A Game Theoretic Approach to Integrate Security with Quality of Service

---

Citation:

Zubair Md. Fadlullah, Athanasios V. Vasilakos, and Nei Kato, "A Game Theoretic Approach to Integrate Security with Quality of Service," IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, Jun. 2012.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6364011

A Game Theoretic Approach to Integrate Security with Quality of Service

Zubair Md. Fadlullah[1⋆], Athanasios V. Vasilakos[2], and Nei Kato[1].
Graduate School of Information Sciences (GSIS), Tohoku University, Japan[1]
Department of Computer and Telecom. Engineering, University of Western Macedonia, Greece[2]
E-mail: ⋆zubair@it.ecei.tohoku.ac.jp

***Abstract*—The concept of Quality of Service (QoS) offers different service levels to the network users. Through Service Level Specifications (SLSs), the users in a wireless network, which supports QoS, are able to express, at run-time, their expected service requirements through well defined parameters. Conventional QoS parameters, such as throughput, delay, jitter, packet loss rates, and so forth, are used for reliably ensuring a certain service level with respect to reliability and/or performance. However, most existing researches have ignored tunable security as a Quality of Service (QoS) parameter. The biggest challenge of integrating QoS and security parameters consists in their contrasting goals. This paper presents an idea to permit the users of an IEEE 802.11 Wireless Local Area Network (WLAN) to specify their security and QoS requirements in their Service Level Specifications (SLSs). Then, a game theoretic approach is presented so that the system can reach Service Level Agreement (SLA) with the users to ascertain a balanced set of security and QoS parameters for the users. The effectiveness of the proposed approach is verified through computer simulations.**

***Index Terms*—Quality of Service (QoS), Quality of Security Service (QoSS), Service Level Specification (SLS), Game theory.**

I. Introduction

The research, development, and deployment of network-centric Quality of Service (QoS) have pre-dominantly focused on problems including bandwidth guarantees, packet loss rate, end-to-end delay, delay variance or jitter, and also other performance-related quality guarantees when transmitting information over the Internet. To provide QoS for real-time traffic and interactive multimedia applications, QoS provisioning models such as Integrated Services (IntServ) [1] and Differentiated Services (DiffServ) [2] architectures have been widely used. Recent developments in Wireless Personal Area Networks (WPANs), Wireless Local Area Networks (WLANs), and peer-to-peer networks have unlocked new directions for researchers in the field of QoS. For instance, widespread and quick deployments of WLANs provide the end-users with a great convenience while accessing the Internet via wireless devices, e.g., laptop computers, Portable Data Assistants (PDAs), or smart phones. The use of IEEE 802.11 WLAN technology is ever-increasing as public access networks for transmitting QoS-sensitive applications, which often comprise sensitive and crucial information. As a consequence, it is also essential to provide security along with QoS. In addition, depending on the specific nature of each application used (e.g., non-realtime applications, real-time applications with adaptive or non-adaptive requirements), the security levels may be perceived differently by the end-users. The traditional QoS schemes may permit such applications to receive assurance on particular QoS parameters such as bandwidth and delay. But, these schemes do not have the adequate support of integrated and differentiated levels of security. Therefore, in order to promote the research of QoS in these new frontiers of wired as well as wireless networking, the notion of QoS must be extended to include multi-level security in an effective fashion.

Though theoretically simple, it has been, indeed, difficult to offer the end-users multiple levels of security with varied performance preferences [3]. To address this important issue, the term: Quality of Security Services (QoSS) has become popular amongst current researchers that delineates the need to protect sensitive information while maintaining QoS in an effective manner. QoSS approaches invariably consider security attributes such as the choice of authentication scheme, the selection of the cryptographic algorithm, and the lengths of the encryption/decryption keys. Indeed, the protection of information exchanges over wireless as well as wired media is usually achieved by employing security mechanisms and cryptographic protocols. One shortcoming of such end-to-end security enforcements consists in the fact that they may lead to QoS degradation because of their impacts on the QoS attributes, e.g., resources, bandwidth, and delay requirements. In order to address these issues, in this paper, we develop a game theoretic real-time system for IEEE 802.11 WLAN that provides an appropriate QoS-security level.

