversity of network management technologies is due to two main reasons. First, different communication technologies use different network management protocols. For example, network management technologies traditionally used to manage a WiFi infrastructure such as SNMP [10], NetConf [11] and CAPWAP [12] are different from network management technologies used in industrial wireless networks such as ISA100.11a. The other reason for diversity in network management technologies is that different network equipment vendors (even vendors of the same communication technology such as ISA100.11a) provide different network management software and likely different network management protocols.

Besides diversity in network management technologies, the scale of the networking infrastructure also constitutes a main concern that increases the complexity of management operations. This concern is particularity relevant in industrial automation where heterogeneous network infrastructures may include hundreds of thousands of devices that need to be managed [13].

The management costs and reliability issues resulting from heterogeneity and large scale constitute a burden that limits the cost savings and productivity improvement potential sought after by integrating various network communication technologies in production systems such as in the case of Industrial Automation. The following sections provide an overview of these costs and reliability issues (summarized in Table I).

A. Management Cost Issues

Network system vendors provide software and training that allow the infrastructure owner to manage the network system after the commissioning phase is over. Such software can be used to manage only the equipment provided by the same vendor. In heterogeneous network infrastructures where different network equipment and network management software are provided by different vendors, the infrastructure owner has to use different network management software to manage the whole infrastructure.

The costs incurred from the multitude of network management software include not only the cost of the different software but also the training costs and the cost of human resources that will be using the software.

Most network management operations such as investigating an alarm, fine tuning configuration settings or upgrading a network node, still require manual intervention by a network administrator. For this reason, the larger the infrastructure becomes the more network administrators are needed, and the more technical support from outside is needed, which translates in additional costs for the infrastructure owner.

TABLE I
ISSUES IN MANAGING LARGE SCALE HETEROGENEOUS NETWORK INFRASTRUCTURES

Category of Issues	**Infrastructure Characteristics**	
	Heterogeneity	**Scale**
Cost Issues	Cost of purchasing multiple management software, training and staff.	The larger the infrastructure the more staff is needed.
Reliability Issues	Delays in manually mitigating coexistence issues due to multitude of management systems.	- Traffic generated from continuous monitoring may generate network bottlenecks. - Delays in diagnosing and mitigating end-to-end communication issues involving multiple management domains.

B. Management Reliability Issues

In heterogeneous infrastructures where different wireless systems are deployed to fulfill various application needs, day to day management operations such as solving coexistence problems due to spectrum scarcity are not obvious [14]. The lack of tools and frameworks for a centralized access to network status and configuration data in the deployed wireless systems may result in conflicts in resource assignments. For example, if the assignment of radio frequency channels is not coordinated properly among the co-existing wireless systems, radio interference issues may arise and communications may be disrupted.

The centralized management of a networking infrastructure involves exchange of network management data with the managed network nodes. Depending on the needs, the network management system may have to communicate with each device in a frequent manner (every second, minute or hour) to maintain up-to-date information about the infrastructure. The traffic generated by such communications may represent additional management burden and if not managed well may cause bottlenecks and reliability issues in the infrastructure as well as the network management system.

Another reliability issue related to infrastructure scale is the dynamic management of end-to-end communications across multiple administrative domains. Manually exchanging network management information between management systems in different administrative domains could be a complicated task and may be subject to delays due to security and authorization related processing. For this reason, the management of end-to-end communications in multi-domain settings may represent reliability challenges.

III. THE EXTENDED NETWORK MANAGEMENT FRAMEWORK

A. Ontology-Driven Network Management

Ontology-driven network management has been the subject of several studies such as IBM's autonomic computing architecture [7] and Motorola's FOCALE project [8]. The ability of ontologies to facilitate the storage of semantic knowledge and reasoning has enabled wider spread of adaptive and autonomic techniques including in network management.

