Sensors and Materials, Vol. 34, No. 7 (2022) 2567–2579
MYU Tokyo

S & M 2991

Cyberattack Defense with Appropriate Address-changing Frequency in Industrial Control Systems

I-Hsien Liu,[1,2] Yen-Yu Chen,[1,2] Chuan-Gang Liu,[3] and Jung-Shian Li[1,2*]

[1]Department of Electrical Engineering, National Cheng Kung University,
No. 1, University Road, Tainan City 701401, Taiwan
[2]Institute of Computer and Communication Engineering, National Cheng Kung University,
No. 1, University Road, Tainan City 701401, Taiwan
[3]Department of Applied Informatics and Multimedia, Chia Nan University of Pharmacy & Science,
No. 60, Sec. 1, Erren Rd., Rende Dist., Tainan City 717301, Taiwan

(Received December 30, 2021; accepted May 31, 2022)

Keywords: industrial control system, moving target defense, secure communication, stochastic process

Most research on moving target defense has focused on how to efficiently change the IP address and the method of IP address replacement, and there have been few studies on the address-changing frequency, making it difficult for a user to decide the appropriate frequency for the system. According to previous research, the higher the address-changing frequency, the higher the system security at the expense of the performance of the server and the utilization of system resources. In this paper, we propose a method for quantifying the security of a moving target defense system that allows the user to decide the address-changing frequency in moving target defense. We show how to achieve the balance between security and system resource use by employing a stochastic process. Our research makes the moving target defense system operate more efficiently in industrial control systems.

1. Introduction

Sensors are widely used in industrial control systems for automated operations. However, over-reliance on information systems can also easily lead to information security incidents. The issue of information security in Industry 4.0 is a concern.(1) To protect systems, moving target defense (MTD) has been proposed as a means of preventing hackers from connecting to devices, and safe communication of programmable logic controllers and human–machine interfaces through MTD has been achieved in an industrial control network environment.(2-4) MTD has been demonstrated to resist a variety of malicious behaviors. However, the MTD architecture is not yet complete; for example, an appropriate address-changing frequency cannot be determined. The address-changing frequency and a system's security are positively correlated. However, if an extremely high address-changing frequency is adopted, the increased use of system resources must be considered. Most of the research on the address-changing frequency has adopted game theory to determine the MTD strategy, which emphasizes the strategies of attackers and

*Corresponding author: e-mail: jsli@mail.ncku.edu.tw
https://doi.org/10.18494/SAM3843

ISSN 0914-4935
https://myukk.org/

defenders.[5,6] However, this approach is inadequate for the study of the address-changing frequency in MTD systems. In this paper, we show how to quantify the security of an MTD system in an industrial control network environment by a stochastic process. We can thus determine an appropriate address-changing frequency for various MTD environments and reduce the cost of address changing while maintaining the same level of security.

2. Related Work

Owing to the popularity of Industry 4.0, an increasing number of industrial systems are connected to the internet. Hackers can attack an industrial control system through the internet and pose a serious threat.[7,8] Any hardware that complies with the TCP/IP protocol specifications, including industrial control systems, may be a target for a hacker. Many studies have attempted to prevent or detect cyberattacks, and MTD is one of the methods used. Traditional defense methods such as firewalls and honeypots can resist most attacks. However, because of the advancement of hacking technology, the security of systems still cannot be ensured. Some researchers believe that the best defense is to make it impossible for hackers to find equipment. In 2011, MTD was proposed,[9] which increases a hacker's exploration space and ensures system security as shown in Fig. 1. A packet-forwarding mechanism makes the MTD architecture possible. Programmable logic controllers (PLCs) and human–machine interfaces (HMIs) send a packet to an MTD device by IP. The MTD device also forwards the packet by IP. In a recent study, it was demonstrated that industrial control systems can be protected from attacks by employing Moving Target IPv6 Defense (MT6D), which can effectively resist decentralized denials of service, replay attacks, black hole attacks, and other malicious behaviors.[2,10] Figure 2(a) shows an industrial control system in which all PLCs and HMIs use IPv4 for communication. Figure 2(b) shows the system with MT6D installed. The PLCs and HMIs still use IPv4 for sending and receiving as before, but packets are forwarded.

