IP Address Mutation Scheme Using Vector Projection for Tactical Wireless Networks

Jong-Kwan Lee(✉)

Cyber Warfare Research Center, Korea Military Academy, Seoul, Korea
jklee64@kma.ac.kr

Abstract. The static address configuration of networks and hosts allows attackers to have enough time to discover target networks and systems. On the other hands, the defenders always lack of time to respond because they can take action after attacker's explicit behaviors. To eliminate the attacker's asymmetric advantage of time, randomization of addresses have been suggested as Moving Target Defense (MTD) which is a promising technique to make the attacker's reconnaissance activities difficult by dynamically changing network properties. In this paper, I propose the address mutation scheme using vector projection for tactical wireless networks that are a leader node centric hierarchical structure. In the proposed scheme, the addresses in the same networks are mutated with a simple vector operation by fully distributed manner and the mutated addresses are shared to all the members in the internal networks. Unlike the conventional schemes, all addresses associated with network entities for data delivery are mutated. I evaluate the performance of the proposed scheme by numerical analysis and experimental simulations. The results show that the proposed scheme could effectively randomize the addresses in tactical wireless networks.

Keywords: Moving Target Defense · Address mutation · Tactical wireless networks

1 Introduction

1.1 Moving Target Defense (MTD)

In general, network configuration, security mechanisms, and system information are static in a traditional passive defense system. Thus, an attacker can gather information about the target system and have enough time to identify and analyze the vulnerability. On the other hand, the defender must be prepared for all possible attacks until the attack signatures are correctly identified, and the response time is not sufficient since the attack is explicitly identified and then a specific response is selected. Therefore, in cyber space, the attacker who is able to select the attack time and the target system is generally more advantageous than the defender [1–3]. This asymmetry between the attacker and the defender has forced the activity in cyberspace to be basically a game against the defender. MTD (Moving Target Defense) technology is an active defense concept that can transform such a cyber paradigm [4].

B. B. Kang and J. Jang (Eds.): WISA 2018, LNCS 11402, pp. 81–92, 2019.
https://doi.org/10.1007/978-3-030-17982-3_7

MTD technology minimizes information and vulnerability exposure of the target system by dynamically changing the main attributes of the objects to be protected, such as network, platform, software, and data, over time. Suppose an attacker has successfully collected information related to the target system at a particular point in time. However, at the time of the attack, the target system transitions to another state, which making the information collected by the attacker meaningless. MTD technology that changes network attributes increases the complexity of attacker's reconnaissance activities and ultimately blocks attacking activities. In order for the attacker's attack to be finally executed, the data collection and vulnerability analysis for the target system should be sufficiently preceded. Attackers will collect information about the target system in a variety of passive and active ways, such as eavesdropping data flowing in the middle of the network or passing specific data to the target system to analyze its response. Attackers are known to spend considerable time and effort in these reconnaissance activities. The MTD technology for mutating attributes does not block the attacker's reconnaissance activity, but makes it difficult to analyze the collected data and makes the use of the collected data meaningless.

1.2 Related Works

MTD techniques can be classified with the type of attributes to be mutated. In this paper, I consider MTD technique to mutate network attributes. Various techniques for varying network attributes have been proposed [5]. Similar to the NAT (Network Address Translation) concept, the techniques that dynamically convert the IP of each host between communicating hosts can effectively hide the actual IP of the host outside the network. On the other hand, DESIR (Decoy-enhanced seamless IP randomization) [6] constructs a virtual network by adding a number of decoy servers that use the same address range as the real servers, in order to reduce the attacker's network scan efficiency and cause analysis confusion. The changed IP address information of the real server is sent to a separate authentication server. Clients that want to access the real server request the IP address of the real server to the authentication server. That is, the IP address information of the authentication server cannot be changed. Therefore, if an attacker disables the authentication server, there is a risk that the use of the entire network may be restricted. Random Port and Address Hopping (RPAH) scheme [7] creates virtual IP address (*vIP*) and virtual port address (*vPort*) very dynamically using a random value generation function that uses the current time, host ID, and service ID as input values, assuming that all servers and clients share the secret key in advance and are synchronized with each other. The actual address information (*rIP*, *rPort*) is not changed and packets are transmitted using the virtual address. In order to request a new connection to a specific server, the RPAH scheme also obtains the changed address information of the server to access through the DNS server or the authentication server. That is, there is a vulnerability that cannot change the address information of the DNS server or the authentication server like the DESIR technique.

1.3 Tactical Wireless Networks

Tactical wireless networks are characterized by wireless transmission that radio waves can be transmitted to unintended unauthorized nodes. Therefore, the attacker's reconnaissance activity is relatively easy compared to a wired network. On the other hand, the tactical wireless network repeats network configuration and withdrawal depending on its mission and purpose. That is, it is an ad hoc network in which there is no network infrastructure because it is temporarily operated in a certain area for a certain period of time. In general, the communication nodes can share necessary information among the network members before deploying in the operation area. The network is generally layered structure and has a leader node to take account of the efficiency of military missions. However, since the limited radio resources are shared by the members, the network transmission capacity is limited. Therefore, we need MTD technology considering characteristics of tactical wireless network which is distinctly different from wired based commercial network.