The automation of network management operations is now generally accepted as the adequate approach to address network management issues in heterogeneous network infrastructures. However, most of the existing works focus on analysis and planning aspects and there is still lack of research regarding the deployment of such network management services in real life heterogeneous network infrastructures.

The network management architecture proposed in this paper, hereafter referred to as the "Extended Network Management Framework (ENM)" aims at facilitating the deployment of ontology-driven network management services for addressing network management issues in large scale heterogeneous network infrastructures. The ENM framework leverages two technologies, namely ontologies as data and knowledge representation platform and the Diameter protocol [9] as a scalable and extensible multi-domain communication framework.

B. Overview of the ENM Framework

As depicted in Figure 3, the ENM framework defines four main components; *ENM Applications*, *ENM Middleware Services*, *ENM Knowledge Base* and *ENM Data Interfaces*. ENM Applications are specialized network management applications used by network management operators to perform network management operations (such as QoS diagnosis and mitigation, security audit, provisioning, etc.). ENM Applications rely on ENM Middleware Services which provide common functionalities such as data path resolution and access to data link configuration information.

The ENM Knowledge Base is responsible for storing data and semantics needed by ontology-driven network management applications. To access the ENM Knowledge Base, ENM Middleware Services and ENM Applications use an extension to the Diameter protocol defined by the ENM framework called *Diameter ENM application*.

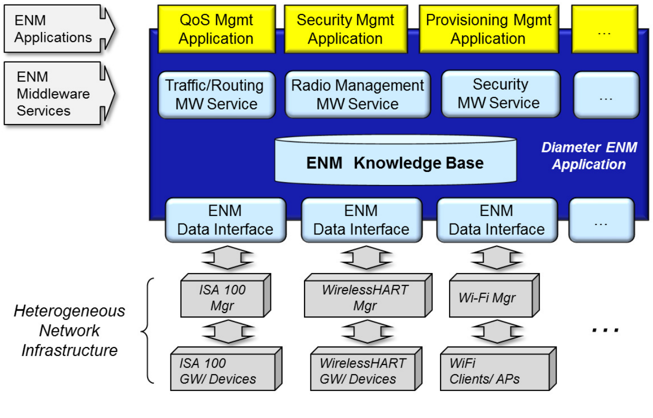

Fig. 3. The Extended Network Management (ENM) Framework

It is the role of the ENM Knowledge Base to provide information on current status and configuration information for all managed network objects. For that purpose, the ENM Knowledge Base maintains network configuration and status information synchronized with the infrastructure. The exchange of information between the ENM Knowledge Base and the infrastructure is carried out through the ENM Data Interfaces. These interfaces are used for reading and writing network management information to and from the infrastructure. The Diameter ENM application is also used for communication between the ENM Knowledge Base and ENM Data Interfaces.

C. The ENM Knowledge Base

Network management operations rely on data and know-how for fault management and preventive maintenance. The ENM Knowledge Base provides access to network management data, including various status and configuration information. The information is organized in a structured form (ontologies) to enhance its machine processability by network management diagnosis and mitigation algorithms.

Besides the storage of up-to-date network management status and configuration information, the ENM knowledge Base uses ontologies to store semantics useful for network management operations. Such semantics include properties such as cause and effect relationships between certain network management configurations and potential network management issues (such as performance and security issues). The ENM Framework does not specify a particular network management ontology. The only requirement is that the ontology is represented using the *Web Ontology Language (OWL)* [15].

The ENM framework leverages the latest World Wide Web Consortium (W3C) standards for the Semantic Web [16], namely OWL [15] for representing ontologies in the ENM Knowledge Base and the SPARQL ontology query language [17] for accessing the ontologies. The SPARQL protocol was originally specified for accessing ontologies in read only mode. More recently, an extension to SPARQL called SPARQL/Update (also known as SPARUL) [18] was specified to add features for writing data and semantics to ontologies.

