A Trade-off Model for Performance and Security in Secured Networked Control Systems

Wente Zeng[1], *Student Member, IEEE*, Mo-Yuen Chow[1,2], *Fellow, IEEE*
[1]Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA
[2]College of Electrical Engineering, Zhejiang University, Hangzhou, Zhejiang Province, China
wzeng3@ncsu.edu, chow@ncsu.edu

Abstract – **Networked Control Systems (NCS) is a fast growing technology that integrates distributed sensors, actuators, and computing processors over a communication network for a vast amount of applications. However, the NCS can be vulnerable to various network attacks when the network used is insecure (e.g., Internet). Thus, secure NCS need to have embedded security mechanism to ensure its security operating requirements, which may sacrifice its performance due to limited system resources. This paper addresses the trade-off between NCS security and its real-time performance and use a secured networked DC motor system for illustration. This paper will present a trade-off model for system dynamic performance and system security. This model can be used to adapt security configurations to provide sufficient protection and satisfy real-time dynamic performance requirements of the NCS simultaneously. The construction of this model includes the development of a set of metrics to quantitatively measure the performance and security levels of NCS and the development of a trade-off objective function incorporating performance and security. A Simulink based test-bed implemented to control the speed of the DC motor is used to illustrate the effectiveness of this model.**

I. INTRODUCTION

With the rapid advancements in networking, embedded systems, and wireless communication technologies in recent years, researches on the NCS have been gaining increasing attentions due to their high potential in widespread applications [1]. Nowadays, the NCS implementations become even easier with the large deployments of wireless systems, which give rise to a wide variety of applications like monitoring and operating manufacturing plants, space projects, robot navigations, traffic management and many more over the years. However, wireless medium is susceptible to easy intercepting, which may pose increasing concern on the protection of communication security. Besides, to reduce operational costs and increase flexibilities, NCS have been transitioned to less expensive standardized technologies, operating systems and protocols currently prevalent, e.g., on the Internet. As a result, real-time monitoring and control information is readily and easily accessible to a large number of people connected to the Internet, which also increases the vulnerability of the NCS to network malicious attacks. Therefore, the data sharing and communication security is of utmost concern in NCS considering the time and data sensitive applications. It is critical to protect transmitted data from unauthorized access and modifications in communication channels of NCS.

The traditional NCS designed without security protection are vulnerable to various security attacks. There is a growing demand of efficient and scalable Intrusion Detection Systems (IDS) embedded in the NCS. Furthermore, using security in an NCS gives rise to many topics like network architecture to support security for NCS, the performance assessment for NCS with security etc. Cardenas et al. [2] gave an overview of security issues in Cyber Physical Systems (CPS), identified and defined the problem of secure control and proposed a set of challenges that need to be addressed to improve the survivability of CPS. Mukherjee [3] established a Criticality Response Modeling (CRM) framework to ensure the networked control system has criticality-awareness – the ability of the system to respond to unusual situations. Tsang and Kwong [4] proposed an efficient and biologically inspired learning model for multi-agent IDS utilized in the network infrastructures of industrial plants. Creery and Byres [5] presented methods to determine and reduce the vulnerability of NCS to unintended and malicious intrusions for an industrial plant. Xu et al. [6] developed core architecture to address the collaborative control issues of distributed device networks under open and dynamic environments by adopting policy-based network security and XML technologies. Gupta et al. [7-8] characterized the NCS application on the basis of security effect on NCS performance and mapped the added security features to additional time delay in the system to show this trade-off for a wireless NCS robot path tracking application.

Although NCS with security from a control system perspective is still in its infancy, many NCS have been well protected by security mechanisms as stated above. However, the added security features may sacrifice system dynamic performance due to limited system resources. The impact of the security mechanisms on the system dynamic performance has not been addressed thoroughly. Security requirements are often in conflict with other performance requirements, like real-time dynamic performance due to limited system resources and extra time delay imposed by security additions.

