International Journal For Technological Research In Engineering
Volume 2, Issue 8, April-2015 *ISSN (Online): 2347 - 4718*

A SURVEY ON ISSUES AND CHALLENGES FOR QUALITY OF SERVICES PROVISIONING IN HETEROGENEOUS MILITARY NETWORKS

Pravalika.S[1], P. I. Basarkod[2]
Dept of Electronics and Communication
Reva Institute of Technology and Management, Bangalore, India

Abstract: ***Military networks are evolving today towards complex heterogeneous networks with various subnetworks in terms of architecture, protocols and security. But QoS provisioning in military networks is a very challenging problem when compared to wired IP networks. This is because of unpredictable node mobility, wireless multi-hop communication, contention for wireless channel access, limited battery power and range of mobile devices as well as the absence of a central coordination authority. In this paper, we examine the major issues and challenges that must be solved in order to provide efficient QoS provisioning and also explains the security over heterogeneous networks. Finally we describe cooperation between QoS and security systems and QoS over heterogeneous networks.***

Index Terms: Quality of service (QOS), Heterogeneous Networks (HN), End-to-End delay (E2E), QoS routing.

I. INTRODUCTION

IN recent years there has been a growing desire to always be connected, and to provide network access to individual war-fighters. To accommodate this need, networks with different characteristics (e.g., transmission technologies, protocols, policies, etc.) must be connected. The consequence is that the resulting network is very heterogeneous, and that heterogeneous networks eventually will become the norm for military tactical mobile networks as it is for strategic networks and in the Internet. The heterogeneous networks (HN) may include both wired and wireless components. At a higher level, heterogeneity may refer to different network policies as well as trust and security management. In tactical military networks the potentially relatively large variation in available network resources and the potentially very low data rates, imply that it is challenging to solve efficient end-to-end (E2E) quality of service (QoS) provisioning in these networks. The importance of providing end-to-end QoS over heterogeneous networks is widely discussed in the related work, in particular if applied to the IP world. Reference [4] states that "The network operators are willing to open up their network resources to innovative new service providers, which include mechanisms for supporting end-to-end QoS guarantees (across multiple domains), and for the flexible and dynamic creation of new services". The norm that medium to large-scale wireless tactical networks are heterogeneous. This incorporates sub networks with significant diversity in terms of latency, data-rate, robustness, traffic load, and so forth. To provide a reliable network for different operation types and in varying terrains, a tactical mobile network infrastructure must consist of a variety of wireless network types, e.g., long-range communication for reach-back connections and a higher bandwidth network for local communication. It is important to be able to combine different radio systems in an operation to provide an efficient and robust network, and in order to improve information flow between neighbourhood partners. Such network of networks will be better utilized, and multiple transmission technologies and routing paths will improve communication reliability by providing alternative routing paths. In this network, the resources will vary and efforts to minimize the signalling traffic in low capacity networks must be taken. The traffic load can often overtake the capacity of the heterogeneous network. It is therefore crucial to support end-to-end QoS and prioritization of operation critical traffic. It is also important to use the network resources in an optimal manner for the mission and thus make sure that only traffic that has a high chance of reaching the destination is admitted into the network. The remaining part of the paper is organized as follows: Section II point to related work. Section III discusses QoS overview in military HN. Issues and challenges in providing QOS in military HN in section IV, section V explains enhancing security over heterogeneous networks, the cooperation between QoS and security systems is explained in section VI and QoS over heterogeneous networks is explained in section VII and in the final section we present the summary.

II. RELATED WORK

Provision of E2E QoS is an important challenge in the area of HN. Many QoS-enabled architectures and protocols have been proposed to solve the problem of end-to-end quality of real-time audio/video and high quality data services. The AQUILA project [5] suggested distributed QoS middleware for the single domain homogeneous IP network. One of the achievements of the project was leveraging the concept of traffic classes, redirection from IntServ to DiffServ architecture and use of BB (Bandwidth Broker). In the EuQoS project [6] a heterogeneous scenario with five different technologies of access networks was considered. The Classes of Service (CoS) proposed were based on the DiffServ concept. The QBone project [7] conducted research in the field of QoS provisioning for the global IP network i.e. multi-domain scenario. The architecture proposed by QBone team was built on DiffServ architecture with Bandwidth Broker. The proposed architectures of the referenced EU