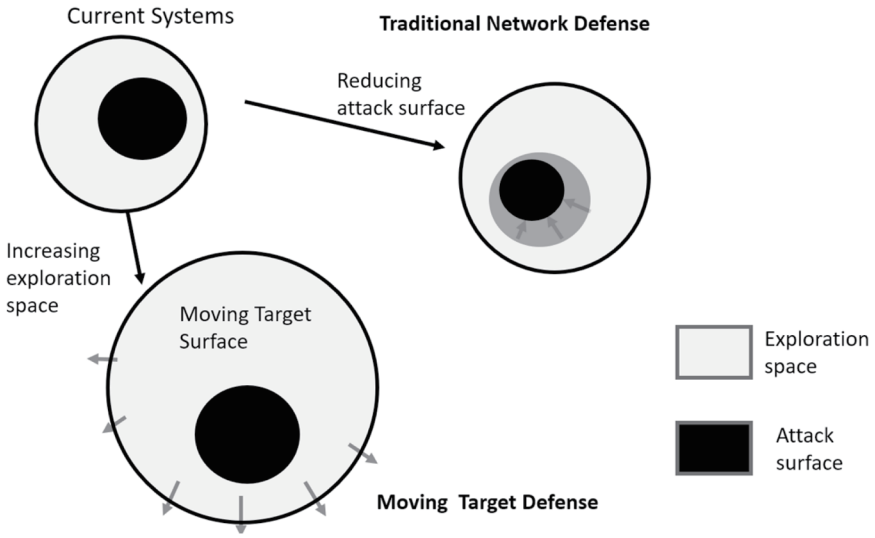

Fig. 1. Comparison of hacker's exploration space between MTD and traditional network defense.

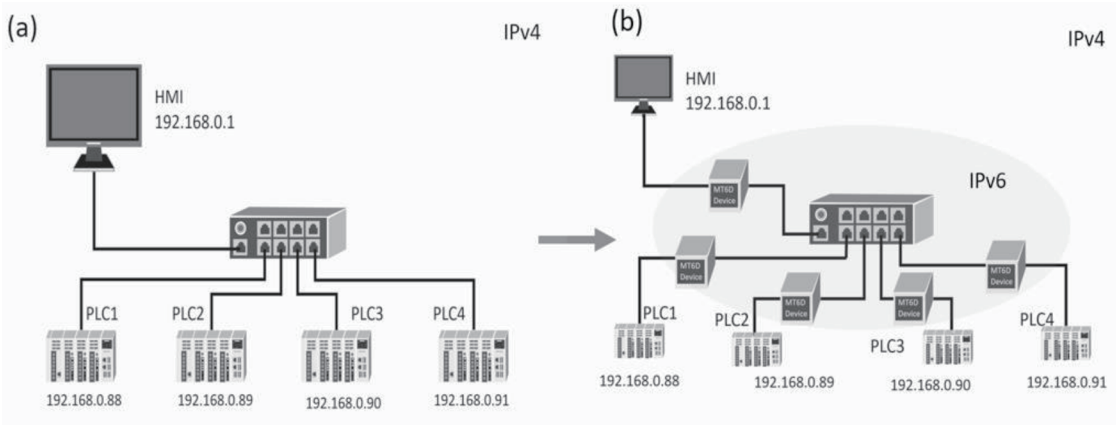

Fig. 2. Packet transmission mechanism in industrial control system with MTD.