Motivated by the above analysis, this paper investigates the effect of the addition of security mechanisms in NCS. In this paper, a secured networked DC motor system is used to illustrate the proposed concept. The DC motor dynamics is modeled by differential equations, while the security mechanisms are modeled by discrete events. A trade-off model for the dynamic performance and security in this secured NCS is established. The construction of the trade-off model involves the development of: (1) a set of metrics to quantitatively measure the DC motor closed-loop dynamic performance and

978-1-4244-9312-8/11/$26.00 ©2011 IEEE

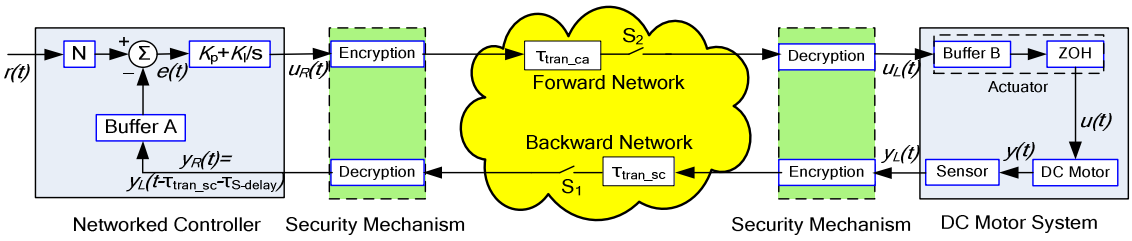

Fig. 1: The structure of the secured networked DC motor system

security levels, and (2) a trade-off objective function incorporating both the performance and the security metrics simultaneously.

The remaining sections are organized as follows: Section II provides the system structure and description of the secured networked DC motor system. Section III describes the trade-off model for performance and security in the secured NCS. The implementation of the Simulink based test-bed is described in section IV, while the test conditions and result analysis are presented in section V. Section VI concludes the paper and briefly discusses the future work.

II. System Description

A secured networked DC motor system is depicted in Fig. 1, where the sensor and the actuator are time-driven with the same synchronized sampling period. The controller is event driven as the controller signal is calculated as soon as the sensor data is available on the controller side. The security mechanism is also event driven by the detection of adversary attacks. This secured networked DC motor system can be divided into four parts: (1) The local DC motor system (including the actuator, the DC motor and the sensor); (2) The networked controller; (3) The security mechanism; and (4) The communication network [9-10]. Each component is described in the following sections.

A. The Local DC Motor System

The electromechanical dynamics of the DC motor is described as:

$$\dot{i}_a = -\frac{R}{L} i_a - \frac{K_b}{L}\omega + \frac{1}{L}u, \tag{1}$$

$$\dot{\omega} = \frac{K_t}{J} i_a - \frac{B}{J}\omega, \tag{2}$$

where i_a is the armature winding current; ω is the rotor angular speed; R is the armature winding resistance; L is the armature winding inductance; K_b is the back-electromotive-force (EMF) constant; K_t is the torque constant; J is the system moment of inertia; B is the system damping coefficient. u is the armature winding input voltage.

Let $x = [x_1, x_2]^T = [i_a, \omega]^T$, the system output is the rotor angular speed $y = \omega$, the DC motor system can be expressed by the state-space equations:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} -\frac{R}{L} & -\frac{K_b}{L} \\ \frac{K_t}{J} & -\frac{B}{J} \end{bmatrix} x(t) + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} u(t) \tag{3}$$

$$y(t) = \begin{bmatrix} 0 & 1 \end{bmatrix} x(t) \tag{4}$$

For simplicity, we assume that the local controller only simply convert the control voltage data sent from the networked controller into a PWM signal to drive the DC motor. Thus $u_L(t) = u(t)$, where $u_L(t)$ is the input of the local controller. Besides, we denote $y_L(t)$ as the output of the sensor measuring the system's rotor angular speed y. Thus, $y_L(t) = y(t)$.