This paper is organized as follows. Section II surveys the related research works on QoSS. The considered system model is presented in Section III. Section IV describes the proposed QoSS approach based on a non-cooperative game played by the users. The effectiveness of the proposed approach is verified in Section V. Finally, the paper concludes in Section VI.

II. Related Research Work

A leading illustration of how security may be integrated as a dimension to existing QoS frameworks can be found in the middleware adaptation proposed in [4]. The users of IEEE 802.11-based wireless ad-hoc networks are presented with a set of security requirements and end-to-end QoS delay requirements. Depending on a user's chosen level of security and delay requirements, the middleware adaptor attempts to attain the minimum end-to-end delay while offering the user the highest possible security level, which is proportional to the encryption key-length. Thus, it achieves a balance

between delay and security levels under varying network loads. Although this tunable QoS/QoP framework for QoS delay and security requirements serves as a pioneering work, a bandwidth consuming attack might exploit the manner in which the encryption key-lengths are downgraded dynamically to maintain a reasonable end-to-end delay requirement for the user, for allowing the attacker to launch cryptographic attacks more effectively and quickly owing to the weakened encryption level. In one of our earlier work [5], we illustrated the significance of this problem of dynamically adjusting the lengths of the encryption keys with varying end-to-end delays.

Some researchers considered the conflicting goal of achieving QoS and security requirements at the same time as a problem, which may be solved by selecting an adequate adaptive theory. For instance, game theory, which has been applied to various disciplines such as Economics, Political Science, and Computer Science, may be applied for choosing the adequate QoS-security level. Game theory consists of a multiplayer decision problem whereby multiple players with different objectives may compete and interact/co-operate with one another to maximize their respective benefits. For instance, the two works in [6], [7] exploit the co-operative game theory-based strategies to model the interaction between intruders and the Intrusion Detection System (IDS) in a wired and a mobile ad hoc network, respectively. The applicability of game theory was demonstrated to be useful to various decision, analysis, and control algorithms in intrusion detection [8]. This work addressed the trade-offs among fundamental network security issues and attempted to find appropriate decision from contrasting goals. On the other hand, Bayesian Nash algorithm is employed in the work conducted by Liu *et al.* [9] to analyze the interaction between an intruder and a defender in both static and dynamic network settings with the aid of monitoring systems. Nash equilibrium based game theoretic studies have also been conducted towards solving QoS problems (i.e., without any security incorporation) involving power and rate control problem where network users compete with each other to obtain maximum throughput with minimum energy consumption [10], [11].

While the afore-mentioned research works focused on a few quality of service and/or security aspects, they did not provide a broad picture of the QoSS model. In this paper, we aim at presenting a complete QoSS solution based on game theory. In the next section, we describe our considered system model whereby the network users can negotiate with the system regarding their service and security level requirements.

III. System Model

We may define the QoSS issue as an optimization problem in terms of mapping available security options to network performance QoS parameters in order to maximize the security while minimizing the impact of the chosen security level on the network performance. In this paper, we consider various QoSS attributes under an IEEE 802.11 WLAN environment.

The decision of QoSS selection is delegated to the WLAN Access Point (AP) to exploit the best available characteristics of the access technologies and network provider to satisfy the expected quality of service and security expectations of the users. Thus, our considered system model depends on the users' short term contractual agreements with the AP. To establish a contractual agreement with the AP, the Quality of Security Service Level Specification (QoSSLS) of a user contains her security requirements in addition to her QoS demands. The integration of security parameters within the QoSSLS enables the WLAN operator to advertise its available security of service to the subscribers so that they can easily know which level of security may be currently gained from the AP to satisfy their preferred services quality.