In addition to the MTD architecture, the tolerance mechanism for communication must also be considered. In our research, MTD has a tolerance mechanism to deal with packet loss when changing addresses. Briefly, each device holds three IP addresses at the same time to prevent packet loss, and each device can communicate with each other safely and stably. However, the address-changing frequency must be considered. Although the use of game theory to analyze the attack and defense strategies of MTD systems has been proposed,[5,6] system environmental factors have not been sufficiently considered. System resources are required to generate and register an IP address in MTD modules. The higher the address-changing frequency, the higher the security of MTD and the greater the resource usage by the system. An appropriate address-changing frequency that balances the security level and resource use is required for MTD systems. In the next section, we quantify the security of MTD systems and discuss how to find an appropriate address-changing frequency.

3. Security Quantification

In this section, we first describe the scenario and parameters in our research. Then we show our calculation for quantifying the security of MTD systems.

3.1 System scenario

We consider an industrial control system using the MTD system shown as Fig. 3. The industrial control system includes several PLCs and HMIs. By connecting to an Ethernet network and using Modbus TCP protocol, hardware can communicate with each other. Generally speaking, an HMI sends Modbus requests to a PLC and waits for it to respond. We also consider the attacker behavior. MTD is an architecture that can hide devices; thus, we focus on the investigation stage, the first stage of a cyberattack. There are many network scanning tools such as Network Mapper (NMAP) and ZMAP, with different speeds of network scanning (v_{scan}) for different tools and network environments.[11] Here, we choose NMAP as the default network

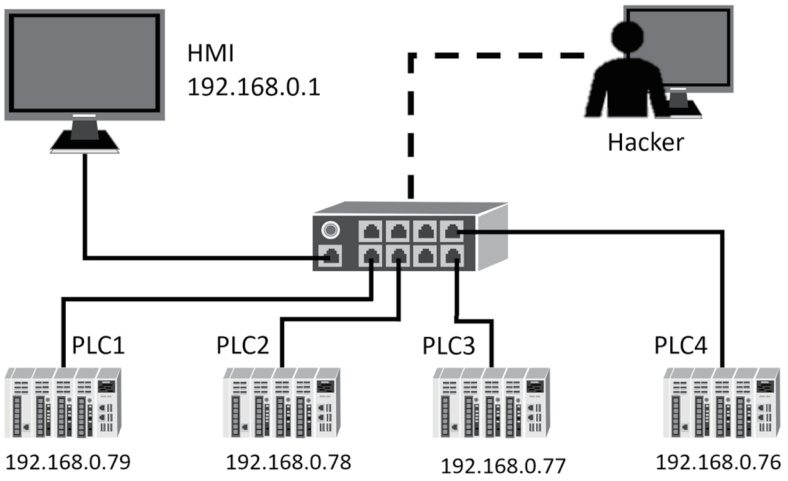

Fig. 3. MTD system and hacker behavior.

Table 1
Parameters for security quantification of MTD.

Parameter	Description
N	Number of PLCs in industrial control system
T	Address-changing period in MTD system
v_{scan}	Speed of network scanning
P	Available addresses for MTD system Available address will be determined by system prefix IP address size. If prefix IP address size = 96, we can consider P as below. $P = 2^{(128-96)}$

scanning tool because of its versatility and stability. NMAP supports hundreds of input parameters, among which are the scanning speeds of six stages (T0–T5).[11] The other parameters considered in our calculation are given in Table 1.

3.2 Quantification calculation

Now we can quantify the MTD system according to the scenario and parameters. We choose the birth–death process to quantify the security of the MTD system.[12] In an MTD system of an industrial control system, each device has two states: secure and insecure. The secure state corresponds to the period that the device cannot be found or connected to by a hacker; the insecure state corresponds to the period that the device had been found or connected to by a hacker. We build a continuous-time Markov chain for our scenario as shown in Fig. 4.