projects are more or less based on the DiffServ IP model. As far as this model is concerned four alternatives are taken into account: no control (where only a basic priority mechanism is applied), static trunks, DiffServ-PCN (Pre Congestion Notification), and BB, not available in the market for now but a great potential for QoS management. In the presented solutions emphasis is put on traffic management, bandwidth optimization, Call Admission Control (CAC), QoS signalling protocols and network planning. The presence of QoS signalling protocols, as RSVP-TE [9], is essential. Mapping the QoS requirements over the different private technologies is a topic for QoS management. The same concept applies if CAC is considered. If there are no signalling schemes to manage resources dynamically, the Service Level Specification (SLS) support is left to the experience of network operators at network planning level. The mentioned QoS architectures are all designed with the focus of E2E QoS support in cellular mobile networks and in fixed networks with several network service providers. However, military tactical networks differ from the typical heterogeneous networks found in civilian infrastructure due to their features such as frequent topology changes, mobility of users and service providers, common use of wireless links, multi-hop wireless paths, relatively low data rates, large variation in maximum available data rate, and limited processing and power capacity of network nodes. The trust relation between network partners is also different in a coalition than between commercial network providers, and the Service Level Agreements (SLAs) can have a different role (not a contractual agreement of quality and cost, but more an approximate agreement of willingness to make resources available). The traffic pattern in the different networks can also be quite different. Mariann Hauge et.al proposed different design of the mechanisms, and by suggesting an interaction between a Multi Topology (MT) routing protocol used in the mobile tactical environment and the QoS provisioning framework running in the tactical backbone. The MT routing protocol is an intra-domain QoS routing protocol. QoS-routing aims to find a route which provides the required service quality for a specific traffic type. This can be done using routing metrics based on parameters like delay, data rate, signal to noise ratio, route stability, etc. These protocols must be combined with a resource manager and a traffic classifier (e.g., DiffServ-like classification) to support QoS in the network. However, most of the QoS-routing schemes are reactive routing protocols. Proactive protocols will be necessary in tactical networks to reduce the routing response time and increase the predictability of the network availability. It is beneficial in a very heterogeneous environment to store several routes with different characteristics to support separate QoS requirements. The multi-topology supported QoS architecture [9] that Mariann Hauge et.al utilizes a simple but powerful scheme with a proactive routing protocol that maintains multiple topologies in the routing domain and consequently provides multiple paths from source to destination. Each topology/path is associated with a single or multiple QoS-class (es).

III. OVERVIEW OF QUALITY OF SERVICE IN HETEROGENEOUS NETWORKS

Quality of service (QoS) is the performance level of a service offered by the network to the user. The goal of QoS provisioning is to achieve more deterministic network behaviour, so that information carried by the network can be better delivered and network resources can be better utilized. A network or a service provider can offer different kinds of services to the users. Here, a service can be characterized by a set of measurable pre specified service requirements such as minimum bandwidth, maximum delay, maximum delay variance (jitter), and maximum packet loss rate. After accepting a service request from the user, the network has to ensure that service requirements of the users flow are met, as per the agreement, throughout the duration of the flow (a packet stream from the source to the destination). In other words, the network has to provide a set of service guarantees while transporting a flow. After receiving a service request from the user, the first task is to find a suitable loop-free path from the source to the destination that will have the necessary resources available to meet the QoS requirements of the desired service. This process is known as QoS routing. After finding a suitable path, a resource reservation protocol is employed to reserve necessary resources along that path. QoS guarantees can be provided only with appropriate resource reservation techniques. QoS provisioning often requires negotiation between host and network, call admission control, resource reservation, and priority scheduling of packets. QoS can be rendered in HNs through several ways, viz., per flow, per link, or per node. In HNs, the boundary between the service provider (network) and the user (host) is not defined clearly, thus making it essential to have better coordination among the hosts to achieve QoS.