A number of challenges exist in formulating an adequate QoSSLS for ensuring good and fair security services along with users QoS requirements. In addition to the QoS parameters (throughput, end-to-end delay, bandwidth ratio, fairness, and error rate), the users can express Quality of Security as follows. QoSSLS should take into account the ability of different users to express their security needs. For example, our proposed QoSSLS format in Fig. 1 allows inexperienced users to easily select QoSS levels from any of the four predefined ones, namely high, medium, low, and none. On the other hand, the more experienced users may be permitted to explicitly configure their QoS levels. As shown in Fig. 1, they may be able to configure quantitative security parameters such as security protocol selection, cryptographic operation mode, cryptographic key size, access control tolerance, and non-repudiation level.

Next, we describe our considered wireless network setting comprising a number of users belonging to an AP. Each user (referred to as a "player" in the game theory context later in Section IV) needs to bind with the AP to receive her QoSS requirements. For this purpose, the user needs to negotiate with the AP on her required QoSS as shown in Fig. 2. In the considered system, the AP has two components, namely (i) a QoSS resolver (QR) and (ii) a Threat Evaluator (TE). QR is in charge of resolving or determining the balanced QoS and security needs of each user i according to her specification. On the other hand, TE acts as a monitoring stub (which was proposed in one of our earlier works [12]) to monitor and detect cyber threats to eventually evaluate the threat level in the network. Note that the threat level estimation is not covered in this paper and we assume that the TE has this functionality. As shown in Fig. 2, TE evaluates the threat level in the network and periodically notifies QR on the current threat level. Upon receiving user i's QoSSLS request, specified in the format described earlier through Fig. 1, QR needs to create an SLS response by assigning the highest possible balanced security and QoS levels to satisfy user i's requirement. Then, QR assesses if the SLS response provides adequate security to combat the current threat level in the network. In case QR finds the SLS response to be sufficiently secure under the prevailing threat, it issues an SLS response message to user i. User i then verifies whether the QoSS parameters in the SLS response message are acceptable. Upon finding acceptable terms, user i sends a confirmation message to QR that is referred to as the Quality of Security Service Level Agreement (QoSSLA).

In the next section, we present our envisioned QoSS approach based on game theory.

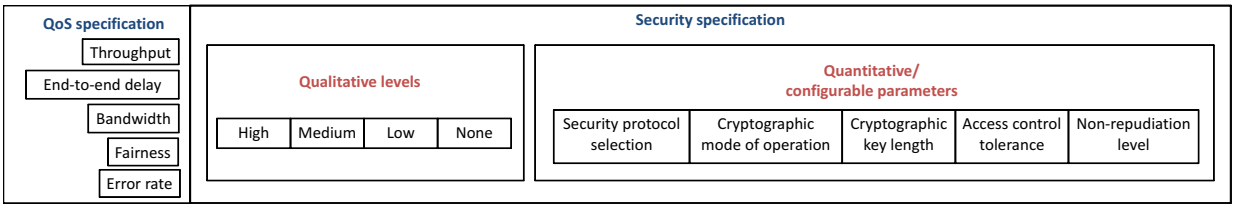

Fig. 1. Proposed Quality of Security Service Level Specification (QoSSLS) format.

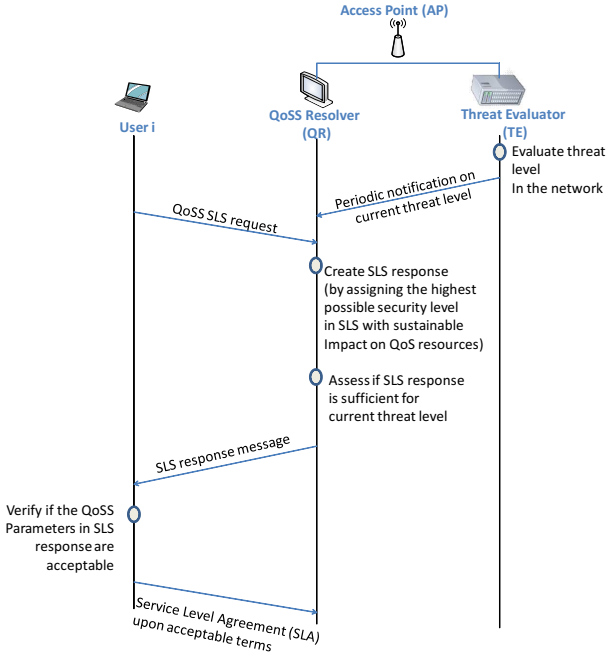

Fig. 2. Considered QoSS negotiation steps.