The Markov chain state S_n denotes that n devices have been found by a hacker. We define the secure state as S_0, which means that no hacker has found or connected to a device. λ_n and μ_n represent the flow rates between states. λ denotes the flow rate from a lower state to a higher state in a device, and μ denotes the flow rate from a higher state to a lower state in a device. Our calculation target, security quantification, is the percentage of the total time for which the system is in the secure state. In the first stage of the quantification, we calculate the values of λ_n

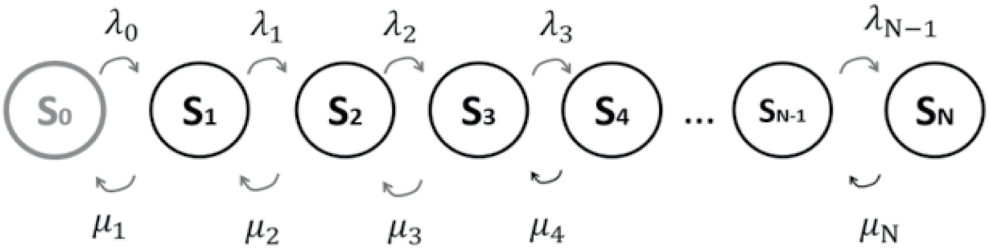

Fig. 4. Continuous-time Markov chain for our research scenario.

and μ_n using the following equation, where X and Y are random variables of the time at which the state of a device is changed.

$$\lambda = \frac{1}{E[X]}$$
$$\mu = \frac{1}{E[Y]} \tag{1}$$

The expected value of X is obtained as

$$E[X] = \sum_{n=1}^{\infty} T(n)\, p(n). \tag{2}$$

Because network scanning is a discrete behavior, we can use Table 2 to obtain $E[X]$. The MTD system selects the IP address of each device from P addresses. Every IP address can exist for three address-changing periods to ensure the connection between HMIs and PLCs. For the hacker, the probability of guessing the device's IP at the required time is $p(n)$ and the required time is $T(n)$ for the nth attempt at network scanning.

The hacker is guaranteed to find the device after scanning P–2 times because every MTD module has one of three IP addresses at each instant. We calculate $E[X]$ as follows:

$$\begin{aligned}
E[X] &= \sum_{n=1}^{P-2} \frac{(P-n)}{P}\frac{(P-n-1)}{(P-1)}\frac{3}{(P-2)} * \frac{n}{v_{scan}} \\
&= \left(\frac{1}{P}\frac{1}{(P-1)}\frac{3}{(P-2)}\frac{1}{v_{scan}}\right)\sum_{n=1}^{P-2}(P-n)(P-n-1)(n) \\
&= \left(\frac{1}{P}\frac{1}{(P-1)}\frac{3}{(P-2)}\frac{1}{v_{scan}}\right)\sum_{n=1}^{P-2}\left(n^3 + (1-2P)n^2 + \left(P^2-P\right)n\right) \\
&= \left(\frac{1}{P}\frac{1}{(P-1)}\frac{3}{(P-2)}\frac{1}{v_{scan}}\right)\left(\frac{((P-2)+1)^2(P-2)^2}{4} + (1-2P)\frac{(P-2)((P-2)+1)(2(P-2)+1)}{6} + \left(P^2-P\right)\frac{(P-2)((P-2)+1)}{2}\right) \\
E[X] &= \left(\frac{P+1}{4v_{scan}}\right)
\end{aligned} \tag{3}$$

Table 2
Moment probabilities and times in $E[X]$.

n	$p(n)$	$T(n)$
1	$\frac{3}{P}$	$\frac{1}{v_{scan}}$
2	$\frac{(P-3)}{P}\frac{3}{(P-1)}$	$\frac{2}{v_{scan}}$
3	$\frac{(P-3)}{P}\frac{(P-4)}{(P-1)}\frac{3}{(P-2)}$	$\frac{3}{v_{scan}}$
4	$\frac{\cancel{(P-3)}}{P}\frac{(P-4)}{(P-1)}\frac{(P-5)}{(P-2)}\frac{3}{\cancel{(P-3)}}$	$\frac{4}{v_{scan}}$
5	$\frac{(P-5)}{P}\frac{(P-6)}{(P-1)}\frac{3}{(P-2)}$	$\frac{5}{v_{scan}}$
⋮	⋮	⋮
i	$\frac{(P-i)}{P}\frac{(P-i-1)}{(P-1)}\frac{3}{(P-2)}$	$\frac{i}{v_{scan}}$