As different applications have different requirements, the services required by them and the associated QoS parameters differ from application to application. For example, in case of multimedia applications, bandwidth, delay jitter, and delay are the key QoS parameters, whereas military applications have stringent security requirements. For applications such as emergency search and rescue operations, availability of network is the key QoS parameter. Applications such as group communication in a conference hall require that the transmissions among nodes consume as minimum energy as possible. Hence battery life is the key QoS parameter here. Unlike traditional wired networks, where the QoS parameters are mainly characterized by the requirements of multimedia traffic, in AWNs the QoS requirements are more influenced by the resource constraints of the nodes. Some of the resource constraints are battery charge, processing power, and buffer space. The position of the QoS system in the network is shown in Fig. 1. QoS architecture consists of the following main elementary parts: QoS identification, QoS classification, QoS congestions management mechanism, and QoS management mechanism, which handle the queue.

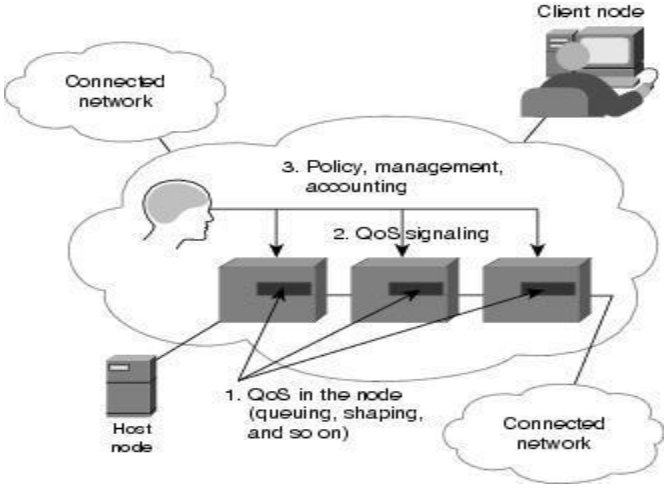

Figure 1: Quality of Service

A. QoS Routing Protocols

QoS routing protocols search for routes with sufficient resources in order to satisfy the QoS requirements of a flow. The information regarding the availability of resources is managed by a resource management module which assists the QoS routing protocol in its search for QoS feasible paths. The QoS routing protocol should find paths that consume minimum resources. Reliability or availability of a link, based on some criteria such as link break-probability is a multiplicative metric. Finding an optimal path with multiple constraints may be an NP-complete problem if it involves two or more additive metrics. To assist QoS routing, the topology information can be maintained at the nodes of HNs. The topology information needs to be refreshed frequently by sending link state update messages, which consume precious network resources such as bandwidth and battery power. Otherwise, the dynamically varying network topology may cause the topology information to become imprecise. This trade-off affects the performance of the QoS routing protocol. As path breaks occur frequently in HNs compared to wired networks where a link goes down very rarely, the path satisfying the QoS requirements needs to be recomputed every time the current path gets broken. The QoS routing protocol should respond quickly in case of path breaks and re-compute the broken path or bypass the broken link without degrading the level of QoS.

IV. ISSUES & CHALLENGES IN PROVIDING QOS

Providing QoS support in HNs is an active research area. HNs have certain unique characteristics that pose several difficulties in provisioning QoS. A detailed discussion on how the characteristic of HNs affects QoS provisioning is given below:

- Dynamically varying network topology: Since the nodes in an ad hoc wireless network do not have any restriction on mobility, the network topology changes dynamically. Hence the admitted QoS sessions may suffer due to frequent path breaks, thereby requiring such sessions to be re-established over new paths. The delay incurred in re-establishing a QoS session may cause some of the packets belonging to that session to miss their delay targets/deadlines, which is not acceptable for applications that have stringent QoS requirements.
- Imprecise state information: In most cases, the nodes in an ad hoc wireless network maintain both the link-specific state information and flow-specific state information. The link-specific state information includes bandwidth, delay, delay jitter, loss rate, error rate, stability, cost, and distance values for each link. The flow specific information includes session ID, source address, destination address, and QoS requirements of the flow (such as maximum bandwidth requirement, minimum bandwidth requirement, maximum delay, and maximum delay jitter). The state information is inherently imprecise due to dynamic changes in network topology and channel characteristics. Hence routing decisions may not be accurate, resulting in some of the real-time packets missing their deadlines.
- Lack of central coordination: Unlike wireless LANs and cellular networks, HNs do not have central controllers to coordinate the activity of nodes. This further complicates QoS provisioning in HNs.
- Error prone shared radio channel: The radio channel is a broadcast medium by nature. During propagation through the wireless medium the radio waves suffer from several impairments such as attenuation, multi-path propagation, and interference (from other wireless devices operating in the vicinity).
- Hidden terminal problem: The hidden terminal problem is inherent in HNs. This problem occurs when packets originating from two or more sender nodes, which are not within the direct transmission range of each other, collide at a common receiver node. It necessitates retransmission of packets, which may not be acceptable for flows that have stringent QoS requirements. The RTS/CTS control packet exchange mechanism, proposed in [2] and adopted later in the IEEE 802.11 standard, reduces the hidden terminal problem only to a certain extent. BTMA [3] and DBTMA provide two important solutions for this problem.
- Limited resource availability: Resources such as bandwidth, battery life, storage space, and processing capability are limited in HNs. Out of these, bandwidth and battery life are very critical resources, the availability of which significantly affects the performance of the QoS provisioning mechanism. Hence efficient resource management mechanisms are required for optimal utilization of these scarce resources.
- Insecure medium: Due to the broadcast nature of the wireless medium, communication through a wireless channel is highly insecure. Hence security is an important issue in HNs, especially for military

