Risk-Aware QoP/QoS Optimization for Multimedia Applications in Wireless Networks

Yanping Xiao[1], Chuang Lin[1], Yixin Jiang[1], Xiaowen Chu[2], and Shengling Wang[1]

[1] Department of Computer Science and Technology, Tsinghua University, Beijing, China
{ypxiao, clin, yxjiang, slwang}@csnet1.cs.tsinghua.edu.cn
[2] Department of Computer Science, Hong Kong Baptist University, Hong Kong, P.R. China
chxw@comp.hkbu.edu.h

Abstract. The unique characteristics of wireless networks pose a number of nontrivial challenges to multimedia applications with security and rigorous QoS requirements. Lack of adequate security protection is incapable of meeting security requirements of applications, whereas enabling excessive security services inevitably leads to further degradation in QoS due to additional computation and payload encapsulation. Early work, e.g. LAP, achieves balance by adjusting security policy according to QoS metrics; but none of them are security guaranteed. In this paper, we present an efficient risk-aware QoP (Quality of Protection) and QoS optimization algorithm for multimedia applications in wireless networks. It can achieve an optimization for QoP/QoS performance metrics through offering hierarchical security services and QoS support. Experiment demonstrates that even in high risk environments our scheme can efficiently balance QoP and QoS requirements.

Keywords: QoP, QoS, Optimization, Security, Risk-aware.

1 Introduction

With the rapid proliferation of wireless networks and real time multimedia applications, providing Quality of Service (QoS) and security protection simultaneously in an efficient manner has become a hot topic of current research in wireless networks. Real-time multimedia applications such as VoIP [2-3] and VOD have their specific QoS and security requirements. For example, VoIP applications in civilian use expect stringent delay and packet loss rate but does not expect too much on security aspect; while in military wireless networks, a majority of voice, image, video and data are required to transmit in real time and security mode, i.e., they have very stringent QoS and security requirements. Therefore, how to provide QoS and security guarantee simultaneously to meet security and performance requirements for different applications is a challenging problem. A novel mechanism is required to consider QoS and security together in a uniform and efficient way.

On the other side, in wireless networks, the bandwidth of a link is unpredictable and possibly very low, and the channel capacities and error rates are time-varying, which makes it harder to design multimedia application with stringent QoS requirements than in wireline networks. Furthermore, the shared channel in wireless

N. Bartolini et al. (Eds.): QShine/AAA-IDEA 2009, LNICST 22, pp. 34–51, 2009.

networks makes it easy for data intercepting and tempering and leads to the breach of security; however, enabling excessive security services inevitably leads to further degradation in QoS due to additional computation and payload encapsulation especially in wireless networks with stringent resource constrains. So how to make a tradeoff between security and QoS is a critical issue for multimedia applications with rigorous security and QoS requirements in wireless networks.

Compared with wireline networks, there are more challenges in security and QoS assurance in wireless networks, such as (1) Highly dynamic topology demand to negotiate and configure QoP/QoS policy; (2) The shared media and attenuation of channel make it more difficult in QoS assurance; (3) Adopting individual QoP configuration in heterogeneous devices can not satisfy the performance requirement.

The experiments demonstrate that implementing stronger security services can affect QoS seriously such as packet loss and delay [15] in wireless networks. Most of the existing schemes focus on guaranteeing either security or QoS, but not both. With the prevalence of wireless multimedia applications, some schemes [11-15] integrating security with QoS have been proposed, which improve the grade of security service as much as possible in the precondition of satisfying the QoS requirements. Once QoS decreases or the systems dissatisfy the QoS requirement of applications, they improve QoS metrics by adopting weaker security services.

However, there are still some shortcomings in such schemes: (1) Some applications do not require QoP such as common web applications, and some do not need over-high QoP. Over-high QoP policies not only lead to further degradation in QoS performance, but also decrease utilization rate of system resource. (2) The method of adjusting QoP according to QoS metrics is vulnerable to attack and information leak on account of adopting low security service to improve QoS. (3) Directly adjusting QoP policies only according to the QoS metrics cannot efficiently guarantee the satisfaction of QoS. It should extensively consider other optimization mechanisms such as traffic classification [1], channel access [2], and packet scheduling [3], etc.

For real time multimedia applications with stringent QoS and security requirement, the existing schemes are neither security guaranteed nor QoS guaranteed. To provide QoS and security support simultaneously perfectly, we propose a risk-aware QoP/QoS model for wireless multimedia applications, which can efficiently select appropriate QoP policy to avoid the impact of excessive QoP on QoS by apperceiving the status of security and system resource. Moreover, it can guarantee QoS by dynamically adjusting QoS policies, and thus makes a nice tradeoff between QoP and QoS.

In summary, the contributions of this paper mainly include three aspects: (1) It provides a novel, adaptive and risk-aware multi-level QoP/QoS optimization model to achieve a balance between QoP and QoS. (2) It provides a multi-level QoS model which can be used in real time QoS assurance. (3) It progresses toward a notion of QoP in security comparable to the notion of QoS in networking.

The rest of the paper is organized as follows. The related work is given in section 2. Section 3 respectively introduces multi-level QoP model, multi-level QoS model, and risk-aware multi-level QoP/QoS model in detail. A generic multi-level QoP/QoS framework is presented in section 4. The optimization algorithms between QoP and QoS are discussed in section 5, followed by the experiments in section 6. Finally, section 7 gives conclusions along with future works.