From this equation, λ is obtained as

$$\lambda = \frac{1}{E[X]} = \left(\frac{4v_{scan}}{P+1}\right). \tag{4}$$

Next, we find the flow rate from the higher state to the lower state. Similarly to the case of λ, we obtain the value of μ by considering

$$E[Y] = \sum_{n=1}^{\infty} T(n)\, p(n). \tag{5}$$

However, we must consider the difference between μ and λ. Figure 5 shows the time domain in which the device encounters hacker behavior. Because of the tolerance mechanism, every IP address generated by MTD modules survives three timeslots ($3t$), after which it is invalid. Assuming that the hacker scans and connects to the device successfully in time T_a, the device enters the insecure state. Thus, a time of $3t - T_a$ is required for the device to return to the secure state.

Next, we show the probability that the device is scanned by a hacker at each instant. Because the changing-state action depends on the hacker's network scanning tool, we also consider it as a discrete behavior. During the survival time of a IP address ($3t$), we consider that the hacker can attempt to connect to the device's IP $v_{scan} \times 3T$ times in this period. Thus, the probability that the device enters the insecure state at each moment can be found (Table 2). The probabilities are the same as those in Table 2 but with $1 \le i \le v_{scan} \times 3T$.

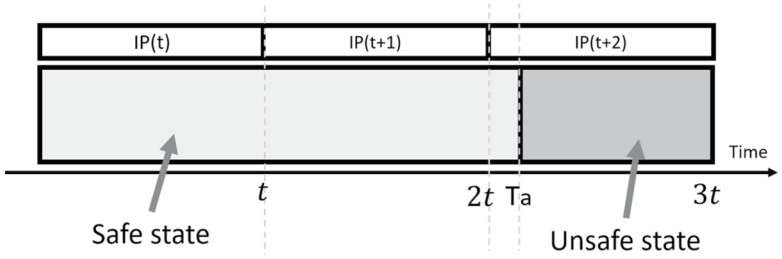

Fig. 5. Time domain of the MTD modules.

In our research, we assume that the MTD system satisfies Eq. (6), making it difficult for the devices to be found by a hacker.

$$P \gg 3v_{scan}T \tag{6}$$

Note that $P \gg 1$ because P is the number of IP addresses that can be used in an appropriate MTD system. For every moment (n), the hacker has the same probability of being able to connect to the devices. Thus, we can simplify the general formula in Table 3 to

$$\frac{P}{P}\frac{P}{P}\frac{3}{P} = \frac{3}{P}. \tag{7}$$

According to the above equation results, at every moment, the devices have the same probability of being connected to by the hacker; thus, we can determine the time required by the hacker to connect the devices at every moment [$T(n)$] using Table 4.

Table 3
Moment probabilities in $E[Y]$.

n	$p(n)$
1	$\frac{3}{P}$
2	$\frac{(P-3)}{P}\frac{3}{(P-1)}$
3	$\frac{(P-3)}{P}\frac{(P-4)}{(P-1)}\frac{3}{(P-2)}$
4	$\frac{\cancel{(P-3)}}{P}\frac{(P-4)}{(P-1)}\frac{(P-5)}{(P-2)}\frac{3}{\cancel{(P-3)}}$
5	$\frac{(P-5)}{P}\frac{(P-6)}{(P-1)}\frac{3}{(P-2)}$
⋮	⋮
i	$\frac{(P-i)}{P}\frac{(P-i-1)}{(P-1)}\frac{3}{(P-2)}$