B. The Networked Controller

The system uses a PI controller to control the DC motor's speed:

$$u_R(t) = K_p e(t) + K_i \int_0^t e(\tau) d\tau \tag{5}$$

$$e(t) = r(t) - y_R(t) \tag{6}$$

where $u_R(t)$ is the control signal from the networked controller to the local controller; $r(t)$ is the referenced speed; $y_R(t)$ is the measured signal received from the sensor. K_p and K_i are the proportional and integral gain for the PI controller to be designed.

C. The Security Mechanism

This paper will focus on the confidentiality aspect of security service using secret key cryptography. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are two symmetric ciphers which are considered secure for wireless systems. DES is one of the most important classical cryptosystems in the history of cryptography. 3DES is very similar to DES and requires three keys (encryption-decryption-encryption) to provide stronger security than DES. Consequently, 3DES is 3 times slower than DES. AES, a successor of DES, works with 128 bits of block size with key sizes 128 or more. As ECB (Electronic Code Book) is considered the fastest mode of operation, it is used commonly in real time systems. Therefore, in this paper, secret key algorithms DES, 3DES and AES [11] with ECB mode are embedded in the NCS to encrypt and decrypt the information flow between the networked controller and the DC motor system [12].

With different encryption algorithms, the security mechanism is modeled as a discrete event system [13], which has three parts: security sensors, security decisions and security actuators.

Security Sensors: to receive the sensor data to check if the system is under attack.

Security Decisions: to process the sensor data, make security decisions (decide which encryption algorithm to use).

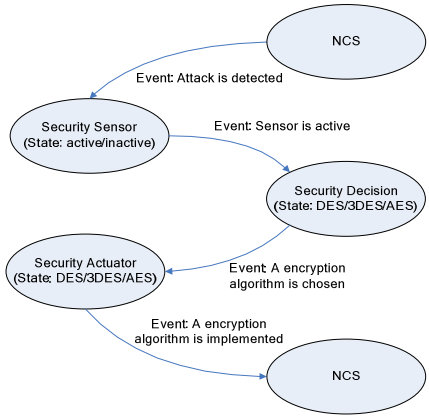

Fig. 2: State flow of the security mechanism based on discrete events

Security Actuators: to encrypt the data packet and result in additional time delay in the system.

The state flow of the security mechanism is shown in Fig. 2. There are four steps in this discrete event process: 1) the security sensors read Boolean status variables from the input at each update and the event that the input is true can trigger its state to active. 2) When the sensor status is active, a broadcast event is sent to the security decision state; 3) An event of changing the security decision state can trigger the security actuator state change from one to another; 4) An event of changing the security actuator state is sent to NCS.

D. The Communication Network

The data packets in the networked DC motor system usually suffer time delay during the transmissions. So we let τ_{sc} denote the sensor-to-controller time delay and τ_{ca} denote the controller-to-actuator delay. Then the total Round Trip Time (RTT) delay can be described as:

$$\tau_{RTT} = \tau_{sc} + \tau_{ca} \tag{7}$$

And τ_{sc} and τ_{ca} can be described as:

$$\tau_{sc} = \tau_{tran\_sc} + \tau_{S-delay}, \tag{8}$$

$$\tau_{ca} = \tau_{tran\_ca} + \tau_{S-delay}, \tag{9}$$

where τ_{tran_sc} and τ_{tran_ca} are the transmission delays; $\tau_{S-delay}$ is the extra time delay imposed by security additions.

Thus, the signal relationship between the networked controller and the local controller and sensors are:

$$u_L(t) = u_R(t - \tau_{ca}) \tag{10}$$

$$y_R(t) = y_L(t - \tau_{sc}) \tag{11}$$

III. THE TRADE-OFF MODELING

A. The Performance Metric

NCS may have different performance requirements for different applications. This paper focuses on the main impact of security mechanisms on the real-time dynamic performance of the system.