2 Related Work

Compared with QoS, the concept of QoP has surfaced in the literatures for the latest several years. The main idea of QoP is to provide multi-level security services for different users and traffic and to meet the requirements in increasingly complicated environments, and has been focused especially in wireless networks.

Ong et al. [5] firstly presents a QoP framework which provides differential security service levels for mobile multimedia applications with heterogeneous devices in wireless networks. Based on idea of [4], Agarwal et al [9] extend the QoP model and study the impact of different security policy on QoS in wireless LAN networks. Furthermore, since authentication is the first line of defense to provide security service, Liang et al. [5-8] deeply study the impact of challenge/response authentication on QoS performance in wireless LANs. To decrease the impact of authentication on performance, Schneck et al. [10] propose a dynamic authentication protocol to improve the performance of the system. Although the above schemes considered and studied the impact of security on QoS, they don't consider how to achieve the optimization between QoP and QoS.

It is no doubt that providing differentiable security service can decrease security impact on performance, but it is not enough to provide QoS assurance. Therefore, some schemes integrated QoP with QoS have been presented. He et al. [11-12] proposes an integrated solution to delay and security support in wireless networks aiming to wireless applications with stringent delay and security requirement. Almost at the same time, Agarwal et al. [14, 15] develops a link-aware protection (LAP) mechanism to coordinate security and QoS in wireless networks. However in MANET there is little research integrated QoS and security as well, So Shen et al. [13] presents a security and QoS self-optimization mechanism to achieve the optimization. However, the schemes are not security-guaranteed, and the policy of improving QoS through adjusting QoP is not enough to provide QoS assurance.

3 Risk-Aware Mutli-level QoP and QoS Model

In this section, an integrated risk-aware multi-level QoP / QoS optimization model is proposed based on the multi-level QoP model and the multi-level QoS model.

3.1 Multi-level QoP Model

Definitions 1: QoP is defined as the protection quality of security services by using security metrics such as authentication, confidentiality, integrity, non-reputation and availability et al. and formally described as a quintuple vector $P =< Au, C, I, N, A >$, where Au, C, I, N and A denotes authentication, confidentiality, integrity, non-reputation and availability respectively. $Au \in [0,1]$, where 0 denotes no authentication service is provided and 1 denotes the highest authentication mechanism. Its quantification can be referred to implementation mechanisms, strength of algorithms, or length of key. And the same definition applies to *C, I* and *N*. A is a real number between 0 and 1, and denotes the probability of whether the service is available.

We can select different security metrics to embody the levels of security services. Without loss of generality, assuming that the available security policy includes m security features such as authentication and confidentiality, and every security feature includes n optional configuration. Therefore, security policy can be described as an $m \times n$ matrix, and each element P_{ij} in the matrix denotes one policy configuration of security feature i.

$$P = \begin{bmatrix} P_{11} & \cdots & P_{1n} \\ \vdots & \vdots & \vdots \\ P_{m1} & \cdots & P_{mn} \end{bmatrix}$$

Different security policy achieves different protection levels. To describe the protection levels of different security policy, we define a protection levels function g on matrix P as

$$G = g(P) \tag{1}$$

Similarly, matrix G has a form like matrix P, every element in G has one-to-one mapping to every element in P. The protection levels of security policy with the same feature can be compared directly. The composite protection levels of security policy involving multi security features need introduce the definition of QoP Composite Metric (QCM).

Definition 2: QCM is a real number which combines multi security metric and reflects the quality of multi security features; its definition is as follows.

$$qop = \sum_{i=1}^{m} P_i \times \omega_i \tag{2}$$

where P_i denotes protection levels of security feature i, $i \in [1, m]$, ω_i denotes the weight of security feature i, which satisfies

$$\sum_{i=1}^{m} \omega_i = 1. \tag{3}$$

Security features can not avoid influencing the performance of system. To describe it, we introduce the definition of Performance Impact Matrix (PIM).

Definition 3: PIM reflects the impact of security policy matrix P on QoS. For any element P_{ij} in P, we can introduce a function f to denote its performance impact, which is defined as

$$C_{ij} = f(P_{ij}). \tag{4}$$

C_{ij} denotes the impact of security policy P_{ij} on QoS, $i \in [1, m], j \in [1, n]$, it corresponds to a vector $C_{ij} = [d_{ij}, j_{ij}, b_{ij}, l_{ij}]$, where d_{ij}, j_{ij}, b_{ij} *and* l_{ij} denotes delay, jitter,

$$C = \begin{bmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \vdots & \vdots \\ C_{m1} & \cdots & C_{mn} \end{bmatrix}$$

bandwidth, and packet loss rate, respectively. Therefore, we can get PIM C, which can be denoted as matrix P.

Different applications require different quality of security services, even the same application may require different quality of security services. Multi-level QoP model can provide tunable security services according to different security requirements, especially in wireless networks with stringent resource constraints, which can be described as $qop_i \in \{qop_1, qop_2, \cdots, qop_n\}$, where qop_i denotes individual security feature or multi security features, i denotes the quality level of security service.

Generally, the impact of QoP on QoS is positive correlation to the level of QoP. When the performance is decreasing, we can improve QoS by decreasing QoP.

Lemma 1: For a given multi-level QoP model with $qop_i \in \{qop_1, qop_2, \cdots, qop_n\}$, the higher qop_i is, the more the impact on system performance is.

Intuitively speaking, QoP levels of security services are positively correlated with time complexity and space complexity of cryptographic algorithms. Whereas the higher the complexity is, the bigger the impact on performance is.

