I.J. Computer Network and Information Security, **2014, 1, 78-85**
Published Online November 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.01.10

Security Solutions for Networked Control Systems Based on DES Algorithm and Improved Grey Prediction Model

Liying Zhang
University of Science and Technology Beijing, Beijing, 100083 China
zly__1021@163.com

Lun Xie, Weize Li and Zhiliang Wang
University of Science and Technology Beijing, Beijing, 100083 China
Corresponding author Email: xielun@ustb.edu.cn

Abstract—Compared with the conventional control systems, networked control systems (NCSs) are more open to the external network. As a result, they are more vulnerable to attacks from disgruntled insiders or malicious cyber-terrorist organizations. Therefore, the security issues of NCSs have been receiving a lot of attention recently. In this brief, we review the existing literature on security issues of NCSs and propose some security solutions for the DC motor networked control system. The typical Data Encryption Standard (DES) algorithm is adopted to implement data encryption and decryption. Furthermore, we design a Detection and Reaction Mechanism (DARM) on the basis of DES algorithm and the improved grey prediction model. Finally, our proposed security solutions are tested with the established models of deception and DOS attacks. According to the results of numerical experiments, it's clear to see the great feasibility and effectiveness of the proposed solutions above.

Index Terms—Security solutions, NCS, DES, detection and reaction mechanism (DARM), grey prediction model.

I. INTRODUCTION

The wide application of network brings in a lot of convenience for industrial control systems, as well as many security vulnerabilities, and more and more incidents at critical infrastructures have been reported. So how to effectively secure NCSs has gone 'mainstream' in terms of public awareness of the threat to them from hackers, cyber spies and terrorists. Consequently, many researchers have shown great concern for the security solutions for NCSs.

DACFEY DZUNG in [1] gives an overview of IT security issues in industrial automation systems, analyses the industrial communication systems' security-relevant characteristics distinct from the general IT systems in detail. Rachana Ashok Gupta in [2] introduces and discusses the different forms of NCSs and possible future directions. As well as [3], Eric Byres and P. Eng summarize the incident information collected in Industrial Security Incident Database (ISID), analyses the consequences of industrial cyber attacks, and identifies the lessons that can be learned from these security events. Alvaro A. C ́ardenas and Saurabh Amin in [4] identify and define the problem of secure control, then propose a set of challenges that need to be addressed to improve the survivability of cyber-physical systems. A. A. Creery in [5] and Peng Jie in [6] present the security vulnerabilities of today's industrial control networks. All the above shows good understanding of the security issues of NCSs, and it's urgent to take some measures to secure NCSs.

Swaminathan P in [7], as well as PANG Zhonghua in [8] analysis and compare several typical encryption algorithms, then introduce DES is the fastest one of them and enough to guarantee the security of the data transmitted in NCSs. Ke-Ya Yuan in [9] describes the advantages of DES algorithm, the hardware and software design of the DES encryption algorithm. So, in this paper we also use the DES algorithm for data encryption and decryption.

Zhong-Hua Pang and Guo-Ping Liu in [10] and [11] design and implement a secure transmission mechanism，which integrates the Data Encryption Standard (DES) algorithm, Message Digest (MD5) algorithm and timestamp strategy. Zhong-Hua Pang in [8] proposes a detection scheme to detect the deception attacks on the backward channel of NCSs integrating the DES algorithm and strong tracking filter (STF). While complex algorithms applied to the NCSs for security will make the performance of the control systems reduce greatly.

Andr ́e Teixeira in [12] deals with two types of attacks: attacks on the network nodes and attacks on the communication between the nodes, and discusses how to reduce the number of observer nodes. Alvaro A. C ́ardenas in [13] propose a new mathematical framework to analyze attacks against control systems, and formulate specific research problems to detect attacks and survive attacks. Wente Zeng in [14] and [15] propose the impact