Table 4
Probabilities of moments and times in $E[X]$.

n	$p(n)$	$T(n)$
1	$\frac{1}{3v_{scan}T}$	$3T-\frac{1}{3v_{scan}}$
2	$\frac{1}{3v_{scan}T}$	$3T-\frac{2}{3v_{scan}}$
3	$\frac{1}{3v_{scan}T}$	$3T-\frac{3}{3v_{scan}}$
4	$\frac{1}{3v_{scan}T}$	$3T-\frac{4}{3v_{scan}}$
5	$\frac{1}{3v_{scan}T}$	$3T-\frac{5}{3v_{scan}}$
⋮	⋮	⋮
$3v_{scan}T$	$\frac{1}{3v_{scan}T}$	$3T-\frac{3v_{scan}T}{3v_{scan}}$

Moreover, the expected value $E[Y]$ is given by

$$\begin{aligned} E[Y] &= \sum_{n=1}^{3v_{scan}T} P(n)T(n) \\ &= \frac{3}{2}T \end{aligned}. \tag{8}$$

and μ is given by

$$\mu = \frac{1}{E[Y]} = \frac{2}{3T}. \tag{9}$$

After finding the flow rates λ and μ, we calculate the duration of each state by a birth–death process. For the model used in an MTD system, the flow rates between states are

$$\begin{aligned} \lambda_n &= (N-n)\left(\frac{4v_{scan}}{P+1}\right) \\ \mu_n &= \frac{2n}{3T} \end{aligned}. \tag{10}$$

We wish to know the duration of every state when the system is stable, which we determine by considering the balance between the inflow rate and outflow rate in each state.

$$\begin{aligned} &\lambda_0 P_0 = \mu_1 P_1 \\ &(\lambda_1 + \mu_1)P_1 = \lambda_0 P_0 + \mu_2 P_2 \\ &(\lambda_2 + \mu_2)P_2 = \lambda_1 P_1 + \mu_3 P_3 \\ &(\lambda_3 + \mu_3)P_3 = \lambda_2 P_2 + \mu_4 P_4 \\ &\cdots \\ &(\lambda_z + \mu_z)P_z = \lambda_{z-1} P_{z-1} + \mu_{z+1} P_{z+1} \\ &\cdots \\ &\mu_N P_N = \lambda_{N-1} P_{N-1} \end{aligned} \tag{11}$$

The probability of each state can be expressed in terms of P_0.

$$
\begin{aligned}
P_1 &= \frac{\lambda_0}{\mu_1} P_0 = \frac{N\lambda}{1\mu} P_0 = \frac{(N)}{1}\left(\frac{\lambda}{\mu}\right)^1 P_0 \\
P_2 &= \frac{\lambda_1}{\mu_2} P_1 = \frac{\lambda_1}{\mu_2}\frac{\lambda_0}{\mu_1} P_0 = \frac{(N-1)\lambda}{2M}\frac{N\lambda}{1M} P_0 = \frac{(N)(N-1)}{2*1}\left(\frac{\lambda}{\mu}\right)^2 P_0 \\
P_3 &= \frac{\lambda_2}{\mu_3} P_2 = \frac{\lambda_2}{\mu_3}\frac{\lambda_1}{\mu_2}\frac{\lambda_0}{\mu_1} P_0 = \frac{(N-2)\lambda}{3\mu}\frac{(N-1)\lambda}{2\mu}\frac{N\lambda}{1\mu} P_0 = \frac{(N)(N-1)(N-2)}{3*2*1}\left(\frac{\lambda}{\mu}\right)^3 P_0 \\
&\cdots \\
P_N &= \frac{\lambda_{N-1}}{\mu_N} P_{N-1} = \frac{(N)(N-1)(N-2)\ldots(1)}{N*\ldots*3*2*1}\left(\frac{\lambda}{\mu}\right)^N P_0 = \left(\frac{\lambda}{\mu}\right)^N P_0
\end{aligned}
\tag{12}
$$