We use three measures 1) the mean square error J_1, 2) the percent overshoot J_2 and 3) the rising time J_3 to evaluate the system dynamic performance:

$$J_1 = \begin{cases} 0 & , \quad MSE \le MSE^* \\ \dfrac{(MSE - MSE^*)}{MSE^*} & , \quad MSE > MSE^* \end{cases} \tag{12}$$

$$J_2 = \begin{cases} 0 & , \quad P_{OS} \le P_{OS}^* \\ \dfrac{(P_{OS} - P_{OS}^*)}{P_{OS}^*} & , \quad P_{OS} > P_{OS}^* \end{cases} \tag{13}$$

$$J_3 = \begin{cases} 0 & , \quad t_s \le t_s^* \\ \dfrac{(t_s - t_s^*)}{t_s^*} & , \quad t_s > t_s^* \end{cases} \tag{14}$$

$$MSE = \frac{\sum_{K=1}^{N} e^2(KT)}{N} = \frac{\sum_{K=1}^{N} [r(KT) - y(KT)]^2}{N} \tag{15}$$

where MSE is the mean square error of the speed tracking. MSE^* is the nominal mean squared error; P_{OS} is the percentage overshoot of the controlled signal value and t_S is the setting time of the system. P_{OS}^* and t_S^* are the nominal values of percentage overshoot and setting time. They are the nominal performance criteria that the system should achieve without time delay in the control loop.

The corresponding cost function can be defined as follows:

$$J = w_1 J_1 + w_2 J_2 + w_3 J_3 \tag{16}$$

where w_1, w_2 and w_3 are the weight factors. They are used to specify the relative significance of J_1, J_2 and J_3 on the overall system performance and map to a scalar measure.

Then, the cost function J is inversed and normalized to define a system performance metric P:

$$P = \frac{J_{\min}}{J}, \; 0 \le P \le 1 \tag{17}$$

where J_{min} is the minimum J that can be obtained.

B. The Security Metric

Existing qualitative metrics classify various security mechanisms to several discrete levels, such as low, medium, and high. Security mechanisms in the higher level can provide better protection than lower levels. However, it is impossible to compare security mechanisms within the same security level. Furthermore, qualitative metrics are too coarse for fine control of the tradeoff between NCS dynamic performance and security. Thus, a quantitative metric that generates a security strength value for each security mechanism is used in this paper, and hence is more suitable for quantitative comparison of the security strength of any two security mechanisms [14].

Without considering any shortcut attacks, brute force attack is the only way used to crack the encryption key in this paper. For example, a DES cipher with a key length of 56 bits has 2^{56} possible key combinations. Assuming unit complexity for testing one key, the worst-case complexity involved in cracking this 56-bit DES cipher is 2^{56}. With this assumption, the security level of an encrypted message frame is decided by its encryption key length. Thus, a security measure with respect to brute force attacks is described to be

$S(N) = log_2(N)$, where N is the encryption key length. Let a message consist of n frames with encryption key length N_i bits for frame $i = 1,2,\dots,n$, and assume that every frame of this message is equally important to decrypt the message, then a reasonable security measure for the whole message is the mean of the security levels achieved by the individual frames [15]. Therefore, the security level is measured by the vulnerability of encryption algorithms to brute force attackers, which denotes the security metric S:

$$S = \frac{1}{nS_{\max}} \sum_{i=1}^{n} \log_2 N_i \,,\ 0 < S < 1 \tag{18}$$

where $S_{max} = max\ (log_2 N_i)$.

C. Performance and Security Requirements

With the defined performance metric P and security metric S, the system requirements can be formulated quantitatively.

The dynamic performance and security operations depend on the operating requirements. For example, the DC motor needs to reach a reference speed in a certain time within a certain overshoot and a certain tracking error, while satisfying the required security level. This could also be called as the minimum requirements that need to be satisfied:

$$P > P_o \,,\ S > S_o \tag{19}$$

where P_o is the operating requirements of the system dynamic performance; S_o is the operating requirement of the system security level.