The combination of the expressive power of OWL and the flexible querying capabilities of SPARQL allows querying for facts that are not explicitly asserted in the ontology, and that require the use of deduction and inference by the knowledge base [19]. This aspect is a key feature for implementing network management algorithms that can deal with complex and large scale infrastructures. The inference capabilities necessary for executing SPARQL queries are assumed to be provided by the knowledge base framework being used (e.g., JENA [20]).

D. The ENM Data Interfaces

The ENM framework defines services called ENM Data Interfaces to distribute the exchange of network management data between the infrastructure and the centralized ENM knowledge base. Each ENM Data Interface is deployed on a separate host and communicates both with the ENM Knowledge Base and with a subset of managed network objects. The ENM framework does not impose a particular partitioning policy of the network infrastructure among ENM Data Interfaces. Such partitioning could be based on technology or on geographical location, for example.

The ENM Knowledge Base issues read and write requests to the ENM Data Interface which translates the requests into a format understandable by the target managed object. The request is then forwarded to the managed network object using the appropriate protocol. Such protocol could be, for example, SNMP [10], NetConf [11] or any other protocol supported by the managed network object for remote management operations. When the ENM Data Interface receives information from a managed network object, the information is forwarded to the ENM Knowledge Base.

The distribution of network management data exchange between the centralized ENM Knowledge Base and the infrastructure through the use of the ENM Data Interfaces prevents the ENM Knowledge Base from becoming a bottleneck when the ENM framework is used in large scale infrastructures.

E. ENM Applications and ENM Middleware Services

The ENM Applications, with which the network administrator interacts for carrying out fault management, network monitoring and maintenance, are problem oriented and leverage abstraction and semantic information in the ENM Knowledge Base to provide machine assistance in otherwise complex diagnosis and mitigation operations. In other words, the reasoning modules for addressing specific network management aspects are part of the ENM Applications.

Common functions needed by the ENM Applications such as the determination of the data path (the list of intermediary nodes) in an end-to-end communication, or the utilization trend of a given resource are implemented as independent services called ENM Middleware Services.

The ENM Middleware Services also act as an interface between ENM Applications and the ENM Knowledge Base for the exchange of raw data. The interface role allows the implementation of role-based access control and authorization on the ENM Knowledge Base. Each request for accessing the knowledge base by an ENM Application is authenticated and authorized by the ENM Middleware Service in charge of that category of information before allowing it through.

The ENM Middleware Services, acting as shared service providers accessible over the network, facilitate the deployment of new ENM Applications and provide the benefits of a Service Oriented Architecture (SOA).

IV. Communications in the ENM Framework

Communication between the different entities in the ENM Framework (ENM Applications, ENM Middleware Services, ENM Knowledge Base and ENM Data Interfaces) is carried out over the Diameter protocol [9]. The Diameter protocol can be considered as a session layer protocol (layer 5 of the OSI model) implemented over TCP/IP, traditionally used for authentication, authorization and accounting of network services. The ENM Framework specifies an extension to the Diameter protocol using Diameter's own extension mechanism called *Diameter applications* to transport messages between the different ENM entities which act as Diameter peers [9]. The extension specified by the ENM framework, called the *Diameter ENM application*, defines the message formats and the rules for processing each message.

A. The Diameter Protocol

Diameter [9] is the next generation authentication, authorization and accounting framework that aims at replacing the well known RADIUS protocol [21]. As a AAA framework, Diameter is originally designed to transport AAA information between different entities in the network. Each authentication, authorization or accounting protocol specifies an extension of the Diameter base protocol. Such extensions, called *Diameter applications* include Diameter-EAP application [22], Diameter-SIP application [23] and Diameter-MIPv6 application [24] for enforcing network access control, managing SIP services and bootstrapping Mobile IPv6, respectively.

The basic role of Diameter is to transport command request and answer messages. Each command request/answer pair is assigned a command code that identifies the type of the command and the payload carried by the Diameter message. The Diameter command code as well as other fields part of the Diameter message are carried in Attribute Value Pairs (AVPs). Diameter applications that extend the Diameter base protocol define new commands. This consists of defining new command codes, and the list of AVPs for each command request and answer message.