IV. Proposed QoSS Solution based upon Game Theory

Although achieving agreeable QoS is crucial for users, they may not be willing to achieve their intended QoS at the expense of arbitrarily low security levels. In this section, we model the users requesting for QoSS as "players". The main objective of our modeling is to derive an optimal QoSS assignment to the players using the mathematical analyses provided by the Game Theory framework described as follows.

We design a non-cooperative centralized game at the wireless AP to ensure the maximum QoS and security levels for all the players belonging to the AP. The game features a player i transmitting her QoSSLS request to the AP. The formulated game provides strategies to the players so that they may interact with the AP to decide upon their best QoSS level. The AP captures interaction between the players by allowing each player to be affected by the actions of all players, and not by her own action alone. Formally, the game is composed of a finite set of players, denoted by $A = a_1, a_2, ..., a_N$ and all the players have a common strategy space $\mathbf{S} = \mathbf{S_i}, \forall i$. The strategy space is constructed from the set of practically possible QoSSLSs, i.e., different QoSS expectations of the players. The game profile is defined as the Cartesian product of the players' strategy vector, $\mathbf{\Psi} = \times_{i \in \mathbf{A}} \mathbf{s_i} = \mathbf{s_1} \times \mathbf{s_2} \times \cdots \times \mathbf{s_N}$. Note that a game profile includes one strategy for each player. Also, $\mathbf{s_{-i}}$ is specially defined as the strategy set chosen by all other players except player i. The utility to any player depends on the entire strategy profile. During each game, the AP accepts QoSSLS requests from new players, or asks existing players to either retain or renegotiate their QoSSLSs. Player i has control over its own QoSSLS selection only, and it receives a utility for its selection.

For representing the game, let us suppose that player i has k^i pure strategies. Then, the number of pure strategies in the game is: $k = \sum_{i=1}^{n} k^i$. The number of pure strategies combinations in the game is given by $K = \prod_{i=1}^{n} k^i$. The players' pure strategies combinations are assigned numeric values or ranks as follows:

$$\begin{aligned} (s_1^1, s_1^2, ..., s_1^{n-1}, s_1^n) &= 1 \\ &\vdots \\ (s_{k^1}^1, s_{k^2}^2, ..., s_{k^{n-1}}^{n-1}, s_{k^n}^n) &= K \end{aligned} \tag{1}$$

where s_j^i denotes the j^{th} pure strategy of player i.

With respect to each pure strategies combination, a player receives an associated utility. In the considered non-cooperative game comprising n players and each player having $k^i, i = 1, 2, ..., n$ pure strategies, the utility matrix of each player can be constructed as a vector of length K. The overall utility matrix can be formulated as follows.

$$\begin{matrix} U_1^1 & U_1^2 & ... & U_1^n \\ U_2^1 & U_2^2 & ... & U_2^n \\ \vdots & & & \\ U_M^1 & U_M^2 & ... & U_M^n \end{matrix} \tag{2}$$

A mixed strategy of player i can be considered as a probability distribution over her strategy space S^i. Let the space of all mixed strategies of player i be represented by $\sum^i = \{\sigma^i \in \mathbb{R}^{k^i +} | \sum_{j=1}^{k^i} = 1\}$. In case of $\sigma^i \in \sum^i$, the probability assigned to pure strategy s_j^i is given by σ_j^i. The straegy space of the game is then $\Sigma = \prod_{i \in N} \sum^i$.

In case a mixed strategy combination σ is played, the probability that the pure strategies combination $s = (s_{j^1}^1, s_{j^2}^2, ..., s_{j^n}^n)$ occurs is given by $\sigma(s) = \prod_{i \in N} \sigma_{j^i}^i$. In this case, the utility allocated to player i is given by $U^i(\sigma) = \sum_{s \in S} \sigma(s) U^i(s)$, where $U^i(s)$ is the utility to player i at the pure strategies combination s.