and tactical applications. HNs are susceptible to attacks such as eavesdropping, spoofing, denial of service, message distortion, and impersonation. Without sophisticated security mechanisms, it is very difficult to provide secure communication guarantees.

A. QOS Challenges

In a military tactical network, one or several of these networks might be a very heterogeneous where mobility can lead to reduction and/or renegotiation of QoS parameters. QoS mechanisms that can adapt to the rapid changes of the QoS characteristics of the E2E path traversing a heterogeneous network domain also needs to be addressed. QoS routing and admission control are among the parameters that are to be discussed here. It should be noted, also, that provision of end-to-end QoS cannot be realized without routing based on valid resource information and resource management and with connected security mechanisms.

Taking this into consideration, the following QoS challenges should be taken into account:

- Signalling: In a multi-domain network, it is imperative to install and manage QoS in each domain. The need is to transfer QoS requirements among network portions implementing their own technologies and protocols. The signalling protocol used to signal the requirements should be designed to rapidly cope with changes in the network topology, and thus end-to-end QoS conditions. In order to increase the robustness of the different connections in the network, the protocol must:
- release resources reserved for a specific traffic-flow if the flow disappears for a certain period of time and
- provide alternative routes to the destination in case of node failure or congestion in the network. Therefore signalling across all domains on the data-path is needed.
- Cross-layer QoS mapping: The data network is composed of functional layers where each layer must cooperate to support end-to-end QoS provision. The overall perceived service quality depends on the QoS achieved at each layer of the network. The QoS requirements at the application layer should be classified into a set of QoS classes with their corresponding application layer metrics. The QoS requirements must flow vertically across the layers and need to be received, understood and satisfied by all layers in the network stack. Therefore a vertical mapping of QoS metrics is critical. If the different layers do not cooperate to support a QoS requirement, but instead choose their best support for the required QoS independent of each other, there is a risk that the layers can in the worst case, select to use mechanisms that undermine each other. Cross-layer mechanisms can be used both to improve QoS support internal in homogeneous networks, but also to provide relevant QoS/resource information between networks in a heterogeneous network.
- QoS routing: Military HN (MHN), are very dynamic in their nature due to the use of mobile nodes and radio resources. The time-varying low-capacity resources of the HNs, which is very often a basic part of a military heterogeneous network, make maintaining accurate routing information very difficult.
- Intra-domain routing: The network layer maintains the end-to-end path whereas the MAC layer is in charge of access to the medium for the next hop on the path. The path selection and the channel access must aim to support the same QoS requirement for the data packet. It is also beneficial to maintain multiple paths/topologies with different QoS characteristics in the network.
- Inter-domain routing: The border routers must be able to automatically reconfigure their routing daemons in order to support end-to-end QoS over deployable networks composed of multiple autonomous systems that can move relative to each other.