B. The Diameter ENM application

The ENM framework leverages Diameter as a scalable and extensible transport framework for communications between the different entities in the ENM framework (ENM Applications, ENM Middleware Services, the ENM Knowledge Base and the ENM Data Interfaces).

The typical flows of information in the ENM Framework are illustrated in Figure 4. For the downward direction (direction from ENM Application to the managed network object), the Diameter ENM application enables ENM entities to issue two types of requests. Fist, requests to write configuration data, used when the ENM Application or ENM Middleware Service needs to change the configuration of the infrastructure. Second, ENM entities may issue requests to read network configuration or status data. For the upward direction (direction from the managed network object to the ENM Application), the Diameter ENM application enables ENM entities to report on the result of a write operation and transport responses to read requests. Also, ENM entities can use the write requests to spontaneously issue an update to another ENM entity upon a change of network status or configuration information.

All ENM requests for reading and writing information from or to the ENM Knowledge Base are authenticated and authorized accordingly. For this purpose, the Diameter ENM application uses the Extensible Authentication Protocol (EAP) [25] for carrying-out authentication against a back-end authentication server.

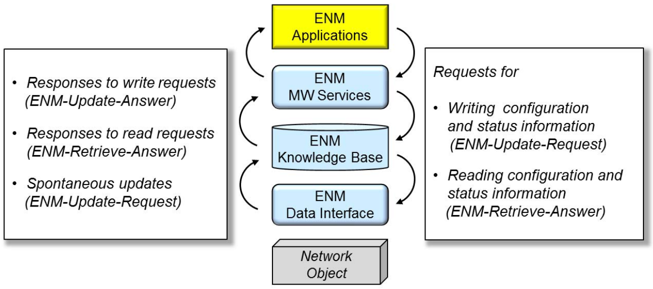
ENM Applications
ENM MW Services
ENM Knowledge Base
ENM Data Interface
Network Object
• Responses to write requests (ENM-Update-Answer)
• Responses to read requests (ENM-Retrieve-Answer)
• Spontaneous updates (ENM-Update-Request)
Requests for
• Writing configuration and status information (ENM-Update-Request)
• Reading configuration and status information (ENM-Retrieve-Answer)

Fig. 4. Diameter ENM messages

The Diameter ENM application provides possibilities for "push" and "pull" modes of communication using two commands for reading and writing network management data. To implement these commands, the Diameter ENM application defines the Attribute Value Pairs (AVPs) and messages illustrated in Table. II and Table. III.

Requests for reading information consists of an ENM-Retrieve-Request message carrying a SPARQL query as specified in [17]. If an ENM Middleware Service receives such request from an ENM Application, the ENM Middleware Service authorizes the ENM Application and forwards the request as it is to the ENM Knowledge Base. The ENM Knowledge Base also issues such requests to ENM Data Interfaces for reading network configuration and status information from the infrastructure. The ENM Data Interface translates the SPARQL request into a request understandable by the target network object then forwards the request to the network object over the communication medium.

As a response to an ENM-Retrieve-Request message, the ENM Knowledge Base as well as the ENM Data Interface issue ENM-Retrieve-Answer messages to communicate the desired information to the requesting entity. The SPARQL response message as specified in [17] is carried in a SPARQL-RESP AVP.