Players will negotiate and change their interdependent strategies in $\mathbf{S}$ in order to achieve an optimal value for the network's aggregate utility. Then two important issues arise:

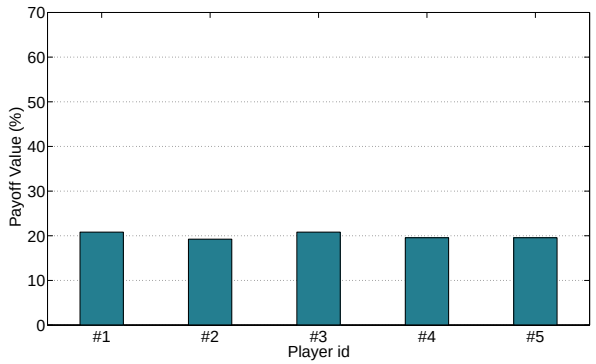

Fig. 3. Payoff values received by individual players in a five-player scenario.

(i) whether they ever reach a consensus, or a steady state, and (ii) if the steady state, indeed, exists, how efficient its performance would be. From this idea, there arises an important concept in Game Theory referred to as *Nash Equilibrium* (NE). The players will meet an agreement on a balanced QoSS level if NE exists. Formal definition of NE, as in [13], [14], is described below.

Definition 1. *σ^*, a mixed strategy profile, is an NE of the game if*

$$U^i(\sigma^*) \geq U^i(\sigma^{*-i}, \sigma^i), \quad \forall i \in N, \forall \sigma^i \in \Sigma^i. \tag{3}$$

According to this definition, for each player i, she cannot receive a better utility than that at the NE, by varying only her own mixed strategy while the other players' strategies remain unchanged. In other words, no player can benefit by deviating from her strategy if other players do not change theirs. Thus, the arrival at an NE guarantees an agreement for negotiations among players. Upon reaching this agreement, it is in the self-interest of each player regarding her expected QoSS to follow this agreement if the other players follow the same.

V. Performance Evaluation

In this section, we evaluate the performance of the game theoretic approach to QoSS provision using MATLAB [15]. For the simulation scenario, we consider a WLAN consisting of an AP in which the number of users/players are varied from two to ten. We consider three types of traffic, namely best effort, voice, and video traffic. For simplicity, we consider that the system (i.e., AP) initially presents different QoS and security options to the players for allowing them to construct SLS. In our conducted simulations, nine contrasting QoSS parameters are considered. Five of these are QoS parameters, and the remaining four are used for security provisioning. The QoS parameters are throughput, end-to-end delay, bandwidth ratio, fairness, and error rate. On the other hand, the considered security parameters are cryptographic algorithm selection, key size, access control, and authentication selection. In the following, we describe the used values of these different QoSS parameters in the conducted simulations.

For throughput assurance, a player may request any of the following three values $\{0.9, 0.75, 0.5\}$. These values represent the minimum throughput ratio expected by the player. For example, if a user specifies and is assured to receive QoS throughput 0.9, she can expect the AP to have adequate resources to avoid packet drop of 10% or lower. The lowest QoS throughput is considered to be 0.5, because this reflects the practical scenario whereby players using either best effort or real-time traffic would not want their expected throughput to drop below 50%. For the next QoS parameter, i.e., end-to-end delay, the system offers players three grades ($\leq$): 150ms, 300ms, and 500ms of end-to-end delay for audio, video, and best effort traffic, respectively. Next, bandwidth ratio in terms of the system offered bandwidth to the user requested bandwidth is offered with three options: $\{0, 0.5, 1\}$ to reflect the worst, average, and best bandwidth availability scenarios. Next, we consider fairness, meaning how fairly the AP will service a given player in contrast with service offered to the other players. Fairness ratio values of 0.25 to one in the interval of 0.25 are taken into account. The final QoS parameter is the bit error rate due to wireless channel conditions that is considered by the system in three grades of zero, 0.25, and 0.5. For example, a player specifying in her SLS an error rate of $\{$zero, 0.25$\}$ indicates that she wants the best possible service without any error rate, and if this is not possible she is willing to sacrifice up to 25% bit error rate. On the other hand, a player specifying only an error rate of zero represents the strict need of quality of service for the application run by that player.