V. ENHANCING SECURITY OVER HETEROGENEOUS NETWORKS

Without adequate security, unauthorized access and usage may violate QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposure. The physical medium of communication is inherently insecure, so it is important to design aware routing algorithms for heterogeneous networks. Because of the difficult properties of mobile wireless networks there has been a suggestion of using soft QoS. The definition of Soft QoS is that after a connection setup, there may exist transient periods of time when QoS specifications is not honored. However we can quantify the level of QoS satisfaction by the fraction of total disruption time over the total connection time. This ratio should not be higher than a threshold. QOS adaptation can be done in several layers. The physical layer should take care of changes in transmission quality, for example by adaptively increasing or decreasing the transmission power. Similarly, the link layer should react to the changes in link error rate, including the use of automatic repeat request (ARQ). A more sophisticated technique involves an adaptive error correction mechanism that increases or decreases the amount of error correction coding in response to changes in transmission quality of desired QoS. As the link layer takes care of the variable bit error rate, the main effect observed by network layer will be a change in effective throughput (bandwidth) and delay.

VI. COOPERATION BETWEEN THE QOS AND SECURITY SYSTEMS

Security is considered as another dimension of QoS parameters, in addition to data rate, packet loss rate, delay, and pricing. Consider a videoconferencing application between the army's field commanders and generals in the

Pentagon that requires high security properties, which include user authentication, message authentication, user access control, an effective encryption key length, and high quality of services. The last property includes high video quality with low delay, at the minimum cost. The objective of the QOS network is to make the cooperation between the two systems more effective. For example, when the QoS system receives a very large amount of incoming traffic from the same source or for the same destination, the QoS system alerts the security system to verify whether the network is being under attack, and concurrently keeps the log file of that traffic for future analysis. The security system can automatically allow some critical QoS information to be served with the highest security service degree.

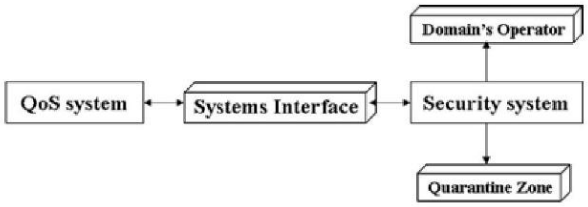

Figure 2: Cooperation between the QoS and security systems.

From Figure 3, the quarantine zone is deployed to keep some packets marked as suspicious as attacking packets while waiting for the user's confirmation. The cooperation between the QoS and security systems is classified into two types:

1. Active cooperation is referred as to when the network tries to prevent the QoS performance from deterioration caused by some specified attacks. Several researches, have addressed QoS attack scenarios, suggested detection methods, and proposed the solutions. In summary, several counter-attack schemes can be proposed based on this active cooperation.

2. Passive cooperation is referred as to when the victim from the attack and authorities attempt to regain information recorded during the attack and to trace the true identity of the attacker. The security system may also be integrated or cooperated with Intrusion Detection System (IDS) to detect ongoing attacks more efficiently. If there are suspicious activities, such as a large amount of traffic generated by a single source or destined to a single destination, the QOS system alerts the security system with in-depth information about involved traffic and the AS administrator is also informed. Early attack information can be recorded such that countermeasures or tracking processes can be rapidly performed. The system interface translates the messages exchanged between the two systems to make messages understandable to each other. Moreover, the AS administrator can configure directly the security system on-line by using router command packets, in emergency cases, especially while being under attacks. Depending on the application QOS is an essential parameter, especially in tactical networks: Digital battlefields have different settings from the existing communication networks and the constantly-changing tactical environment may demand many real-time needs in both data collection and data delivery. Talking about QOS with regards to security, two mainly orthogonal matters are considered: Firstly, data payload has different priority and thus, some packets should have an higher claim on network resources than other packets. Furthermore, there are requirements for multi-level priority and pre-emption as discussed. Because of the importance of QOS in military environments, many proposals for Military oriented QoS (M-QoS)-mechanisms have been made on the past few years. Secondly, real-time applications delivering voice, for instance, requires a short and constant packet delay. Both requirements of the transmission technology as well as the delivered service have to be considered carefully. Roughly speaking, one could remark that, it is a good practice that the employed security schemes should not affect the QOS more than the transmission technology does itself.