3.2 Multi-level QoS Model

Different applications have special QoS requirements. For example, for VoIP, its QoS metrics may be denoted as, $\{delay < 150$ ms, $Jitter < 50$ms, $Bandwidth > 64$kbs, $lose\ rate < 3\%\}$.

Most of QoS requirements can be described as a quadruple $\zeta =< d, j, b, l >$, where d, j, b, l respectively denotes delay, jitter, bandwidth, and packet loss rate. Each QoS parameters can be divided into n levels, which can be described as a matrix S,

$$S = \begin{bmatrix} d_1 & d_2 & \cdots & d_n \\ j_1 & j_2 & \cdots & j_n \\ b_1 & b_2 & \cdots & b_n \\ l_1 & l_2 & \cdots & l_n \end{bmatrix},$$

Each element in matrix S indicates a range of a QoS parameter. For delay, jitter, and packet loss rate, the lower the level is, the higher the quality is. For bandwidth, the higher the level is, the higher the quality is.

Individual QoS parameter can be compared directly; the comparison of multi-QoS parameter is required to introduce the definition of Satisfied Degree of QoS (SDQ) and Composite Satisfied Degree of QoS (CSDQ).

Definition 4: SDQ is defined as a real number and is denoted the degree of QoS satisfaction of applications.

Taking delay as an example, and assuming that $delay < D\,ms$, the delay of epoch t is d, then the satisfied degree of delay is calculated as follows,

$$qos\_d(d) = \begin{cases} \dfrac{D-d}{D} & d \in [0, D] \\ 0 & d > D \end{cases} \tag{5}$$

Similarly, the satisfied degree of Jitter, Bandwidth and Loss rate can be respectively define as follows.

$$qos\_j(j) = \begin{cases} \dfrac{J\text{-}j}{J} & j \in [0, J] \\ 0 & j > J \end{cases} \tag{6}$$

$$qos\_b(b) = \begin{cases} 0 & b < B \\ \dfrac{b}{B} & b \geq B \end{cases} \tag{7}$$

$$qos\_l(l) = \begin{cases} \dfrac{L-l}{L} & l \in [0, L] \\ 0 & l > L \end{cases} \tag{8}$$

Definition 5: CSDQ is defined as follows,

$$\begin{aligned} qos(d, j, b, l) = {} & qos\_d\ (d) \times \omega_d + qos\_j\ (j) \times \omega_j \\ & + qos\_b\ (b) \times \omega_b + qos\_l\ (l) \times \omega_l \end{aligned} \tag{9}$$

where $\omega_d, \omega_j, \omega_b$ *and* ω_l denote the weight of each parameters respectively, and $d \in [0, D],\ j \in [0, J],\ b \in [B, +R],\ l \in [0, L]$.

The value of $\omega_d, \omega_j, \omega_b$ *and* ω_l in Eq. (9) is relative to certain types of network traffic. For example, the most concern are delay and packet loss rate for VoIP traffic, so both of the corresponding weight may be set to 0.4, and the other may be set to 0.1 equally.

QoS parameters fluctuate constantly in real scenarios. Multi-level QoS model can be described as $qos_i \in \{qos_1, qos_2, \cdots, qos_n\}$, where qos_i indicates a single QoS parameter or a composite QoS parameter, i denotes the level of QoS.

If the system fails to guarantee qos_i, we can relax from qos_i to qos_{i-1}. If the system cannot meet the lowest level qos_1, we can only drop the application.

3.3 Risk-Aware Multi-level QoP/QoS Model

Risk-aware multi-Level QoP/QoS model can efficiently decrease the impact of QoP on QoS by selecting multi-level QoP according to the risk level of system, and can also provide multi-level QoS service by adjusting QoS policies according to the monitored QoS metrics, which is especially appropriate to applications with stringent QoS and security requirement in wireless networks.

Assuming that $S_0 = [d_0, j_0, b_0, l_0]$ denotes QoS of the application without introducing any security services, $f(P_{ij})$ denotes the impact of security policy P_{ij} on QoS, so the objective is maximum QoS in the precondition of security assurance, that

is to find a m dimensional vector Γ, which can maximize QoS of applications with m security policy configurations,

$$\Gamma = \arg \max_{j_i \in [1,n]} (\alpha \times qos(d_0, j_0, b_0, l_0) - \beta \times qos(\sum_{i=1}^{m} f(P_{ij_i}))) \tag{10}$$

Subject to

$$\begin{cases} g(P_{ij_i}) \geq R_i, i \in [1,m]; \\ d_0 \in [0,D]; \\ j_0 \in [0,J]; \\ b_0 \in [B,+R]; \\ l_0 \in [0,L]; \end{cases} \tag{11}$$

where α, β denotes a constant respectively, they depend on the status of wireless network, and often are set to 1. In Eq. (11) $g(P_{ij})$ denotes the protection level of security service, R_i denotes the risk levels to be introduced in the following.

Theorem 1: For a risk-aware multi-level QoP/QoS model, if it satisfies QoS/QoP requirements of an application, the following conditions $qos(d_0, j_0, b_0, l_0) + qos(\sum_{i=1}^{m} f(P_{ij})) > 1$ must hold.