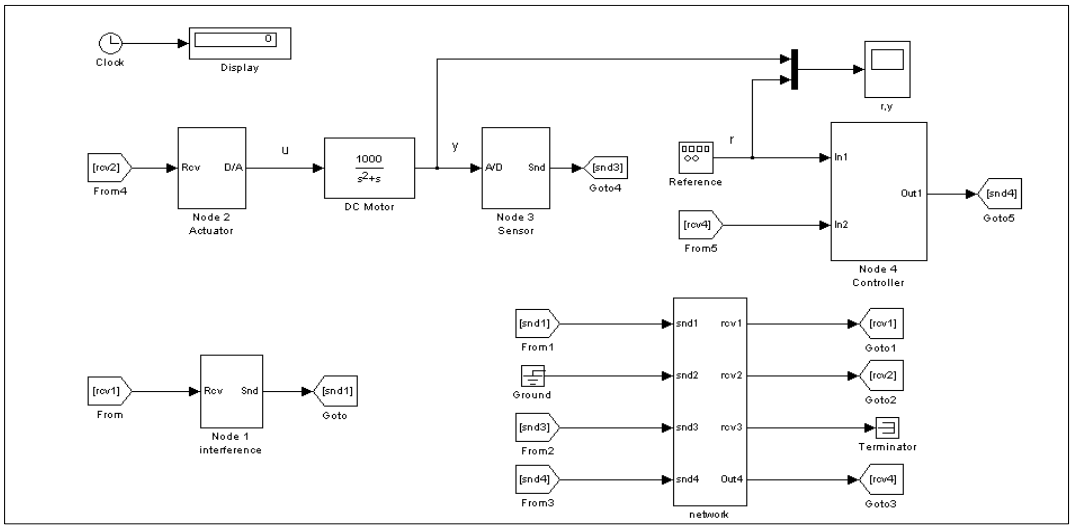

Figure 1. Simulation platform

of the security policy on system performance, and then present a trade-off model for system dynamic performance and system security. As well as Rachana A Gupta and Mo-Yuen Chow, in [16] addresses the issue of NCS information security as well its time-sensitive performance and their trade-off. [17] develop several attack scenarios and evaluate the impact of denial of service (DOS) attacks on scalar linear systems, while [18] analyze the performance of a proportional-integral controller (regulatory layer), and a model-based diagnostic scheme (supervisory layer) under a class of deception attacks. Alvaro A. Cárdenas in [19] explore security mechanisms that detect attacks by monitoring the physical system under control, and the sensor and actuator values, then develop a new attack detection algorithm and study the methodology on how to evaluate anomaly detection algorithms and their possible response strategies. While most of the research efforts focus on prevention (authentication, access controls, cryptography etc) or detection (intrusion detection systems), in practice there are quite a few response mechanisms.

Grey theory is a truly multidisciplinary and generic theory, as it is introduced in [20], and grey forecasting models have been extensively used in many applications. Qi Xie and Yan Xie in [21] introduced grey forecast modeling is the most important part of gray theory, and it is widely used in the various fields for the forecast because of less information needs and conveniently computing. Jianfeng Dong in [22] presents a network security situation evaluation and prediction model based on grey theory, and the model includes two parts: current situation evaluation and future situation prediction. Given the above, in this paper, we use grey theory to predict legal data of the next moment.

In this paper, we implement security solutions for the DC motor networked control system in TrueTime platform, and some numerical simulations are carried out. In part Ⅱ of the paper, we introduce the setup of simulation DC motor networked control system, followed by part Ⅲ where we propose related work for security solutions. Part Ⅳ presents the model of deception and DOS attacks. In part Ⅴ we analyze the results of numerical simulations and show the good feasibility and effectiveness of the above security solutions. Conclusion can be seen in part Ⅵ.

II. SETUP OF SIMULATION SYSTEM

In this brief, we build a DC motor networked control system in TrueTime as Fig. 1 shows. Among them, the actuator, sensor, controller and interference nodes are simulated by four kernel blocks respectively, while a real-time network block is used as the network. Furthermore, the sensor node is assumed to be time driven, whereas the controller and actuator nodes are event driven.

The model of DC motor and the control algorithm which is applied into the system are described in detail as following.

A. Mathematical model of the DC motor

As we all known, the electromechanical dynamics of the DC motor can be described as:

$$\frac{di_a}{dt} = -\frac{R}{L}i_a - \frac{K_b}{L}\omega + \frac{1}{L}u \tag{1}$$

$$\frac{d\omega}{dt} = \frac{K_t}{J}i_a - \frac{B}{J}\omega \tag{2}$$

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

Then we can obtain the transfer function after Laplace transform of the above two equations:

$$H(s) = \frac{A}{Bs^2+Cs+D} \tag{3}$$

Let A=1000, B=C=1, D=0, then the DC motor process can be specified as:

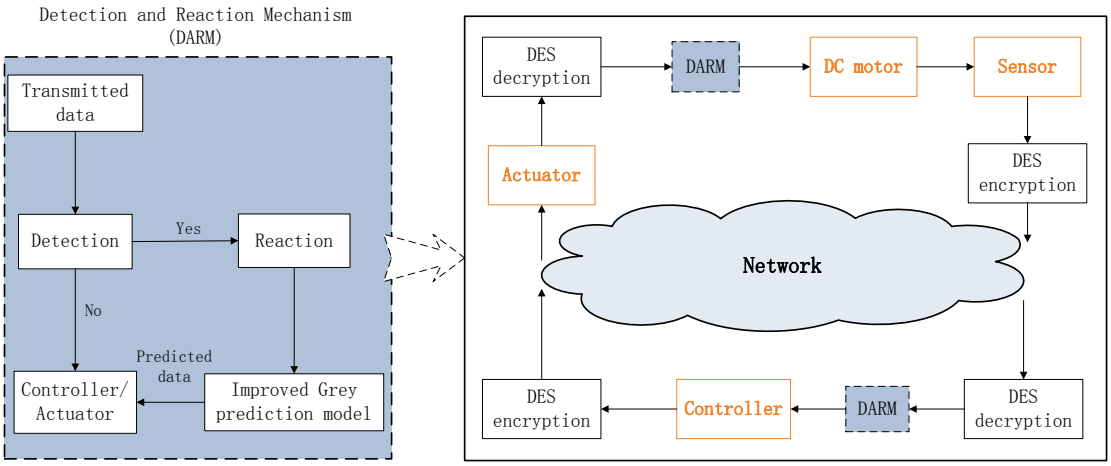

Figure 2. System architecture

$$G(s) = \frac{1000}{s^2+s} \quad (4)$$

We model the DC motor as defined in (4) for the simulation system and numerical experiments can be performed based on it.

B. Control algorithm

The traditional PID control algorithm is defined as:

$$u(t) = K_p \left[e(t) + \frac{1}{T_i}\int_0^t e(t)d_t + T_d \frac{de(t)}{dt} \right] \quad (5)$$

$$e(t) = y(t) - r(t) \quad (6)$$

where $u(t)$ is the control signal, K_p is the proportional gain, T_i and T_d are integral and differential constants for the PID controller, $y(t)$ is the measured signal received from the sensor, and $r(t)$ is the referenced speed, then the error defined as $e(t)$ can be calculated from (6).

For the conventional PID controller is difficult to reach ideal control effect, we design the expert PID control algorithm which is based on controlled object and knowledge on control rules to better control the DC motor.

We define the following formula:

$$\Delta e(k) = e(k) - e(k-1) \quad (7)$$

$$\Delta e(k-1) = e(k-1) - e(k-2) \quad (8)$$

where $e(k)$, $e(k-1)$ and $e(k-2)$ represent the error at discrete time k, k-1, k-2 respectively. Then we adopt different control strategies according to the different ranges of the absolute value of the error, and then it can improve the performance of the system very well.

III. RELATED WORK IN SECURITY SOLUTIONS

Based on the above simulation system, we propose some security solutions for the DC motor networked control system, and the architecture is shown as Fig. 2. The design of DES algorithm and detection and reaction mechanism is described in following parts in detail.

A. Implementation of DES algorithm

DES algorithm is the most commonly used symmetric cipher for its fast speed, and it is based on block cipher mode. In our simulation system, the data transmitted over the network are all decimals that are in the range of -1 and 1, so we should process the data into the single format firstly. Then the data as plaintext is replaced by initial permutation (IP) matrix, and divided into a left (L_0) and a right (R_0) in half. Next, we convert the 64-bit initial key to 56-bit by key permutation, and also divided it to two parts C_0 and D_0 in half. After that, 16 rounds of the same iterations involving permutations, substitutions and XOR operations are carried out.

Finally, the output of the last round passed through a final permutation (IP-1) to produce the cipher data.

Decryption is a reverse process of encryption, and data after decryption should be restored to the original format.

All of the above is completed in M-file of matlab. Taking encryption process as an example, the flow chart is depicted in Fig. 3.

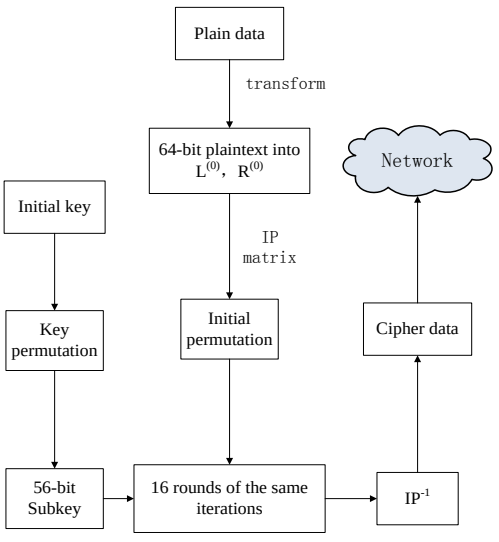

Figure 3. DES algorithm flow chart

B. Detection and reaction mechanism

As we all known, data sharing and communication security is critical for the NCSs to protect transmitted data from unauthorized access and modification. While in industrial applications, data encryption alone is not enough for system security, especially in some mission-critical areas. So we propose other security solutions for the DC motor networked control system---detection and reaction mechanism (DARM) to unusual situations such as cyber attacks, and we implement the mechanism based on DES algorithm and improved grey prediction model so that system can be protected from getting out of control under attacks.

1). Design of detection part

The modification of transmitted data in NCSs, including the sample data from the sensor and the output value of the controller, will affect the stability of the system, and even bring in enormous losses in our real life. And we can detect attacks by checking the data whether is modified with DES algorithm. The process (taking the channel from sensor to controller as an example) is shown in Fig. 4.