For writing information or issuing notifications, ENM entities issue an ENM-Update-Request message which contains a SPARUL request as specified in [18]. If the ENM entity receiving the message is an ENM Knowledge Base, the request is processed by applying the changes to the local ontologies and forwarding the same request to the appropriate ENM Data Interface for effectively making the change on the infrastructure. When an ENM Data Interface receives an ENM-Update-Request message, it translates the SPARUL request into a request understandable by the target network objects before forwarding it. ENM Middleware Services process ENM-Update-Request messages either by processing the message locally or by forwarding the request to an ENM Application if the ENM Middleware Service is acting as an interface to the ENM Knowledge Base. The ENM entity receiving an ENM-Update-Request message issues an ENM-Update-

TABLE II
DIAMETER ENM AVPS

AVP Name	Content
SPARQL-REQ	A SPARQL request.
SPARQL-RESP	A SPARQL response.
SPARUL-REQ	A SPARUL request.
SPARUL-RESP	Carries the outcome from processing of an ENM-Update-Request message.
EAP-REQ	An EAP request message as defined in [25].
EAP-RESP	An EAP response, success or failure message as defined in [25].

TABLE III
DIAMETER ENM MESSAGES

Command / Message	Main AVP
ENM-Retrieve-Request	SPARQL-REQ
ENM-Retrieve-Answer	SPARQL-RESP
ENM-Update-Request	SPARUL-REQ
ENM-Update-Answer	SPARUL-RESP
ENM-Auth-Request	EAP-REQ
ENM-Auth-Answer	EAP-RESP

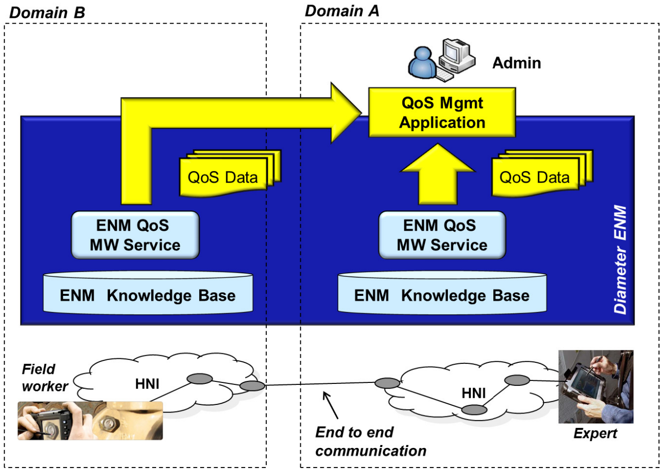

Fig. 5. ENM Support for inter-domain end-to-end communications

Answer message to inform the requesting entity about the outcome from processing the ENM-Update-Request message.

Besides the core commands described above used for exchanging data, each ENM Middleware Service defines its own commands and AVPs to deliver its services to ENM Applications. Such commands and AVPs can be easily integrated into existing ENM frameworks without breaking inter-operability since the changes extend the Diameter ENM application and do not imply modification of existing commands and AVPs that are already in use.

To ensure authentication and to enforce access control on information and services, each communication session between two ENM entities is authenticated using the ENM-Auth-Request and ENM-Auth-Response messages which carry EAP payloads. Thanks to the transparency provided by EAP, any EAP method, such as such as EAP-TLS [26], could be used for achieving mutual authentication between the two entities.

C. Inter-domain Operations

The ENM framework is intended to support large scale heterogeneous network infrastructures that span across multiple management domains. For this purpose, the ENM framework leverages inter-domain capabilities of the Diameter protocol for connecting ENM Applications and ENM Middleware Services from different domains.

Figure 5 illustrates an example of ENM inter-domain operations for managing an end-to-end communication that involves two separated administrative domains. In the example scenario, a field worker in an industrial automation setting is using a multimedia system (video/audio) to send video to a maintenance expert located in a remote site. The maintenance expert examines the troubled asset using the streamed high definition video and guides the worker using voice over IP.

To ensure the reliability of the end-to-end communication, an ENM Quality of Service (QoS) Management application is deployed. The ENM QoS Management application uses the ENM framework to obtain QoS information (list of intermediary nodes, load on intermediary nodes, etc.) from the ENM QoS Middleware services in both domains involved in the communication.