Proof: For an application with rigorous QoS requirement, it must satisfy conditions $d_0 < D, j_0 < J, b_0 \geq B, l_0 < L$. To provide normal service to an application, its QoP levels must larger or equal the risk levels. However QoP cannot avoid affecting QoS,

$$qos(\sum_{i=1}^{m} f(P_{ij})) = qos(\sum_{i=1}^{m} C_{ij}) \tag{12}$$

Extending Eq. (12), we can get the following equation.

$$\begin{cases} qos(\sum_{i=1}^{m} f(P_{ij}))_d = qos(\sum_{i=1}^{m} d_{ij}) = \sum_{i=1}^{m} \frac{D - d_{ij}}{D} \\ qos(\sum_{i=1}^{m} f(P_{ij}))_j = qos(\sum_{i=1}^{m} j_{ij}) = \sum_{i=1}^{m} \frac{J - j_{ij}}{J} \\ qos(\sum_{i=1}^{m} f(P_{ij}))_b = qos(\sum_{i=1}^{m} b_{ij}) = \sum_{i=1}^{m} \frac{b_{ij}}{B} \\ qos(\sum_{i=1}^{m} f(P_{ij}))_l = qos(\sum_{i=1}^{m} l_{ij}) = \sum_{i=1}^{m} \frac{L - l_{ij}}{L} \end{cases}$$

We take delay as an example. If the in-equation $qos(d_0) + \sum_{i=1}^{m} qos(d_{ij}) \leq 1$ holds, then $\sum_{i=1}^{m} d_{ij} + d_0 \geq D$ must holds. Obviously it contradicts total $d < D$, so the equation holds. For the other parameters, the conclusion also holds. □

Improving S_0 or decreasing QoP levels can improve QoS, S_0 can also be improved by QoS mechanisms such as resource reservation, access control, packet scheduling and traffic classification etc. Decreasing QoP levels can be achieved through altering

security policy with higher levels to those policy with lower levels. Therefore, it is required to introduce the notion of risk levels.

Definition 6: Risk levels correspond to the protection levels of security features and can be described as a column vector $[r_1, \cdots, r_i, \cdots r_m]$, $r_i \in [1, n]$.

Wireless networks are subject to many attacks such as data intercepting, tempering etc; therefore, there exist many potential risks. The degree of risks is relative to the environments and application requirements. Risk levels justly reflect the extent of potential threats. We assume IDS/IPS can report the potential risk levels in real time, and then we can adjust security policy according to the risk levels.

Normal services can be provided only when the QoP levels are higher than risk levels. So there is a problem how to select security policy. The related algorithm can be described as follows:

Algorithm 1. Optional-Policy-Matrix-Cal

Optional - Policy - Matrix - Cal(P, D)\{
01 : $D \leftarrow P$
02 : *for* $i = 1$ *to* m *get*(r_i)
03 : *for* $i = 1$ *to* m
04 : *for* $j = 1$ *to* n
05 : *if* $P[i, j] < r_i$ *then*
06 : $P[i, j] = null$
07 : \}

Supposing that the risk levels vector from IDS/IPS is $R = [1, 2, \cdots, n]$, then we can get an optional policy matrix D,

$$D = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ 0 & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & P_{mn} \end{bmatrix}$$

Every element in matrix D indicates an optional security policy configuration. The total of schemes provided by the system is $\prod_{i=1}^{m} N_i$, where N_i denote the number of optional policy.

To understand the impact of QoP on QoS further, we get a theorem as follows.

Theorem 2: For a risk-aware multi-level QoP and QoS model, if there exists a security policy p which satisfy QoS and QoP requirements simultaneously, then its impact on QoS must satisfy the equation, $\sum_{i=1}^{m} C_{ir_i} \le f(p) \le \sum_{i=1}^{m} C_{in}$, where $r_i \in [1, n]$ denotes the current risk levels of the corresponding security feature.

Proof: If the security policy p satisfies requirement of QoS/QoP simultaneously, then the protection levels corresponding to the security policy p are not smaller than risk

levels vector $r_i, i \in [1, m]$ at least. So if we can choose the security policy with the same level of risk, the impact I on QoS is calculated as below.

$$I\_min = \sum_{i=1}^{m} f(P_{ir_i}) = \sum_{i=1}^{m} C_{ir_i} \tag{13}$$

When choosing the security policy with the maximum QoP level, the impact of QoP on QoS is calculated as

$$I\_max = \sum_{i=1}^{m} C_{in}. \tag{14}$$

When choosing the security policy in the optional sets at random mode, the impact of QoP on QoS is calculated as

$$I = \sum_{i=1}^{m} \frac{1}{n-r+1} \sum_{j=r}^{n} C_{ij}. \tag{15}$$

According to Lemma 1, $f(p)$ must be limited in the range of value of the Eq. (14) and Eq. (15), so the equation is easy to be proofed.

4 Generic Risk-Aware Multi-level QoP/QoS Framework

In this section we present a generic multi-level QoP/QoS framework for wireless multimedia networks. The progress of wireless technique enables more mobile devices such as PDA, Mobile Phone to access internet through wireless networks. Deploying real time multimedia applications in these devices not only require considering their capability of CPU, Memory and IO fully, but also require providing enough security. So we provide a generic risk-aware multi-level QoP/QoS framework which can provide tunable security service and performance support, especially appropriate to wireless networks with stringent resource constraints.