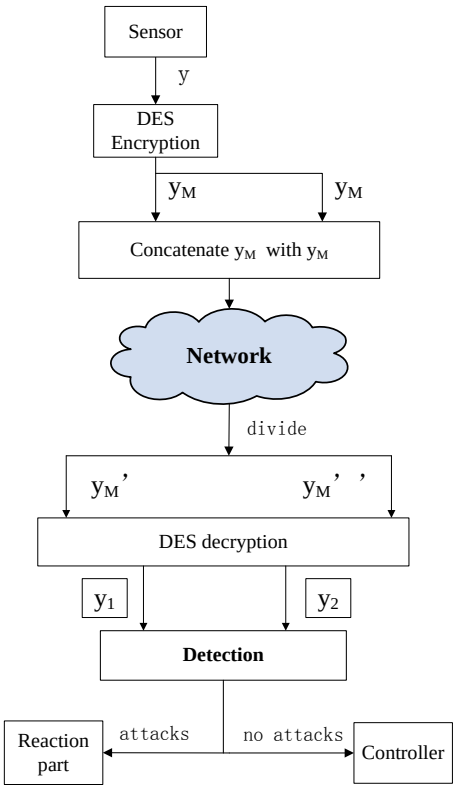

Figure 4. Detection module

At time k, we consider the measurement sampled from sensor as the plain data y and sent to the DES encryption module, then we can get the cipher data y_M. We concatenate y_M with y_M as a new variable to be sent to the controller over the network. At the destination, the variable is first divided into two parts called y_M'、y_M'', and the messages are decrypted to plain data called y_1 and y_2 respectively. Then we can detect attacks by comparing the two plain data whether they are equal. Once the system is attacked, the data transmitted over network will be modified and the two data after decrypted are not equal.

This method to detect attacks is easier and quicker compared with the other detection mechanisms shown in [8] and [10] because of less algorithms that applied into the control system.

2). Original grey prediction model

The fields covered by grey theory include systems analysis, data processing, modeling, prediction, decision making and control. Grey prediction models have been extensively used in many applications.

Traditional first-order gray prediction model, which is called GM (1, 1) model, is one of the most frequently used forecast model. This model is encompassing a group of differential equations adapted for parameter variance, and its constructing process is described as below.

Firstly, denote the original data sequence by:

$$x^{(0)} = \left(x^{(0)}(1),\ x^{(0)}(2) \ldots\ x^{(0)}(i) \ldots x^{(0)}(n) \right) \quad (9)$$

where $x^{(0)}(i)$ is the time series data at time i, n is the total amount of the original data. And then the data need to be ratio tested using the following formula:

$$\sigma(t) = \frac{x^{(0)}(t)}{x^{(0)}(t-1)}, \quad t = 2, 3, \ldots n. \quad (10)$$

where $\sigma(t)$ indicates the smooth degree of the sequence $x^{(0)}$, and when the value of $\sigma(t)$ falls within 0.1345-7.389, it means that the sequence passes the test, and we can take the next step, otherwise, add a translation to the original data sequence and calculate the ratio value again, finish the step until it passes the ratio test.

Secondly, on the basis of the initial sequence $x^{(0)}$, a new sequence $x^{(1)}$ is set up through the accumulated generating operation in order to provide the middle message of building a model and to weaken the variation tendency, i.e.

$$x^{(1)} = \left(x^{(1)}(1),\ x^{(1)}(2) \ldots\ldots x^{(1)}(n) \right) \quad (11)$$

where $x^{(1)}(t) = \sum_{i=1}^{t} x^{(0)}(i), t = 1,2, \ldots, n.$

Thirdly, we define the mean sequence $z^{(1)}$ of $x^{(1)}$ as below:

$$z^{(1)} = \left(z^{(1)}(1),\ z^{(1)}(2) \ldots\ldots z^{(1)}(n) \right) \quad (12)$$

where $z^{(1)}(t) = \frac{1}{2}\left(x^{(1)}(t) + x^{(1)}(t-1)\right), t = 2, 3..n.$

Next, we establish the grey prediction model, and consider the sequence $x^{(1)}$ as a continuous function, then we can get the differential equation i.e.