VII. QOS OVER HETEROGENEOUS NETWORK

The QoS architecture in military tactical networks must consist of a set of mechanisms and solutions for the mobile tactical edge and a set of mechanisms and solutions for the deployed backbone and its connections to the strategic network. The mechanisms must interact very well. In this section we describe a possible architecture for providing connectivity and differentiated QoS support in heterogeneous mobile tactical networks. The purpose of this solution is to exploit the existence of parallel paths in the network to support differentiated QoS. It is assumed that the heterogeneous network might consist of radios based on different transmission technologies (capacity, range, delay, etc.). The purpose of the design is to find the path that traverses the group of transmission technologies that best suits the requirement of a traffic class. In the current phase this solutions supports multiple networks organized in a single domain, but it can also be extended to support multiple domains. The suggested solution defines multiple routing topologies in the network in order to support different QoS-classes. These topologies are then used to ensure that data packets are only forwarded on topologies with sufficient capabilities to support the requirements of the dataflow. We combine Multi-Topology (MT) routing and traditional DiffServ-like mechanisms to utilize all available transmission means in the tactical network and increase the robustness of the network.

VIII. SUMMARY

With emerging standards such as 5G, and the convergence of the telecom and Internet industries on IP-based technologies, the ability to provide high QoS has become paramount. In this paper several issues and challenges are discussed in the literature for QoS provisioning in military networks which involves the queuing protocols and security enhancement system for supporting quality of service. Provision of E2E QoS is an important challenge in the area of heterogeneous military networks and the importance of providing end-to-end QoS over heterogeneous networks widely discussed in this paper.

REFERENCES

[1] Mariann Hauge , Lars Landmark, Piotr Lubkowski, Marek Amanowicz and Krzysztof Maslanka, "Selected Issues of QoS Provision in Heterogeneous Military Networks", International Journal of Electronics and Telecommunicatons,2014.
[2] T.Bheemaruna Reddy, I. Karthigeyan, B.S. Manoj, C. Siva Ram Murthy,"Quality of service provisioninh in ad hoc wireless networks: a survey of issues and solutions", ELSEVIER, Ad Hoc Networks,2006.
[3] Md. Zahirul Islam, Md. Mirza Golam Rashed, " A Comparative analysis on traditional Queuing ang Hybrid Queuing Mechanisms of VOIP's QoS Properties", International Journal Of Advance Innovations, Thoughts & Ideas.
[4] S. Giordano, S. Salsano, S. Van den Berghe, G. Ventre, and D. Giannakopoulos, "Advanced QoS Provisioning in IP Networks: The European Premium IP Projects," IEEE Communications Magazine, vol. 41, no. 1, pp. 30–37, January 2003.
[5] AQUILA – Adaptive Resource Control for QoS Using an IP-based Layered Architecture, Project Number: IST-1999-10077, http://wwwst.inf.tu-dresden.de/aquila/.
[6] EuQoS – End-to-end Quality of Service support over heterogeneous networks, http://www.euqos.eu.
[7] QBoneArchitecture,http://qos.internet2.edu/wg/documentsinformational/draft-i2-qbone-arch-1.0/.
[8] P. Eardley (ed.), "Pre-Congestion Notification (PCN) Architecture," RFC5559, June 2009.
[9] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC3209, December 2001.
[10] M. Hauge, J. Andersson, M. A. Brose, and J. Sander, "Multi-Topology Routing for QoS Support in the CoNSIS Convoy MANET," in Meaning, Context & Cognition (MCC), Gda´nsk, Poland, October 2012.
[11] Sufyan Al- Irhayim, Junaid Ahmed Zubairi, Qahhar Mohammed & Suhaimi Abdul Latif, " Issues in Voice over MPLS and DiffServ domains".
[12] Yan Chen, Toni Farley and Nong Ye," QoS Requirements of Network Application on the Internet", Information Knowledge Systems Management 4, 2004.
[13] Ammar Alkassar and Christian Stuble, "Security Framework for Integrated Networks", IEEE MILITARY COMMUNICATIONS CONFERENCE, 2003.
[14] Sarvesh Tanwar, Prema K.V, "Threats &Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering(IJSCE), Volume-2, Issue-6, January 2013
[15] Mukesh Kumar, Rahul Rishi and D.K.MAdan, "Issues and Challenges of Quality of Service in Mobile Ad hoc network", International Journal of Computer Science & Engineering Technology (IJCSET)
[16] Pitipatana Sakarindr, Nirwan Ansari, Roberto Rojas-Cessa and Symeon Papavassiliou, "Security-Enhanced quality of Service(SQOS): A Network Analysis".