Secondly, the control system should have a feasible operating region. Out of this region, the system may have oscillation, even out of control. Thus, P and S must be within this stable region. This could be called as the stabilization requirements that need to be satisfied:

$$P < P_s \,,\ S < S_s \tag{20}$$

where P_s is the stabilization requirement of the system dynamic performance; S_s is the stabilization requirement of the system security level.

By combining these two parts together, the overall system dynamic performance and security requirements cab be described as follows:

$$P_o < P < P_s \,,\ S_o < S < S_s \tag{21}$$

D. The Trade-off Objective Function

The dynamic performance and security metrics allow us to quantitatively calculate how much protection a security mechanism can provide and how much dynamic performance will be reduced by using that security mechanism. Hence, we can make the trade-off between dynamic performance and security by adjusting the system control inputs and security parameters, within the boundary of the system requirements.

When both the dynamic performance and security requirements are satisfied, the system is capable of using the available resources for improving the performance and/or the security. A tradeoff objective function between the performance metric and the security metric can be formulated as a utility function:

$$\text{Max } U = w_{u1} P + w_{u2} S$$
$$\text{with } P_o < P < P_s \,,\ S_o < S < S_s \tag{22}$$

where w_{u1} and w_{u2} ($w_{u1} + w_{u2} = 1$) are two weighting factors representing the preferences on performance and security, respectively.

With the objective function U, the system can compute and choose the best security parameters together with optimal control inputs according to the system requirements to achieve the best trade-off between dynamic performance and security.

IV. Simulink Based Test-bed Description

We developed a Simulink based test-bed to evaluate the trade-off model in the secured networked DC motor system in real-time with utility constraints and varying inputs. The DC motor system was embedded with a networked PI controller to control the speed of the motor over a network.

As shown in Fig. 3, the test-bed is implemented in Matlab Simulink according to the system description in Section II. The DC motor dynamics is simulated using equations (3) and (4). A wireless network environment with random time delay and packet drop rate was simulated such that each desired network parameter can be user controlled. The network security algorithms were implemented on this test-bed to study the effect of network security additions. In DES/3DES and AES, the total time for encryption as well as decryption depends upon the encryption key length between controller and the plant. Experiments were performed on a Linux Machine (Kernel 2.4.18-3 i386) to find out the mean processing time for DES, 3DES and AES, and the statistic results are shown in Table I. While the DC motor system dynamics is implemented in the continuous domain, the security mechanism is simulated as a discrete event system by the State Flow in the Simulink, which is also a subsystem of the encryption/decryption blocks in Fig. 3.

TABLE I: Induced Time-delay with respect to Security Algorithms

Encryption Algorithms	DES	3DES	AES
Processing Delay (ms)	21.1	54.1	68.5

V. Test Conditions and Result Analysis

A. Test Conditions

The parameters of the DC motor are listed in Table II. To achieve the desired closed loop performance, the nominal gains have been tuned to be $K_p = 1$ and $K_i = 0.01$. The sensor and the output data are sampled with sampling period $h = 1$ ms by considering the buffer size equals to 1.

The network transmission delay on the Internet is random in nature. Generally speaking, it is in the order of a few hundreds of millisecond, typically 100 ms to 600ms on the Internet. Therefore, $\tau_{\text{tran\_sc}}$ and $\tau_{\text{tran\_ca}}$ is set to be in the range of [100ms, 600ms]. The additional time delay imposed by the security additions, $\tau_{\text{S-delay}}$, is simulated according to the statistic results of the processing delay for DES, 3DES and AES, which have been shown in Table I.