Thus, the probability of each state is

$$
\begin{aligned}
P_n &= \frac{(N)(N-1)(N-2)\ldots(N-n+1)}{n!}\left(\frac{\lambda}{\mu}\right)^n P_0 \\
&= \frac{N!}{n!(N-n)!}\left(\frac{\lambda}{\mu}\right)^n P_0 \\
&= C_n^N \left(\frac{\lambda}{\mu}\right)^n P_0
\end{aligned}
\quad . \tag{13}
$$

Because the sum of the probabilities of each state is equal to 1, we have

$$
\sum_{i=0}^{N} P_i = 1 . \tag{14}
$$

Thus,

$$
P_0\left(\sum_{n=0}^{N} C_n^N \left(\frac{\lambda}{\mu}\right)^n\right) = 1 . \tag{15}
$$

Obtained by the binomial theorem, Eq. (16) shows the relationship between the environmental parameters and the quantified MTD security S. We can adopt an appropriate address-changing frequency for an MTD using this equation.

$$
S = P_0 = \frac{1}{\left(1 + \frac{6v_{scan}T}{(P+1)}\right)^N} \tag{16}
$$

4. Results

This section shows the calculation results and some extended results. According to Eq. (16), when the speed of the network scanning tool (v_{scan}) or the address-changing period (T) increases, the system's security S decreases, but when the number of IP address pools (P) increases, S increases. Moreover, an MTD system with more devices (N) has lower security because

$$\frac{6v_{scan}T}{(P+1)} \geq 0 . \tag{17}$$

We also can analyze the scalability (δ) of the MTD system. It is necessary to consider the resource consumption of an MTD system. In an actual industrial control system, if the address-changing period is halved, the amount of resources required by the MTD system for the registration and generation of moving target IP addresses is doubled, affecting the performance and stability of the system. The operating system and hardware require considerable time to calculate and generate the registration IP addresses. To properly allocate system resources, the scalability of the system must be considered. We define Q as the environment variable [Eq. (18)], which will differ for each MTD environment. It is determined as the ratio of the attacker's scanning speed to the number of available IP addresses in the device's address pool. To calculate δ, we use the equation for quantifying the MTD security.

$$Q = \frac{6v_{scan}}{P+1} \tag{18}$$

The security of the original MTD system before the address-changing frequency is changed is

$$S = \frac{1}{(1+QT)^N} . \tag{19}$$

We now assume that the address-changing frequency of the system is doubled, meaning that the resources required to generate and register the IP addresses are also doubled.

$$S' = \frac{1}{\left(1+\frac{1}{2}QT\right)^N} \tag{20}$$

We evaluate δ as follows.

$$\delta = \frac{S'}{S} = \frac{\dfrac{1}{\left(1+\dfrac{1}{2}QT\right)^N}}{\dfrac{1}{(1+QT)^N}} = \left(\frac{1+QT}{1+\dfrac{1}{2}QT}\right)^N \tag{21}$$

Then we analyze the scalability of the system as follows.

$$\begin{aligned} &\text{Let } Q \cong 0 \\ &\delta \cong \left(\frac{1+0}{1+0}\right)^N = 1 \end{aligned} \tag{22}$$

This means that we use more system resources to increase the address-changing frequency, but the system cannot increase the level of security. Thus, system resources are wasted because they do not improve the defense.

$$\begin{aligned} &\text{Let } Q \gg 1 \\ &\delta = \left(\frac{1+QT}{1+\dfrac{1}{2}QT}\right)^N \\ &\cong \left(\frac{QT}{\dfrac{1}{2}QT}\right)^N \\ &= 2^N \end{aligned} \tag{23}$$

In this situation [Eq. (23)], we find that the security has been significantly improved. The security of the MTD system can be enhanced by using twice the computing resources. To avoid wasting system resources, the appropriate address-changing frequency should be considered for every environment.