To collect QoS information about the intermediary nodes in the remote domain, the ENM QoS Management application uses the Diameter ENM application to communicate with the ENM QoS Middleware Service in the remote domain. In order to route the messages to the remote ENM Middleware Service, the ENM QoS Management application uses the Destination-Realm AVP [9] to specify the domain to which the Diameter ENM messages are destined. The Diameter base protocol as specified in [9] will use the pre-configured or dynamically configured realm routing table to forward the message to the appropriate host in the remote domain.

The realm-based routing, originally specified for addressing the needs of inter-domain AAA operations, provides a reusable mechanism for connecting network management systems such as the ENM framework in different administrative domains, enabling more centralization and automation in the management of federated network infrastructures.

V. PROOF OF CONCEPT: PROTOTYPING THE ENM FRAMEWORK

In order to validate the concept of the ENM framework and investigate its feasibility, we implemented a prototype for monitoring quality of service (QoS) information in a heterogeneous network infrastructure.

In the proof of concept implementation, we used the open source freeDiameter [27] implementation of Diameter and JENA, the open source ontology framework [20]. To emulate a heterogeneous network infrastructure composed of multiple infrastructures based on different technologies, the test-bed that we used has two infrastructures, however, both are based on IP technologies due to hardware constraints (Figure 6).

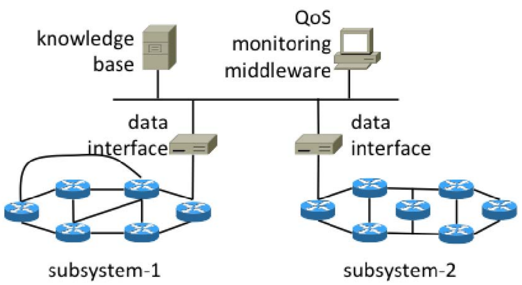

Fig. 6. The prototyped QoS monitoring system

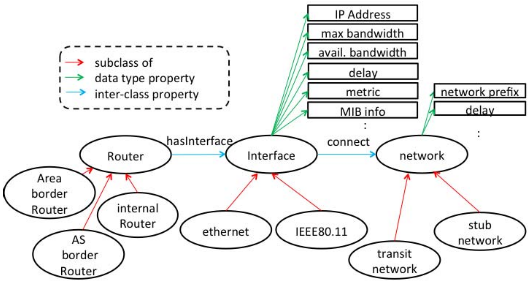

Fig. 8. Network ontology

A. Diameter ENM Application

The Diameter ENM Application described in Section .IV-B is used in the communication between the data interface and the JENA knowledge base and between the knowledge base and the QoS monitoring middleware. As shown in Figure 7, authentication and authorization procedure is executed between the data interface and the knowledge base and between the QoS monitoring middleware and the knowledge base using the ENM-Auth-Request and the ENM-Auth-Answer messages.

After authentication and authorization, the data interface updates the information in the knowledge using the EMN-Update-Request and the ENM-Update-Answer messages. The QoS monitoring middleware then retrieves the information in the knowledge base using the ENM-Retrieve-Request and the ENM-Retrieve-Answer messages.

B. Data Interface

In both infrastructures deployed in the test-bed, OSPF is used as the routing protocol. The data interface learns the network topology by accessing the OSPF link state database in the managed devices. Since the subsystems are based on IP technologies, the data interface uses SNMP to obtain information from each router. SNMP was used to periodically read the bandwidth of each interface and the number of bytes transmitted to each interface in the managed routers. From this information, the data interface calculates the consumed bandwidth of each link between each router pair and updates the knowledge base using the Diameter ENM application.