$$\frac{dx^{(1)}}{dt} + ax^{(1)} = b \quad (13)$$

Then the least square estimate sequence of the grey difference equation of GM(1,1) can be defined as follows:

$$x^{(0)}(t) + az^{(1)}(t) = b \quad (14)$$

In above, $B = (a,\ b)^T$ is a sequence of parameters that can be found as follows:

$$B = \begin{pmatrix} a \\ b \end{pmatrix} = (X^T X)^T X^T Y \tag{15}$$

where

$$X = \begin{pmatrix} -\frac{1}{2}[x^{(1)}(1) + x^{(1)}(2)] & 1 \\ -\frac{1}{2}[x^{(1)}(2) + x^{(1)}(3)] & 1 \\ \vdots & \vdots \\ -\frac{1}{2}[x^{(1)}(n-1) + x^{(1)}(n)] & 1 \end{pmatrix}$$

$$Y = \left[x^{(0)}(2), x^{(0)}(3), \dots, x^{(0)}(n)\right]^T$$

Substituting *X* and *Y* in (15), the approximate equation becomes the following:

$$\hat{x}^{(1)}(t+1) = \left[x^{(0)}(1) - \frac{b}{a}\right] e^{-at} + \frac{b}{a} \tag{16}$$

where $\hat{x}^{(1)}(t+1)$ is the predicted value of $x^{(1)}$ at time *(k+1)*.

Finally, after the completion of an inverse accumulated generating operation in (16), the predicted value of $x^{(0)}$ at time *(k+1)*, $\hat{x}^{(0)}(t+1)$, becomes available and therefore,

$$\hat{x}^{(0)}(t+1) = \hat{x}^{(1)}(t+1) - \hat{x}^{(1)}(t), k = 0, 1, \dots \tag{17}$$

The above process is depicted in Fig. 5 in detail.

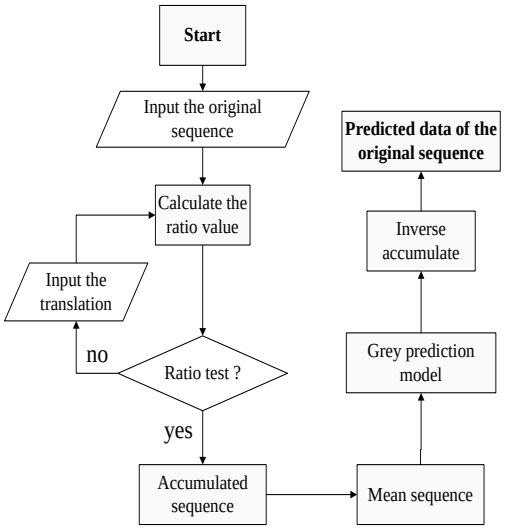

Figure 5. Grey prediction model

3). Reaction part with improved grey prediction model

For the purpose of improving the accuracy of the prediction value, in this study, residual series have been used to modify the grey model, and the detail process is shown in Fig. 6.

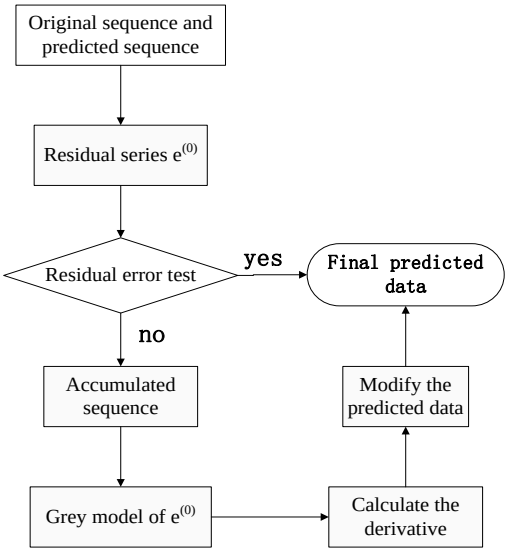

Figure 6. Improved grey model

Consider the $x^{(0)}$ sequence in (9) and the predicted series $\hat{x}^{(0)}(t+1)$ given by the GM(1,1), then the error residual series of $x^{(0)}$ can be defined as:

$$e^{(0)} = \left(e^{(0)}(2), e^{(0)}(3), \dots, e^{(0)}(n)\right) \tag{18}$$

where $e^{(0)}(k) = x^{(0)}(k) - \hat{x}^{(0)}(k),\ k = 2,3 \dots n.$

This article adopts the residual error test method based on (18) to compare the actual value and predicted value, and modify the model when the predicted data doesn't pass the residual test.

By using the same methods described as (9)–(16), a GM(1,1) model of $e^{(0)}(k)$ can be established. Denote the forecast residual series as $\widehat{e_1}(t+1)$, then

$$\widehat{e_1}(t+1) = \left[e_0(1) - \frac{\hat{\beta}}{\hat{\alpha}}\right] e^{-\hat{\alpha}t} + \frac{\hat{\beta}}{\hat{\alpha}},\ t = 1,2, \dots \tag{19}$$

where $\hat{\alpha}$ and $\hat{\beta}$ are the parameters of $e^{(0)}(k)$. Then we can calculate the derivative of (19) as:

$$C = -\hat{\alpha}\left(e_0(1) - \frac{\hat{\beta}}{\hat{\alpha}}\right) e^{-\hat{\alpha}(t-1)} \tag{20}$$