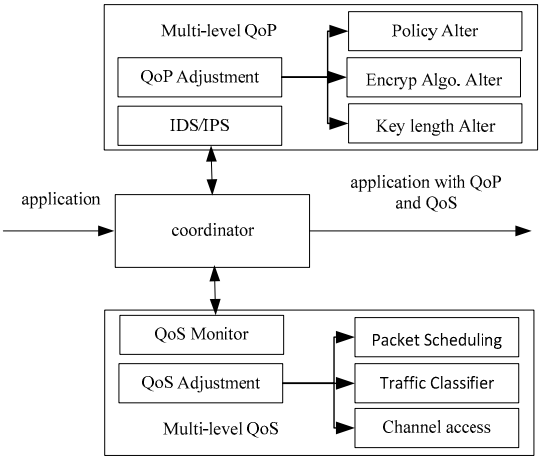


Fig. 1. A Generic Tunable QoP and QoS Framework

Fig. 1 shows a generic multi-level QoP/QoS framework, which consists of multi-level QoP module, multi-level QoS module, and a coordinator module. The coordinator module is charge of negotiating and providing service for QoP/QoS requirements. When the negotiation is agreed, it constantly adjusts the QoP levels and QoS policy to meet the requirement of an application according to system risk levels and status of system resource.

Multi-level QoP module includes IDS/IPS and QoP adjustment components. IDS/IPS monitors the incoming and outgoing network traffic, the system files and the running process, and reports the risk according to the abnormality distance [19]. Multi-level QoP components provide the response according to the risk levels issued by the IDS/IPS. The most likely responses [20] in wireless network is to reinitialize communication channels between nodes, the corresponding measures may include the adjustment of the security policy such as adding the authentication, integrity, or confidentiality mechanisms, altering encryption algorithms, or altering key lengths of algorithms. In this paper we focus on the alteration of cryptographic algorithm and key lengths.

Multi-level QoS module consists of QoS monitor and QoS adjustment components, they coordinate to satisfy QoS requirement of applications. QoS monitor module is uninterruptedly monitoring the QoS metrics of real-time applications. The metrics of performance monitor includes delay, jitter, and bandwidth, and packet loss rate. If the metric is in the critical rang of its value, QoS adjustment components will be invoked to improve QoS performance according to the status of system resource. QoS adjustment components mainly consist of traffic classifier, packet scheduling, and channel access. In this paper, we only focus on the packet scheduling through altering the priority of packets.

5 Risk-Aware Multi-level QoP/QoS Optimizations Algorithms

Since the implementation of QoP inevitably affects QoS, to decrease the impact of QoP on QoS and meet QoS requirements simultaneously in wireless networks with limited resources, some effective algorithms are required to achieve the optimization and tradeoff between QoP and QoS. The objective of optimization is to maximize QoS under the condition of certain QoP.

To accomplish the optimization and tradeoff between QoP and QoS in wireless networks, we adopt the method of dynamically selecting security policy, which is especially fit to the devices with limited computation resource. When risk levels change, we select security policy with the same QoP level. In such a way, we can decrease the impact of QoP on QoS to minimum. At the same time, if QoS can't be satisfied because of variability of channel in wireless networks, we can also call QoS adjustment components such as altering the priority of packets to improve QoS according to QoS monitor.

Our algorithms consist of two parts, one is risk-aware multi-level QoP adjustment algorithms, and the other is QoS optimization algorithms. Some parameters are listed in Table 1.

Table 1. Parameters in Algorithms

Parameters	Descriptions
qos^*	A variable denoting an initial QoS value being negotiated by the parties, satisfying $qos^* \in \{qos_1 \le qos_2 \le \cdots \le qos_{\max}\}$
qop^*	A variable denoting an initial QoP value being negotiated by the parties, satisfying $qop^* \in \{qop_1 \le qop_2 \le \cdots \le qop_{\max}\}$
pr^*	A variable denoting an initial priority value being negotiated by the parties, satisfying $pr^* \in \{qop_1 \le qop_2 \le \cdots \le qop_{\max}\}$
$S(t)$	QoS value of an application in real time
$R(t)$	Risk level issued by IDS in real time
$pr(t)$	Priority of packets for an application in real time

In Table 1, qos^* and qop^* are calculated by the Eq. (9) and Eq. (2), respectively, pr^* denotes the priority of packets. $qos_{\max}$ and qos_1 denote the highest QoS level and the lowest QoS level respectively. $qop_{\max}$ and qop_1 denote the highest and lowest level of security services. $pr_{\max}$ and pr_1 denote the highest and lowest priority level.

5.1 Risk-Aware Multi-level QoP Adjustment Algorithms

Wireless networks are more subject to attacks, and thereby some strong security mechanisms are adopted. However, these mechanisms may affect the performance severely. To decrease the impact to minimum, risk-aware multi-level QoP adjustment algorithm is presented in this paper. When the risk levels are larger than the level of security protection, QoP adjustment components will be enabled to improve QoP level in order to weaken potential threats. There are many modes to adjust security policy. The minimization protection mode may be the best choice. QoP adjustment algorithm is described as follows.

Algorithm 2. QoP-Adjust

QoP_Adjust(qop^*){
01 : *if* $R(t) > qop^*$ *and* $R(t) = qop_i$ *then*
02 : $qop^* = qop_i$ *and Call* $QoS\_Ada(qos^*)$ *and* $Pr\_Adjust(pr^*)$
03 : *else*
04 : *keep* qop^* *unchanged*
05 : }

5.2 QoS Optimization Algorithms

The shared media and attenuation of channel in wireless network make QoS assurance more challenging than in wireline networks, therefore more QoS mechanisms should be considered when providing QoS support. Once performance

decreasing, the mechanisms can be invoked. We take priority adjustment as an example to introduce QoS optimization algorithms. We assign a priority of packets according to the QoS requirements in initialization, and then adjust the priority of packets to improve QoS according to the monitoring of QoS in run-time. At the same time, the system adaptively changes QoS according to the priority and the monitored QoS metrics. The optimization algorithms consist of QoS adaptive algorithm and priority adjustment algorithm, which are depicted as below respectively.