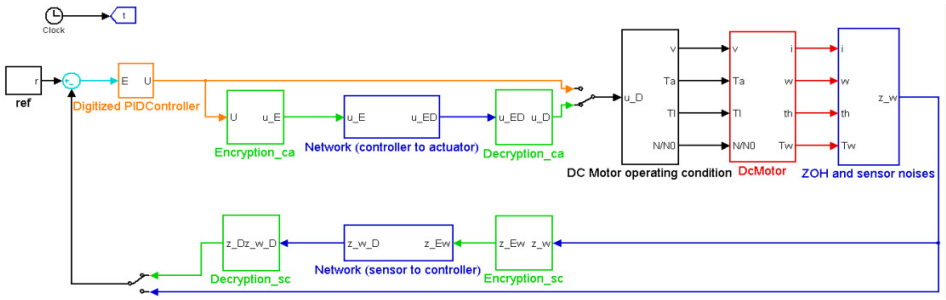

Fig. 3: Simulink based test-bed for the secured networked DC motor system

TABLE II: THE PARAMETERS OF THE DC MOTOR

J	Motor Moment of Inertia	$3.53 \times 10^{-5} kg \cdot m^2$
L	Motor Winding Inductance	$2.88 \times 10^{-3} H$
R	Motor Winding Resistance	6.43Ω
K_t	Electric Torque Constant	$2.55 \times 10^{-2} N \cdot m/A$
K_b	Back-EMF Gain Constant	$2.55 \times 10^{-4} V \cdot s/rad$

The performance metric specifications for the networked DC motor speed control system are:

– Mean square error of the speed tracking: $MSE^* \leq 0.05$;

– Percentage overshoot: $P_{OS}^* \leq 15\%$;

– 5% settling time: $t_S^* \leq 5s$;

– $w_1 = w_2 = w_3 = 1/3$.

The security metric specifications for the networked DC motor speed control system are:

No security: $N = 1$; DES: $N = 56$; 3DES: $N = 112$; AES: $N = 128$; $S_{max} = log_2 128$.

B. *Result Analysis (static case)*

Our experimental task is to drive the networked DC motor to a reference speed 50 rad/s with different encryption algorithms. Fig. 4 shows the system dynamic performance and security levels using different encryption algorithms. The security level increases while the dynamic performance level decreases with respect to different encryption algorithms. A paired t-test was conducted to compare the mean dynamic performance and security levels of different encryption algorithms using 10 samples in each algorithm.

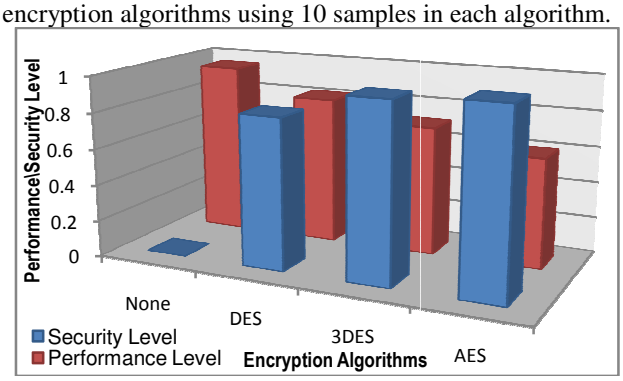

Fig. 4: The system performance and security levels using different encryption algorithms

As we can see in Table III, all the confidence levels do not cover zero, all of these conditions conclude that there is a statistically significant difference between the performance and security levels for each pair of compared algorithms at 5% level of significance. Therefore, as we increase the security level, statistically, there is a significant reduction in the performance level. Table IV shows the averaged amount of reduction in the performance levels of different encryption algorithms as compared to the condition without encryption algorithms. This value was computed as:

$$\% \text{ Reduction} = \frac{P_{none} - P_{DES/3DES/AES}}{P_{none}} \times 100\% \qquad (22)$$

TABLE III: PAIRED T-TEST COMPARING THE MEAN PERFORMANCE AND SECURITY LEVELS OF DIFFERENT ENCRYPTION ALGORITHMS

Pair of Encryption Algorithms	Security Level Difference	95% CI of Performance Level Difference
(None, DES)	0.8296	[-0.1438, -0.1316]
(DES, 3DES)	0.1429	[-0.1156, -0.0954]
(3DES, AES)	0.0275	[-0.1295, -0.0819]

Table IV suggests that the reductions in performance level are practically significant due to different encryption algorithms. This means encryption algorithms do have significant effect on NCS performance and our model can show this trade-off quantitatively clearly.