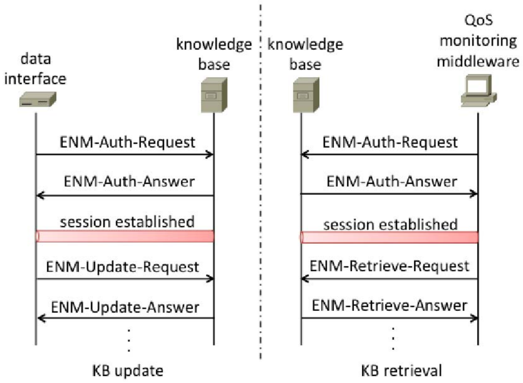

Fig. 7. Message exchanges in the QoS monitoring system using the prototyped Diameter ENM Application

C. Knowledge Base

In this proof of concept, the network information is represented in an ontology as shown in Figure 8. There are three class hierarchies: the `router` class hierarchy, the `interface` class hierarchy, and the `network` class hierarchy. Each class has several subclasses such as the `AS border router` class under the `router` class and the `Ethernet` class under the `interface` class. The `router` class and the `interface` class are connected by the `hasInterface` property. The `interface` class and the `network` class are connected by the `connect` property. The `router` class has several data type properties such as the max bandwidth and the available bandwidth. The `network` class has several data type properties such as the network prefix.

D. QoS Monitoring Middleware/Application

The QoS monitoring middleware (QoSMW, for short) acts as an ENM Middleware Service with integrated ENM Application functionalities (graphic interface) allowing a network administrator to monitor and diagnose QoS issues.

QoSMW retrieves network topology information and QoS information such as available bandwidth and delay from the knowledge base using the Diameter ENM application. If the administrator wants to know the data path between two routers that satisfies some QoS property, e.g., 10 Mbps of bandwidth and minimum delay, the QoSMW first removes the links from the network topology that do not have available bandwidth more than 10 Mbps. Next, the QoSMW calculates the shortest path in term of delay using the Dijkstra's algorithm. Figure 9 shows a screen capture of the QoSMW interface.

VI. Conclusion

The costs and reliability issues in managing large scale heterogeneous networks constitute a burden that limits cost savings and productivity improvement potential sought after by integrating various network communication technologies in production systems such as in the case of Industrial Automation.

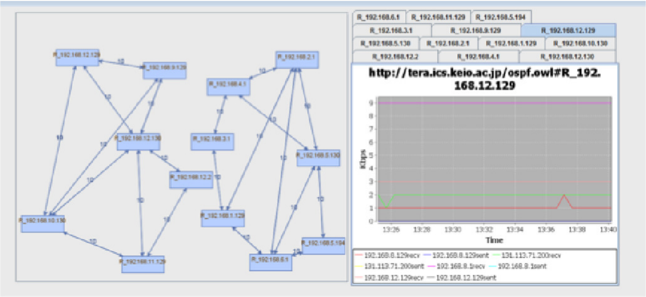

Fig. 9. Screen capture of QoSMW

The automation of network management operations is now generally accepted as the adequate approach to address network management issues in large heterogeneous network infrastructures. The use of ontologies as a core technology for automating network management operations has been the subject of several studies such as IBM's autonomic computing architecture [7] and the FOCALE project [8]. Such works are focused on knowledge engineering aspects by defining the role of ontologies in automated network management and describing the control loop [7] necessary for achieving autonomous networks. However, there is still lack of research regarding the deployment of such network management services in real life infrastructures.

The ENM framework complements existing works on cognitive and autonomous networking by providing a scalable deployment framework for ontology-driven network management systems. The ENM framework defines the different entities involved in deploying ontology-driven network management services (ENM Applications, ENM Middleware Services, ENM Knowledge Base and ENM Data Interfaces) and specifies a scalable and flexible communication protocol (the Diameter ENM application) between these entities.

We have demonstrated the feasibility of the ENM framework by implementing a prototype featuring the main components using available open source software. In our future works, we intend to incorporate more advanced network diagnosis and mitigation mechanisms by leveraging latest advances in the field of cognitive and autonomous networking. Also, we intend to deploy our prototype in a heterogeneous, multi-technology network environment.

References

[1] International Organization for Stanradization (ISO), "ISO/IEC 4798-4: Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 4: Management Framework," 1989.

[2] The International Society for Automation (ISA), "ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications," 2011.