We use the derivative C to modify the model as:

$$\hat{x}^{(1)}(t+1) = \left[x^{(0)}(1) - \frac{\hat{b}}{\hat{a}}\right] e^{-\hat{a}t} + \frac{\hat{b}}{\hat{a}} + \lambda C(t) \tag{21}$$

$$where = \begin{cases} 0, & k < 2 \\ 1, & k \geq 2 \end{cases}.$$

In this paper, we define a five-dimensional vector to store the latest five legal data, which are determined not to be attacked by the detection module. The five-dimensional vector is considered as the original sequence $x^{(0)}$, once it is updated, we calculate a predicted data by the proposed method, in case of the next sample value attacked. So we can use the latest predicted data as the next time sample measurement once the system detects attacks, and prevent the system getting out of control effectively.

IV. Design of Attack Models

According to the above analysis of the mathematical model of DC motor, we can get the discrete linear dynamical systems as follows:

$$x_{k+1} = Ax_k + Bu_k \quad (22)$$

$$y_k = Cx_k \quad (23)$$

where x_k is the state of the system at time k, A models the physical dependence of the state of system, while B is the input matrix. Furthermore, u_k is the controller signal, y_k is the measurement collected by the sensor at time k.

Attacks to NCSs can be divided into two categories: physical attacks against the actuators, sensors or other physical devices; cyber attacks implemented through the communication network.

Motivated by our previous work, we consider DOS and deception attacks. We establish the following attack models taking the sensor node for an example.

In deception attacks (a compromise of integrity), the adversary sends false information $\tilde{y} \neq y$ or $\tilde{u} \neq u$ to sensors or controllers. Then deception attacks model can be expressed as below taking y_k for an example:

$$\widetilde{y_k} = \begin{cases} y_k, & \delta < \varepsilon \\ a, & \delta \geq \varepsilon \end{cases} \quad (24)$$

In DOS attacks, the adversary prevents the controller from receiving sensor measurements or the actuators from receiving control information. A DOS attack on the sensor can be modeled as:

$$\widetilde{y_k} = \begin{cases} y_k, & \delta < \varepsilon \\ 0, & \delta \geq \varepsilon \end{cases} \quad (25)$$

In above, δ is a uniform random number; y_k is the legal value, ε is a constant representing the attack level; while a and 0 in (24) and (25) represent the illegal data that simulates deception attacks and DOS attacks respectively. At each sampling time, a random number generator produces a number δ. When δ is greater than the given constant ε, the illegal data is sent to the controller, otherwise, the valid data is sent to the controller.

V. Simulation Results

To validate the proposed security solutions, we carry out the following numerical simulations based on the DC motor networked control system in TrueTime, and the experimental results are shown as below.

A. Expert PID-based NCS without attack

The square wave of the expert PID-based NCS without attacks is shown in Fig. 7, which indicates that the output can smoothly track the desired reference with the sampling period 0.01s. And the initial parameter values are: $k_p = 0.05$, $k_i = 0.01$, $k_d = 0.04$.

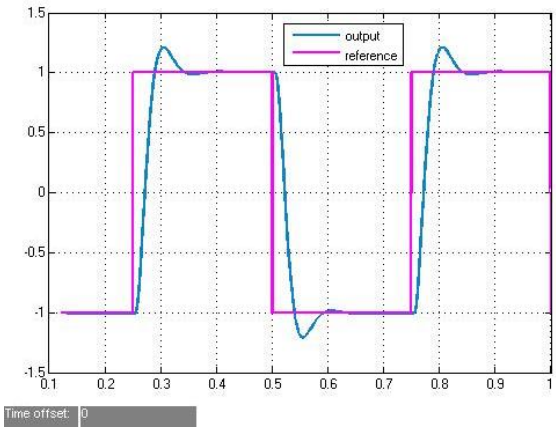

Figure 7. Expert PID-based NCS without attacks

B. System with security solutions under deception attacks

To simulate deception attacks, we use the above deception attacks model to carry out the following experiments. We let $\varepsilon = 0.7$, then the attack rate is 30%, and the green line is the output value, while the pink one represents the reference value. The left of Fig. 8 which