When the priority of packets is maximal and detectable QoS level is larger than minimum level, qos^* can be degraded properly. But it should be ensured in the pre-specified range. When qos^* is smaller than the minimum and qop^* level is larger than the risk level, qop^* level can be decreased to improve qos^*, otherwise the application should be discarded.

Algorithm 3. QoS-Ada

QoS_Ada(qos^*){
01 : *if* $pr(t) = pr_{\max}$ *and* $S(t) < qos^* \neq qos_1$ *then* $qos^* = qos_{i-1}$
02 : *if* $pr(t) = pr_{\max}$ *and* $S(t) < qos^* = qos_1$ *then*
03 : *if* $R(t) < qop^*$ *then* $qop^* = qop_{i-1}$ *until* $qop^* = R(t)$
04 : *else Drop the application*
04 : *if* $pr(t) < pr_{\max}$ *and* $qos_{i+1} > S(t) > qos_i$ *then* $qos^* = qos_i$
05 : *else* $qos^* = qos_{i+1}$ *until* $qos^* = qos_{\max}$
06 : }

When detected qos^* is smaller than pre-specified requirement, we can increase the priority of packets to improve qos^*. When qos^* is larger than pre-specified requirement, we can decrease the priority the algorithms is described as below.

Algorithm 4. Pr-Adjust

Pr_Adjust(pr^*){
01 : *if* $S(t) < qos^*$ *and* $pr^* = pr_i$ *then*
02 : $pr^* = pr_{i+1}$ *until* $pr^* = pr_{\max}$
03 : *else if* $S(t) > qos^*$ *then*
04 : $pr^* = pr_{i-1}$ *until* $pr^* = pr_1$
05 : *else*
06 : *keep* pr^* *unchanged*
07 : }

Although we can adjust the priority of packets to improve qos^*, it cannot assure the satisfaction of QoS. Our algorithms consist of monitoring of QoS performance, so we can adjust pr^* and QoP policy to assure QoS before exacerbation of QoS.

6 Experimental Studies

VoIP application is a very typical of multimedia application. In this section we take wireless VoIP as an example to simulate and demonstrate our model and algorithms.

6.1 Experiment Setup

We set up a wireless LAN test bed to simulate 802.11 wireless network transmit. The test bed consists of two servers (an ftp server and a voice gateway server) behind an access point, and three mobile clients. The access point and stations send packets by the rate 11Mbps. We assume use of G.729 as audio codec, and emulate VoIP traffic by UDP packets with 32 byte data at the rate of 50 packets percent second between a voice gateway and a voice station. We also simulate the background data stream by ftp uploading and downloading between one ftp server and two data stations. All the computers are running RedHat Linux 9 with kernel version 2.6.9-5. Fig. 2 shows the topology of the test bed, in the figure the voice station send packets to voice gateway, Data station 1 and 2 uploads and downloads files to simulate the background streams respectively.

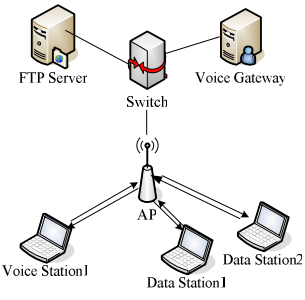


Fig. 2. Network Topology for Experiment

6.2 Experimental Results

In this subsection, we take DES, AES with three different key lengths as encryption policy and MD5, SHA1 as integrity policy to simulate the impact of different QoP policies on QoS, and we also assume risk levels with one-to-one mapping relation to QoP policy. Then we simulate the Risk-aware Multi-level QoP and QoS algorithms (RMQQ) as described in Section 5.

To measure the impact of QoP on QoS in wireless VoIP applications, we used a VoIP performance metric R proposed in [16-17], which takes into account delay, loss rate, and the type of the encoder. R is defined in Eq. (16), which reflects QoS of VoIP application and should provide a value above 70. If the value is blow 70, the quality of VoIP can't meet the requirements.

$$R = 94.2 - 0.024d - 0.11(d - 177.3)H(d - 177.3) \\ -11 - 40\log(1 + 10e) \tag{16}$$

where d denotes delay, it consists of codec delay, playback delay and network delay. If we consider the delay caused by different security level services, the delay should include qop delay denoted by d_{qop}.

$$d = d_{code} + d_{playout} + d_{network} + d_{qop} \tag{17}$$

Some experimental parameters and the combination of algorithms are shown in Table 2 and Table 3 respectively.

Table 2 lists some delay parameters in Eq. (18). $d_{network}$ and d_{qop} are parameters which are attained by our experiment.

Table 2. Experimental Parameters

Parameters	Value
d_{codec}	25ms
$d_{playout}$	60ms
$e_{playout}$	0.005
sending rate	50packet/sec
packet size	32byte
wireless bandwith	11Mpbs

Table 3 lists the combination of encryption algorithms and integrity algorithms. DES and AES can achieve encryption feature. DES is replaced by AES in wireless networks by virtue of lower security level of DES in comparison with AES. Both MD5 and SHA1 can achieve integrity, the security level of MD5 is lower than SHA1, but its efficiency is more than SHA1.

In order to calculate QoP levels of different algorithms combinations in Table 3, we compile Cypto Libraries [18] in gcc at the voice station IBM T60 with the configuration Genuine intel® CPU T2400@1.83GHz and 512M memory. We do 1000 experiments to get the average throughput of algorithms as shown in Table 4.