[3] "IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," IEEE Standards, 2009.

[4] International Electrotechnical Commission (IEC), "IEC 62591 WirelessHART- Industrial communication networks - Wireless communication network and communication profiles," 2011.

[5] "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Standards, 2007.

[6] "IEEE 802 Part 16: Air Interface for Broadband Wireless Access Systems," IEEE Standards, 2009.

[7] International Business Machines Corporation (IBM), "An Architectural Blueprint for Autonomic Computing," 2005.

[8] Strassner, John and Agoulmine, N. and Lehtihet, E., "FOCALE: A Novel Autonomic Networking Architecture," in *Latin American Autonomic Computing Symposium (LAACS)*, 2006.

[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588 (Proposed Standard), Internet Engineering Task Force, Sep. 2003, updated by RFCs 5729, 5719, 6408. [Online]. Available: http://www.ietf.org/rfc/rfc3588.txt

[10] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411 (Standard), Internet Engineering Task Force, Dec. 2002, updated by RFCs 5343, 5590. [Online]. Available: http://www.ietf.org/rfc/rfc3411.txt

[11] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," RFC 6241 (Proposed Standard), Internet Engineering Task Force, Jun. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6241.txt

[12] P. Calhoun, M. Montemurro, and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," RFC 5416 (Proposed Standard), Internet Engineering Task Force, Mar. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5416.txt

[13] Shell Global Solutions, "CNOOC and Shell Petrochemicals Company Limited (CSPC) - Nanhai project," 2006.

[14] D. A. Roberson, C. S. Hood, J. L. LoCicero, and J. T. MacDonald, "Spectral Occupancy and Interference Studies in support of Cognitive Radio Technology Deployment," in *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, sept. 2006, pp. 26 –35.

[15] World Wide Web Consortium (W3C), "OWL 2 Web Ontology Language Document Overview," *http://www.w3.org/TR/owl2-overview/*, 2009.

[16] T. Berners-Lee, J. Hendler, and O. Lassila, "The Semantic Web," *Scientific American Magazine*, 2001.

[17] World Wide Web Consortium (W3C.), "Sparql query language for rdf," *http://www.w3.org/TR/rdf-sparql-query/*, 2008.

[18] World Wide Web Consortium (W3C), "SPARQL 1.1 Update," *http://www.w3.org/TR/sparql11-update/*, 2011.

[19] M. Kohar, M. Brady, and K. Baclawski, "Roles of Ontologies in Radios ," *Cognitive Radio Technology*, 2006.

[20] B. McBride, "Jena: a semantic web toolkit," *Internet Computing, IEEE*, vol. 6, no. 6, pp. 55 – 59, nov/dec 2002.

[21] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865 (Draft Standard), Internet Engineering Task Force, Jun. 2000, updated by RFCs 2868, 3575, 5080. [Online]. Available: http://www.ietf.org/rfc/rfc2865.txt

[22] P. Eronen, T. Hiller, and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," RFC 4072 (Proposed Standard), Internet Engineering Task Force, Aug. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4072.txt

[23] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales-Valenzuela, and K. Tammi, "Diameter Session Initiation Protocol (SIP) Application," RFC 4740 (Proposed Standard), Internet Engineering Task Force, Nov. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4740.txt

[24] J. Korhonen, J. Bournelle, H. Tschofenig, C. Perkins, and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction," RFC 5447 (Proposed Standard), Internet Engineering Task Force, Feb. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5447.txt

[25] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), Internet Engineering Task Force, Jun. 2004, updated by RFC 5247. [Online]. Available: http://www.ietf.org/rfc/rfc3748.txt

[26] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," RFC 5216 (Proposed Standard), Internet Engineering Task Force, Mar. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5216.txt

[27] S. Decugis and F. Teraoka, "freeDiameter: An Open Source Framework for an Authentication, Authorization, and Accounting Infrastructure," *JSSST Computer Software*, vol. 28, no. 4, 2011.