The first security parameter considered is the algorithm selection. The players can choose from a wide range of cryptographic algorithms for encrypting/decrypting the traffic. The considered algorithms are Blowfish, RC6, AES, DES, 3DES, RC2, ECC, and RSA. Note that each of these have increasing order of impact on the end-to-end communication delay. The next security parameter taken into account is the cryptographic key size, where six different key sizes ranging from 164 bits to 1024 bits are used to reflect the increasing order of encryption strength. The values of the access control parameter are graded into four levels, namely $\{$zero, 0.25, 0.75, one$\}$. These values represent the tolerance level of a player to allow access to the AP. In other words, access control parameter value of zero refers to the strictest access control preference of the player, i.e., the player wishes not to be restricted by any access control by the AP. The last QoSS attribute is the authentication parameter. For simplicity, we only consider the presence or absence of Diffie-Hellman algorithm for performing AP-player authentication.

In order to implement the non-cooperative game over the strategies for each game and construct the utility values of the players, we need to normalize the afore-mentioned QoSS parameters and specify a weight for each of the parameters. For sake of simplicity and without any specific purpose, we set equal weights (0.2) to all the normalized parameters. Note that for the QoSS parameters which are required to be minimized from the players' point of view, the applied weight is set to negative. In the simulations, the number of players is varied from two to ten. For each simulation scenario, a player is arbitrarily assigned two to five different levels from which she can construct her SLS and request the AP on her preferred service and security grade.

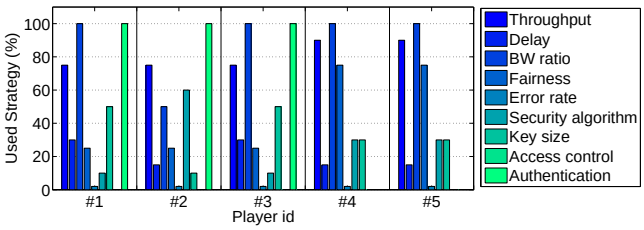

Fig. 4. Used strategies by individual players in the five-player scenario.

Based on the above scenario and simulation parameters, simulations were conducted a hundred times and the average of these simulation runs are used as results to reduce the impact of accidental/extreme simulation runs on the performance of the proposed approach. First, Fig. 3 demonstrates the payoff values of the individual players in a scenario consisting of five players. The player id in the figure refers to the individual users in this scenario. In the adopted approach, all the involved players play the proposed game until NE, and the results in this figure suggest that all five players receive similar payoff or utility values, approximately 20%. This means that the proposed game theoretic approach satisfies the players' expected QoSS levels in an even manner. To further analyze the individual QoSS components of each of these individual users, Fig. 4 demonstrates all nine QoSS component percentages obtained in the used strategies for the scenario comprising five players. For example, all the players receive more than 70% throughput. Amongst all the players, player #1 experiences the highest end-to-end delay (approximately 30%). This happens due to the arbitrary SLSs requested by the player #1 in different simulation trials. The adopted approach attempts at balancing all the QoSS parameters not only for player# 1 but also all other players, and the best delay assurance that it can give to player#1 is approximately 30%. The figure also projects other QoS and security components in the used strategy. From security point of view, players #1,2, and 3 receive authenticated communication with the AP as per their SLS requests while the remaining players are not required to do the same. The results also demonstrate that player #2 uses the strongest cryptographic algorithm in contrast with other players. In fact, the users are granted the strongest possible cryptographic suite according to their selected set of cryptographic algorithms. Thus, it is evident from these results that there are contrasting demands from two perspectives: (i) each individual player's demands for the nine QoSS componetns are different, and (ii) each player's demands for the overall QoSS are different from other users.