Table 3. QoP Level of Different Policy Configuration

QoP Policy	QoP Level	System Risk Level
DES-MD5	1	1
AES128-MD5	2	2
AES192-MD5	3	3
AES256-MD5	4	4
DES-SHA1	5	5
AES128-SHA1	6	6
AES192-SHA1	7	7
AES256-SHA1	8	8

Table 4. Throughput of Different Algorithms (Mbps)

Alg.	Key Length(bits)	IBM T60
DES	56	109.2Mbps
AES	128	85.0Mbps
AES	192	79.5Mbps
AES	256	72.9Mbps
MD5	-	288.7Mbps
SHA1	-	103.8Mbps

According to the average throughput of each algorithm, we can easily to sort and set their QoP levels due to the positive correlation between the QoP levels of algorithms and compute complexity.

In order to simulate RMQQ algorithm, assume that we can get the risk levels from IDS or IPS. Because the risk levels are varied with the potential attacks and the environments, so in the experiment we adopt a random method to simulate the variation of risk levels. We assume that risk levels change once per hour, and we don't distinguish specific security features and adopt composite QoP level in Eq. (2) to correspond to risk levels. When risk levels are varied, we adopt QoP policy with the same level or the higher level. System risk levels and QoP policy corresponding to risk levels are also shown in Table 3.

We adopt the security algorithms in Table 4 to simulate the adjustment of QoP policy, i.e, we encrypt packets in information source and decrypt them in receiving end. At the same time, data station 1 uploads big movie files to the ftp server and data station 2 downloads files from the same ftp server. Our monitoring time is about 1 minute, 3000 packets. We do experiments about one hour for every algorithm combination, then we average the delay and packet loss, the results is shown in Fig. 3 and Fig. 4, respectively.

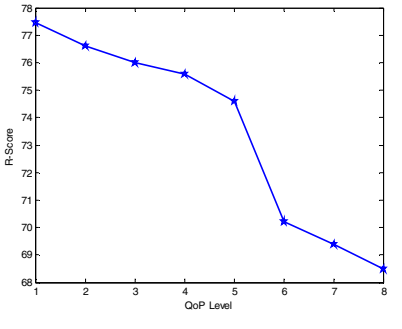
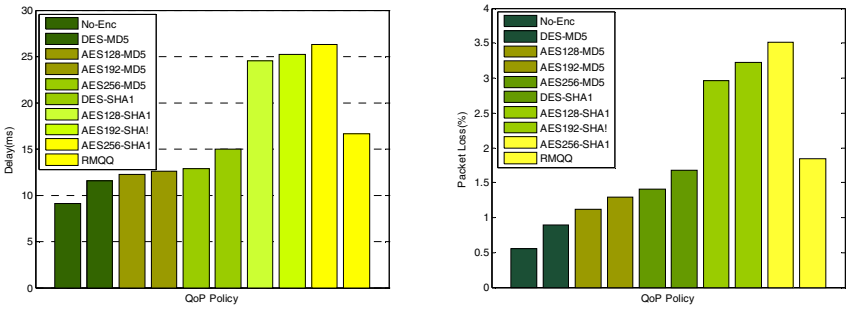


Fig. 3. Variation of R-Score with QoP Level



(a) Delay with QoP Policy (b) Packet Loss with QoP Policy

Fig. 4. Performance of QoP Policy

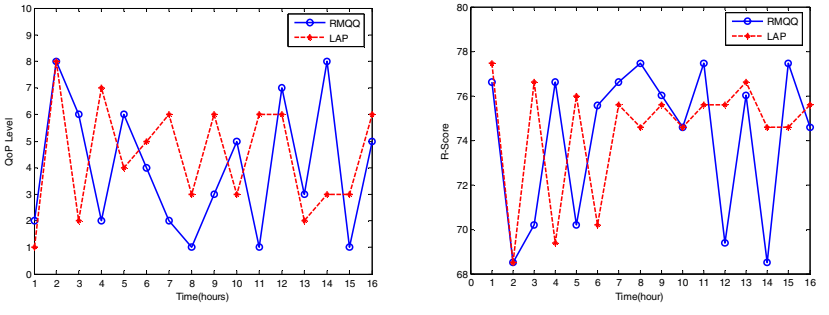


Fig. 5. Variation of Risk level for RMQQ/LAP **Fig. 6.** Variation of R-Score for RMQQ / LAP

Fig. 3 shows the relation between QoP level and R-Score. From the graph we can draw a conclusion that R-Score decreases with QoP level increasing.

Fig. 4 shows the VoIP delay and packet loss rate with different QoP policy. The higher the QoP level of security policy is, the more the performance impact on QoS is. RMQQ gets the result in the range of the minimum and maximum owing to adjusting the policy according to the variation of risk levels.

In comparison with LAP [15], we simulate the snapshot of RMQQ and LAP. Fig.5 shows the variation of QoP policy with the risk levels in RMQQ and LAP. We choose QoP policy in minimum protection mode because of the negative correlations between QoP and QoS. The line of RMQQ accords with the variation of risk level, so the line of the risk level variation is not depicted in the Fig. 5 and Fig. 6. As for LAP, there is a probability of near 50% that QoP levels are lower than risk levels. That is because LAP adjusts QoP policy according to QoS. Relative to RMQQ, LAP cannot guarantee QoP level is higher than risk level, so it suffers from more security threats.