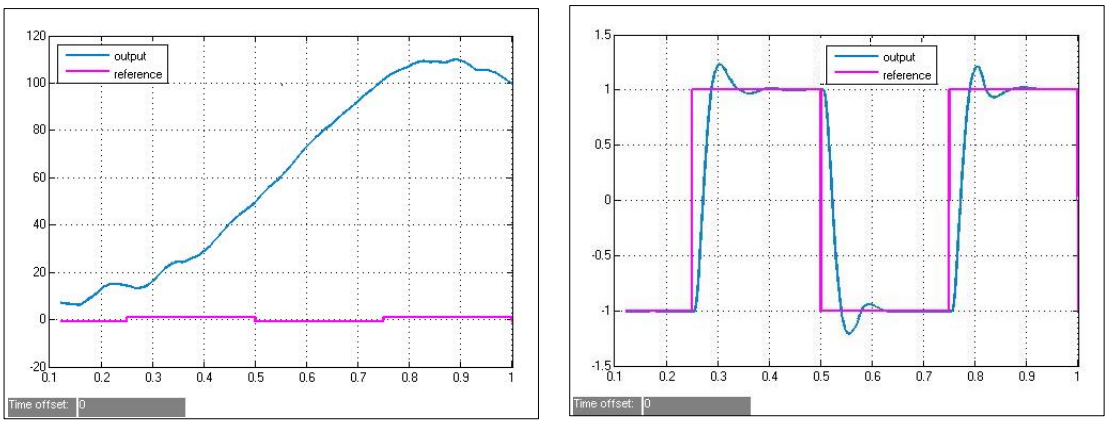

Figure 8. Simulation of deception attacks

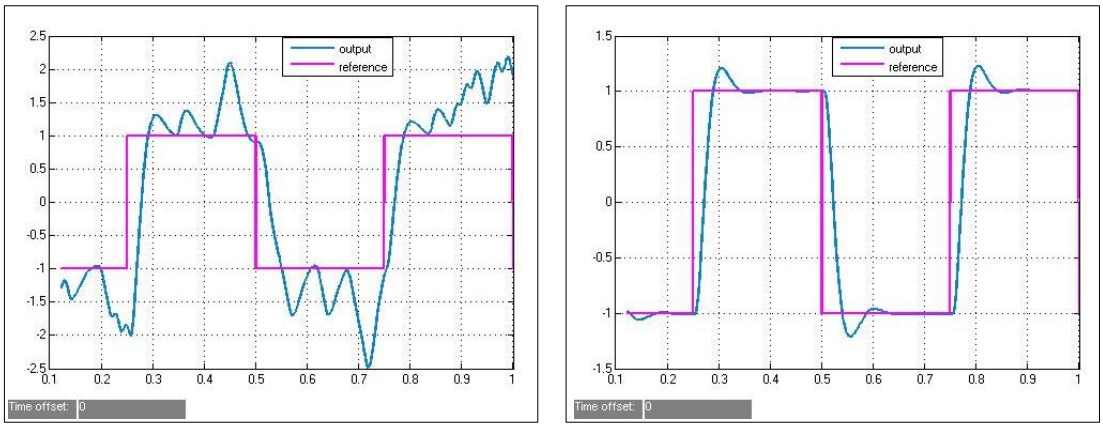

Figure 9. Simulation of DOS attacks

displays the square wave reaction to data modification attacks in the forward channel (from the sensor to the controller), confirms that the performance of the system without security solutions degrades greatly under deception attacks. However, the right of Fig. 8 shows great stability with DES encryption and DARM even under deception attacks.

C. System with security solutions under DOS attacks

In DOS attacks model, we also let $\varepsilon = 0.7$, and the attack rate is 30%. Comparing the left and the right of Fig. 9, it is clear that the system with DARM based on DES algorithm and improved grey prediction model can well track the reference inputs under DOS attacks.

VI. CONCLUSIONS

In this paper, we present security solutions for the DC motor networked control system and validate them under DOS and deception attacks. The system integrates DES algorithm and improved grey prediction model in TrueTime to implement the data confidentiality and DARM. Finally, the results of some numerical simulations demonstrate the effectiveness of our proposed security solutions.

ACKNOWLEDGMENT

This work is supported by National Science Foundation of China(No. 61170115; No. 61170117; No. 61105120), and the 2012 Ladder Plan Project of Beijing Key Laboratory of Knowledge Engineering for Materials Science(No. Z121101002812005).

REFERENCES

[1] Dzung, Dacfey, et al, "Security for industrial communication systems", Proceedings of the IEEE 93.6, pp. 1152-1177, 2005.

[2] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends", *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, pp. 2527-2535, Jul. 2010.

[3] Byres, Eric, and Justin Lowe, " The myths and facts behind cyber security risks for industrial control systems ", Proceedings of the VDE Kongress, vol. 116, 2004.

[4] Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry, " Secure control: Towards survivable cyber-physical systems", Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on IEEE, pp. 495-500, 2008.

[5] Creery, A.; Byres, E.J., "Industrial cybersecurity for power system and SCADA networks," *Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual* , vol., no., pp.303,309, 12-14 Sept. 2005.

[6] Peng Jie; Liu Li, "Industrial Control System Security," *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2011 International Conference on* , vol.2, no., pp.156,158, 26-27 Aug. 2011.