Finally, we investigate regarding the convergence time to Nash Equilibrium Point (NEP) for different numbers of players in the conducted simulations. The time to reach the convergence time increases with the number of players playing the adopted game. For the two-player game, it only takes tens of milliseconds. For up to four players involved in the adopted game, the convergence time to NEP remains below 100ms. However, for six players, the NE convergence time increases up to 800ms. When the number of players increases to seven, this exceeds 5s. In particular, for the ten users scenario, the average results from multiple simulation runs demonstrate that the NE convergence time takes nearly 300s. This is still acceptable given that this waiting time may be considered as a trade-off for all the users to gain their expected quality of service and security at the same time in a balanced manner rather than overwhelming the AP with their contrasting QoSS demands.

VI. CONCLUSION

While quality of service and security provisioning are interconnected, it becomes more difficult to provide the best possible QoS for different services with different security requirements as perceived by the users. In this work, we proposed a game theoretic approach to integrate both quality of service and quality of security. The proposed approach enables the users to participate in a non-cooperative game, which is played until the Nash equilibrium point is reached. Upon arriving at the Nash equilibrium, the users receive the best possible quality of secure service levels. Simulation results show that the proposed approach provides similar utilities or pay-offs to the users participating in the game. Also, it reveals complex and contrasting demands for different quality of service and security parameters both for individual and contending users.

REFERENCES

[1] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: An Overview," IETF, RFC 1633, Jun. 1994.
[2] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," IETF, RFC 2475, Dec. 1998.
[3] S. N. Foley, S. Bistarelli, B. O'Sullivan, J. Herbert, and G. Swart, "Multilevel Security and Quality of Protection," in *First Workshop on Quality of Protection*, Como, Italy, Sep. 2005.
[4] W. He and K. Nahrstedt, in "An Integrated Solution to Delay and Security Support in Wireless Networks," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Las Vegas, NV, USA, Apr. 2006.
[5] Z. Fadlullah, T. Taleb, N. Nasser, , and N. Kato, "Exploring the security requirements for quality of service in combined wired and wireless networks," in *Proc. IWCMC'09*, Leipzig, Germany, Jun. 2009.
[6] H. Otrok, M. Mehrandish, C. Assi, M. Debbabi, and P. Bhattacharya, "Game theoretic models for detecting network intrusions," *Computer Communications*, vol. 31, no. 10, Jun. 2008, pp. 1934-1944.
[7] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications*, vol. 31, no. 4, Mar. 2008, pp. 708-721.
[8] T. Alpcan and T. Basar, "A game theoretic analysis of intrusion detection in access control systems," in *Proc. 43rd IEEE Conf. on Decision and Control (CDC)*, Atlantis, Paradise Island, Bahamas, Dec. 2004.
[9] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. ACM GameNets'06*, Pisa, Italy, Oct. 2006.
[10] L. Chen and J. Leneutre, "A game theoretic framework of distributed power and rate control in ieee 802.11 wlans," *IEEE Journal on Selected Areas in Communications*, vo. 26, no. 7, Sep. 2008, pp. 1128-1137.
[11] L. Chen and J. Leneutre, "Selfishness, not always a nightmare: Modeling selfish mac behaviors in wireless mobile ad hoc networks," in *Proc. ICDCS'07*, Pisa, Italy, Oct. 2007.
[12] Z. M. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, and N. Kato, "Dtrab: Combating against attacks on encrypted protocols through traffic-feature analysis," *IEEE/ACM Transactions on Networking*, vol. 18, no. 4, Aug. 2010, pp. 1234-1247.
[13] A. Mackenzie, "Game Theory for Wireless Engineers," 1st ed. *Morgan & Claypool Publishers*, May 2006.
[14] B. Chatterjee, "An optimization formulation to compute Nash equilibrium in finite games," in *Proc. International Conf. on Methods and Models in Computer Science*, Delhi, India, Dec. 2009.
[15] MATLAB, available at: www.mathworks.com