Fig. 6 shows the impact of RMQQ on QoS, and the impact of LAP on QoS in the threshold of packet loss 1.8% and threshold of delay 13ms. The average R-Score of two schemes are 74.11 and 74.44 respectively and are very close. But when the risk levels are higher, R-Score of LAP is a little better than that of RMQQ, that is because that LAP does not consider the potential risk, and change QoP policy according to

QoS only. When the risk is lower, RMQQ choose the QoP policy with lower level while the QoP polices of LAP varies little, and their R-Scores are 76.0048 and 69.39 respectively. Relative to LAP, VoIP quality of RMQQ increases about 10%. From Fig.5 and 6, the fluctuation of scheme RMQQ seems rapider than LAP, that is because we assume that the variation of risk levels occurs every an hour in interval at random. However in reality the changing of risk levels often varies slowly.

7 Conclusion

In this paper, a risk-aware multi-level QoP/QoS optimization model is presented, which can efficiently solve real time multimedia applications with security and stringent QoS requirement in wireless networks. It can dynamically adjust QoP policy according to the risk issued by IDS, and provide multi-level security services, decrease the impact of QoP on the QoS, and guarantee QoS of applications. Experiments demonstrate that the risk-aware multi-level QoP/QoS model can not only provide multi-level QoP/QoS services, but also achieve optimization and make a nice tradeoff between QoP and QoS. The more important is that it extends the early idea of adjusting QoP policy according to QoS metrics only and integrates security with QoS into one model, which can efficiently coordinate QoP with QoS. Future work will introduce heuristic algorithm to solve the multi-level QoP/QoS optimization problem.

Acknowledgments. This research was supported by the National Grand Fundamental Research 973 Program of China (No.2010CB328105) and the National Natural Science Foundation of China (No.60970101, No. 60673187, No. 60872055 and No. 60803123).

References

1. Barry, M.G., Campbell, A.T., Veres, A.: Distributed Control Algorithm for Service Differentiation in Wireless Packet Network. In: Proc. IEEE INFOCOM (2001)
2. Hanley, G., Murphy, S., Murphy, L.: Adapting WLAN MAC Parameters to Enhance VoIP Call Capacity. In: Proc. of the 8th ACM MSWiM 2005, October 2005, pp. 250–254 (2005)
3. Yu, J., Choi, S., Lee, J.: Enhancement of VoIP over IEEE 802.11 WLAN via Dual Queue Strategy. In: Proc. IEEE ICC (2004)
4. Ong, C.S., Nahrstedt, K., Yuan, W.: Quality of Protection for Mobile Multimedia Applications. In: Proc. IEEE ICME, vol. 2, pp. 137–140 (2003)
5. Liang, W., Wang, W.: An Analytical Study on the Impact of Authentication Local Area Networks. In: Proc. IEEE 13th Intel. Conf. and Networks (ICCCN 2004), pp. 361–366 (2004)
6. Liang, W., Wang, W.: A Quantitative Study of Authentication Networks. In: Proc. IEEE INFOCOM, vol. 2, pp. 1478–1489 (2005)
7. Liang, W., Wang, W.: On Performance Analysis of Challenge/Response Based Authentication in Wireless Networks. Computer Networks 48(2), 267–288 (2005)
8. Wang, W., Liang, W., Agarwal, A.K.: Integration of Authentication and Mobility Management in Third Generation and WLAN Data Networks. Wireless Comm. and Mobile Computing (WCMC) 5(6), 665–678 (2005)

9. Agarwal, A.K., Wang, W.: On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility. Mobile Networks and Applications 12, 93–101 (2007)
10. Schneck, P.A., Schwan, K.: Dynamic Authentication for High performance Networked Application. In: Proc. of the sixth International Workshop on QoS, pp. 127–136 (1998)
11. He, W., Nahrstedt, K.: An Integrated Solution to Delay and Security Support in wireless network. In: Proc. IEEE WCNC, Las Vegas, vol. 4, pp. 2211–2215 (2006)
12. He, W., Nahrstedt, K.: Impact of Upper Layer Adaptation on End-to-End Delay Management in Wireless Ad Hoc Networks. In: Proc. IEEE Real-Time Embedded Technology and Application Symposium, RTAS 2006, April 2006, pp. 59–70 (2006)
13. Shen, Z., Thomas, J.P.: Security and QoS Self-Optimization in Mobile Ad Hoc Networks. IEEE Trans. on Mobile Computing 7(9), 1138–1151 (2008)
14. Agarwal, A.K., Wang, W.: DSPM: Dynamic Security Policy Management for Optimizing Performance in wireless networks. In: Proc. IEEE MILCOM 2006, pp. 1–7 (2006)
15. Agarwal, A.K., Wang, W., Gupta, R.A., Chow, M.: LAP: Link-Aware Protection for Improving Performance of Loss and Delay Sensitive Applications in Wireless Lans. In: Proc. IEEE MILCOM 2007, pp. 1–7 (2007)
16. Cole, R., Rosenbluth, J.: Voice over IP performance monitoring. ACM Comput. Commun. Rev. 31, 9–24 (2001)
17. ITU-T Recommendation G.107, The E-model, a Computational Model for Use in Transmission Planning (1998)
18. Dai, W.: Crypto++, `http://www.eskimo.com/weidai/cryptlib.html`
19. Hariri, S., Qu, G., Modukuri, R., Chen, H., Yousif, M.: Quality-of-Protection (QoP) – An Online Monitoring and Self-Protection Mechanism. IEEE Journal on Selected Areas in Communications 23(10) (2005)
20. Mishra, A.: Security and Quality of Service in Ad Hoc Wireless Networks. Cambridge University Press, Cambridge (2008)