5. Discussion

We expect more future applications and developments of MTD systems through the combination of current network technologies and theory, which will create a more secure

network environment in the near future. For example, innovational network technologies, virtual private networks, software-defined networks, and mobile IPv6 communication are used in some MTD applications.[13,14] However, most previous studies discussed the system design and implementation of the MTD scheme in a given network. In this study, we find that the frequency of changing IP addresses is a core performance issue in designing MTD systems, which is a novel feature not addressed in previous MTD-related works. We also design a standard suitable for most network scenarios, with which future researchers can easily design a high-performance MTD-based network environment.

6. Conclusion

In this paper, we propose a method to quantify MTD system security that allows a suitable address-changing frequency to be found in different MTD environments. With Eq. (16), the appropriate address-changing frequency and the scalability of an MTD system can be calculated using the user-defined quantification value. In an industrial control environment that requires immediate responses, less resource usage often means higher stability and performance. It is important to find a balance between system security and system resource usage for MTD systems. The results of this study can be used in future MTD research to improve the performance of MTD by reducing the address-changing frequency for MTD systems.[15] In the future, we expect to further increase the reliability and security of MTD systems.

Acknowledgments

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 110-2218-E-006-013-MBK and MOST 111-2218-E-006-010-MBK.

References

1 History of Industrial Control System Cyber Incidents: https://doi.org/10.2172/1505628 (accessed December 2021).
2 C. Liu, C. Wu, I. Liu, C. Wu, and J. Li: Proc. 2020 Intelligent Computing and its Emerging Applications Conf. (ACM, 2020) 1–6.
3 J. Li, C. Liu, C. Wu, C. Wu, C. Huang, C. Li, and I. Liu: Sens. Mater. **33** (2021) 3415. https://doi.org/10.18494/SAM.2021.3513
4 Y. Chen, I. Liu, C. Wu, C. Liu, and J. Li: Proc. 2021 Int. Siberian Conf. Control and Communications (IEEE, 2021) 381–385.
5 C. Lei, D. Ma, and H. Zhang: IEEE Access **5** (2017) 156. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7805250
6 X. Feng, Z. Zheng, D. Cansever, A. Swami, and P. Mohapatra: Proc. 2017 IEEE Int. Conf. Computer Communications (IEEE, 2017) 1–9.
7 A. Adamov, A. Carlsson, and T. Surmacz: Proc. 2019 IEEE East-West Design & Test Symp. Conf. (IEEE, 2019) 1–5.
8 Florida Hack Exposes Danger to Water Systems: https://www.pewtrusts.org/zh/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems (accessed December 2021).
9 M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront: Proc. 2011 Military Communications Conf. (IEEE, 2011) 1321–1326. https://doi.org/10.1109/MILCOM.2011.6127486

10 V. Heydari and S. Yoo, S. Kim: Proc. 2016 IEEE Global Communications Conf. (IEEE, 2016) 1–6.
11 The Official Nmap Project Guide to Network Discovery and Security Scanning: https://nmap.org/book/toc.html (accessed December 2021).
12 S. Ross: Introduction to Probability Models, S. Ross, Ed. (Elsevier, USA, 2014) 11th ed., Chap. 6.
13 D. S. Kim, M. Kim, J. H. Cho, H. Lim, T. J. Moore, and F. F. Nelson: Proc. 2020 50th Annu. IEEE-IFIP Int. Conf. Dependable Systems and Networks-Supplemental Volume (IEEE, 2020) 43–44.
14 V. Heydari: IEEE Access **6** (2018) 33329. https://doi.org/10.1109/ACCESS.2018.2844542
15 Y. Chen, I. Liu, C. Wu, C. Liu, and J. Li: Proc. 2021 IEEE Int. Conf. Electronic Communications (IEEE, 2021) 36–39.