TABLE IV: PERCENTAGE REDUCTION IN PERFORMANCE LEVEL USING DIFFERENT ENCRYPTION ALGORITHMS

Encryption Algorithm	DES	3DES	AES
% Reduction	14.42%	25.48%	36.55%

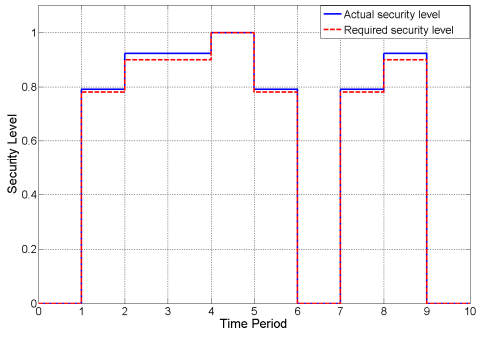

Fig. 5: The comparison between the required security level and actual security level of the secured networked DC motor system

C. *Result Analysis (dynamic case)*

Let us carry out the same task above while satisfying the following dynamic security level (the dash line in Fig. 5). There are 10 different security requirements in 10 different consecutive time periods. In order to fulfill the requirement, different encryption algorithms are applied in 10 time periods in the simulation (listed in Table V). After applying the security mechanisms above, the actual security level

achieved in the system is shown in Fig. 5 in solid line. Since the actual security level is above the minimum required security level, the comparison indicates that the security mechanisms applied in the simulation have satisfied the minimum system security requirements.

TABLE V: THE SECURITY MECHANISMS CONFIGURATION

TIME PERIOD	SECURITY ALGORITHM	KEY LENGTH
1	None	1
2	DES	56
3	3DES	112
4	3DES	112
5	AES	128
6	DES	56
7	None	1
8	DES	56
9	3DES	112
10	None	1

While maintaining the required minimum security level, we ran the simulation through the 10 time periods and measured the corresponding system performance and security levels. Fig. 6 shows the averaged system performance and security levels in 10 consecutive time periods based on 10 repeated simulations. As we can see, the trade-off between the system performance and security of the secured networked DC motor system is presented clearly. Apparently, the trade-off model and its relevant metrics show the trade-off between performance and security of the secured networked DC motor system very well, which demonstrates that the proposed trade-off model provides a satisfactory quantitatively performance and security measurements for the NCS.

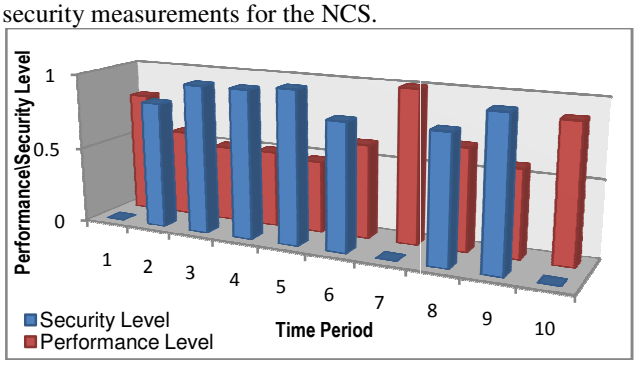

Fig. 6: The trade-off between the system performance and security of the secured networked DC motor system

VI. CONCLUSION AND FUTURE WORK

This paper has modeled a secured networked DC motor system by differential equations and the discrete event system and then presented a trade-off model in this system for showing the trade-off between system performance and security with limited resources. The quantitative performance and security metrics have been developed and combined in a tradeoff objective function with two weighting factors representing the preferences on performance and security. The simulation results are given to show the effectiveness of the trade-off model and its corresponding performance and security metrics.