[7] Swaminathan, P.; Padmanabhan, K.; Ananthi, S.; Pradeep, R, "The Secure Field Bus (SecFB) Protocol-Network Communication Security for secure Industrial Process control ", TENCON 2006. 2006 IEEE Region 10 Conference , vol., no, pp.1,4, 14-17, Nov. 2006.

[8] Zhonghua, Pang, Liu Guoping, and Zhou Donghua, "Detection of deception attacks on the backward channel of networked control systems", Control Conference (CCC), 2012 31st Chinese. IEEE, pp. 5972-5977, 2012.

[9] Ke-Ya Yuan; Jie Chen; Guo-Ping Liu; Jian Sun, "Design and implementation of data encryption for networked control systems", Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on. IEEE, vol. no, pp.2105-2109, 11-14 Oct. 2009.

[10] Zhong-Hua Pang; Guo-Ping Liu, "Design and Implementation of Secure Networked Predictive Control Systems Under Deception Attacks", Control Systems Technology, IEEE Transactions on , vol.20, no.5, pp.1334-1342, Sept. 2012.

[11] Zhong-Hua Pang; Geng Zheng; Guo-Ping Liu; Chun-Xiang Luo, "Secure transmission mechanism for networked control systems under deception attacks", Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011 IEEE International Conference on , vol., no., pp.27-32, 20-23 March 2011.
[12] Teixeira, A.; Sandberg, H.; Johansson, K.H., "Networked control systems under cyber attacks with applications to power networks", American Control Conference (ACC), 2010, vol., no., pp.3690-3696, June 30 2010-July 2 2010.
[13] Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry, "Research challenges for the security of control systems", Proceedings of the 3rd conference on Hot topics in security. USENIX Association, pp.1-6, 2008.
[14] Wente Zeng; Mo-Yuen Chow, "A trade-off model for performance and security in secured Networked Control Systems", Industrial Electronics (ISIE), 2011 IEEE International Symposium on , vol., no., pp.1997-2002, 27-30 June 2011.
[15] Wente Zeng; Mo-Yuen Chow, "Optimal Tradeoff Between Performance and Security in Networked Control Systems Based on Coevolutionary Algorithms", Industrial Electronics, IEEE Transactions on , vol.59, no.7, pp.3016-3025, July 2012.
[16] Gupta, R.A.; Mo-Yuen Chow, "Performance assessment and compensation for secure networked control systems", Industrial Electronics, 2008. IECON 2008. 34th Annual Conference of IEEE , vol., no., pp.2929-2934, 10-13 Nov. 2008.
[17] Hussain, Alefiya, and Saurabh Amin, "NCS security experimentation using DETER." Proceedings of the 1st international conference on High Confidence Networked Systems. ACM, pp. 73-80, 2012.
[18] Amin, S.; Litrico, X.; Sastry, S.; Bayen, A. M., "Cyber Security of Water SCADA Systems-Part I: Analysis and Experimentation of Stealthy Deception Attacks," *Control Systems Technology, IEEE Transactions on* , vol.PP, no.99, pp.1,1, 0, 2012.
[19] Cárdenas, Alvaro A., et al, "Attacks against process control systems: risk assessment, detection, and response", Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, pp. 355-366, 2011.
[20] Hsu, Che-Chiang, and Chia-Yon Chen, "Applications of improved grey prediction model for power demand forecasting", Energy Conversion and Management, vol. 44, no. 14, pp. 2241-2249, 2003.
[21] Qi Xie; Yan Xie, "Forecast of the Total Volume of Import-export Trade Based on Grey Modelling Optimized by Genetic Algorithm", Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on , vol.1, no., pp.545-547, 21-22 Nov. 2009.
[22] Jianfeng Dong, "The Building of Network Security Situation Evaluation and Prediction Model Based on Grey Theory", Challenges in Environmental Science and Computer Engineering (CESCE), 2010 International Conference on , vol.2, no., pp.401-404, 6-7 March 2010.

Zhang Liying , born in 1988. master. candidate in School of Computer and Communication Engineering, University of Science and Technology Beijing , China.

Her main research interests include the security of industrial control systems and data acquisition using OPC data transfer protocol.

Xie Lun, born in 1968. Ph. D. and professor in School of Computer and Communication Engineering, University of Science and Technology Beijing, China.

His main research interests are security of networked control systems, security of industrial networking and artificial intelligence.

Li Weize , born in 1988. master. candidate in School of Computer and Communication Engineering, University of Science and Technology Beijing , China.

Wang Zhiliang , born in 1956. master. Ph. D. and professor in School of Computer and Communication Engineering, University of Science and Technology Beijing, China.

How to cite this paper: Liying Zhang, Lun Xie, Weize Li, Zhiliang Wang,"Security Solutions for Networked Control Systems Based on DES Algorithm and Improved Grey Prediction Model", IJCNIS, vol.6, no.1, pp.78-85,2014. DOI: 10.5815/ijcnis.2014.01.10