Future researches include how to achieve the maximum performance, the maximum security and the optimized balance between performance and security by adjusting the weighting factors based on the trade-off model. Furthermore, more experiments are needed to conduct the study about improving the security metric when other security mechanisms are involved, e.g., QoS and intrusion detections.

ACKNOWLEDGMENT

This research was supported under NSF-ECS-0823952 “Impaired Driver Electronic Assistant (IDEA)” project.

REFERENCES

[1] Gupta R., Chow M.-Y., “Networked Control System: Overview and Research Trends,” Industrial Electronics, IEEE Transactions on , vol.PP, no.99, pp.1-1, 2009

[2] Cardenas A.A., Amin S., Sastry S., “Secure Control: Towards Survivable Cyber-Physical Systems,” Distributed Computing Systems Workshops, 2008. ICDCS08. 28th International Conference on, pp.495-500, 17-20 June 2008

[3] Mukherjee, T., Gupta, S.K.S., “A Modeling Framework for Evaluating Effectiveness of Smart-Infrastructure Crises Management Systems,” Technologies for Homeland Security, 2008 IEEE Conference on, pp.549-554, 12-13 May 2008

[4] Tsang C-H, Kwong S., “Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction”, IEEE International Conference on Industrial Technology, 14-17 Dec. 2005 Page(s):51 – 56.

[5] Creery A., Byres E.J., “Industrial cyber security for power system and SCADA networks”, Industry Applications Society 52nd Petroleum and Chemical Industry Conference, 12-14 Sept. 2005 Page(s):303 – 309.

[6] Xu Y, Song R, Korba L, Wang L, Shen W, Lang S, “Distributed Device Networks With Security Constraints”, IEEE Transactions on Industrial Informatics, Vol. 1, No. 4, November 2005.

[7] Gupta R. A., Chow M.-Y., Agarwal A., Wang W., “Information security with real-time operation: performance assessment for next generation wireless distributed networked-control-systems”, 33rd Annual Conference of the IEEE Industrial Electronics Society, November 5-8, 2007, Taipei, Taiwan.

[8] Gupta R. A., Agarwal A., Chow M.-Y., Wang W., “Performance assessment of data and time-sensitive wireless distributed networked-control-systems in presence of information security”, Military Communication Conference, October 29-31 2007.

[9] Li Hongbo, Chow Mo-Yuen, Sun Zengqi, “Optimal Stabilizing Gain Selection for Networked Control Systems With Time Delays and Packet Losses,” Control Systems Technology, IEEE Transactions on , vol.17, no.5, pp.1154-1162, Sept. 2009

[10] Li Hongbo, Chow Mo-Yuen, Sun Zengqi, “EDA-Based Speed Control of a Networked DC Motor System With Time Delays and Packet Losses,” Industrial Electronics, IEEE Transactions on, vol.56, no.5, pp.1727-1735, May 2009

[11] Kaufman C., Perlman R, Speciner M., “Network Security: Private Communication in a Public World”, Prentice Hall, Englewood Cliffs, New Jersey, 1995. 504 pp. (ISBN 0-13-061466-1).

[12] Gupta R.A., Chow M.-Y., “Performance assessment and compensation for secure networked control systems,” Industrial Electronics, 2008. IECON 2008. 34th Annual Conference of IEEE, pp.2929-2934, 10-13 Nov. 2008

[13] Zhai Y., Ning P., Iyer P., Reeves D.S., “Reasoning about complementary intrusion evidence,” Computer Security Applications Conference, 2004. 20th Annual, pp. 39- 48, 6-10 Dec. 2004

[14] Yau S.S., Yin Yin, An H.G., “An Adaptive Tradeoff Model for Service Performance and Security in Service-Based Systems,” Web Services, 2009. ICWS 2009. IEEE International Conference on, pp.287-294, 6-10 July 2009

[15] Haleem M.A., Mathur C.N., Chandramouli R., Subbalakshmi K.P., “Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks,” Dependable and Secure Computing, IEEE Transactions on, vol.4, no.4, pp.313-324, Oct.-Dec. 2007