In this paper, I propose an IP address mutation scheme that can change the IP address of all communication entities in the same network through common information that is calculated based on received data from the leader node. If the IP address of a particular node changes, the new IP address should be informed to the network members. The DESIR and the RPAH are schemes for individually transmitting the changed IP address information of the node to the necessary members through the third communication entity (DNS server, authentication server, etc.). Therefore, it is not possible to change the address of an entity that is capable of delivering a changed IP address. The existence of an object that cannot change IP address can be critical security vulnerability because it can cause a critical failure of the network operation by a cyber-attack. In the proposed scheme, the changed IP address information is not explicitly transmitted and is shared with the network members by calculating individually. Moreover, the changed IP address information is implicitly transmitted to the members belonging to other networks groups through a layered network structure. Therefore, a third party entity for notifying the changed IP address information is unnecessary. That is, there is an advantage that the IP address information of all communication entities can be changed unlike existing schemes.

This paper is composed as follows. The system model and the threat model are described in Sect. 2. We explain the specific IP mutation procedure of the proposed scheme in Sect. 3 and analyze the performance in Sect. 4. Finally, we conclude in Sect. 5.

2 System and Threat Model

The structure of the layered wireless tactical network considered in this paper is shown in Fig. 1. A network is composed of multiple layers, and each network uses different frequencies. There are many member nodes in each hierarchical network, one of which is a leader node. A leader node of a certain layer may be a member node of an upper layer. For example, Fig. 1, the node h is the leader node of the network A of the layer 1 and the member node of the network C of the layer 2.

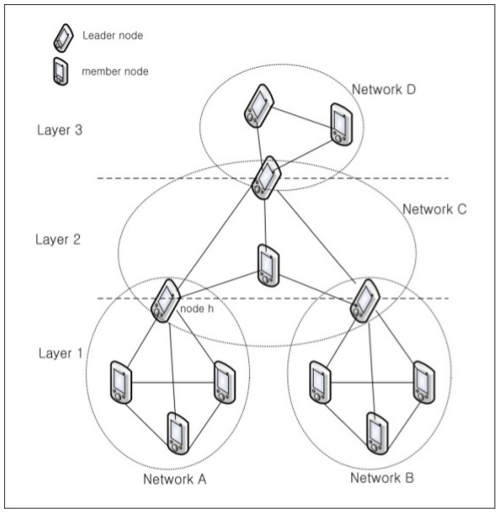

Fig. 1. Tactical wireless network structure

The leader node transmits the data of the upper layer to the lower layer and the data of the lower layer to the upper layer when necessary. To perform this role, the leader node has two IP addresses. The leader node transmits the basic data for the IP mutation to the network members. On the other hand, all nodes have a fixed IP address, *rIP*, which does not change, and a virtual IP address, *vIP*, which changes periodically. An attacker located within the wireless transmission range can obtain information about the frequency used in the network through frequency scanning. Therefore, it is possible to receive data that is transmitted by the legitimate nodes. However, the attacker does not know the IP address information used by the legitimate nodes and uses an arbitrary IP address to access the target system.

3 Address Mutation Scheme Using Projection Matrix

In this section, the projection matrix that is the rationale of the proposed scheme, the address mutation procedures, and data flow between the internal and external network members, are described. Table 1 shows the notation used in this paper.

3.1 Projection Matrix

The proposed scheme basically transforms the IP address by projecting the IP address vector used for each network into an arbitrary vector. When the number of network members is n, the vector $\bar{r}$ and vector $\bar{c}$ are expressed as follows

$$\bar{r} = [rIP_1, rIP_2, \cdots\ rIP_n] \tag{1}$$

$$\bar{c} = [cIP_1, cIP_2, \cdots \ cIP_n] \tag{2}$$

The projection matrix for projecting the vector $\bar{r}$ to a vector $\bar{c}$ is as follows

$$P = \frac{c \cdot c^T}{c^T \cdot c} \tag{3}$$

On the other hand, $\bar{t} = P \cdot \bar{r}$ is the result of projecting the vector $\bar{r}$ to a vector $\bar{c}$.

Table 1. Notation

rIP_i	Fixed IP address for i^{th} node
vIP_i	Mutation IP address for i^{th} node
cIP_i	i^{th} value in reference information vector transmitted by a leader node
uIP_i	i^{th} value in available IP address to be assigned
$\bar{r}$, $\bar{v}$, $\bar{c}$	Vectors with elements of rIP_i, vIP_i and cIP_i
U, V	Sets with elements of uIP_i and vIP_i

3.2 Address Mutation Procedure

The IP address is periodically mutated based on the reference information vector $\bar{c}$ that is transmitted by the leader node. The period in which the leader node transmits the reference information is a system parameter that can vary according to network threat and security requirements.

The leader node constructs a reference information vector $\bar{c}$ by selecting n values randomly within the available address range that do not overlap with each other, and transmits it to the member nodes. Member nodes generate vector $\bar{t}$ by projecting vector $\bar{r}$ to vector $\bar{c}$. By the way, it can be possible that an element of the vector $\bar{t}$ is not be an element of the set of available addresses, **U**. Therefore, it is necessary to map the element of the vector $\bar{t}$ to the element of the set **U**. In the proposed scheme, the elements of the vector $\bar{t}$ are compared with the elements of **U**, and the vector $\bar{q}$ is obtained by mapping the elements of **U** with the smallest value difference. Since the vector $\bar{q}$ is derived from the vector projected into the vector $\bar{c}$, the correlation between the vector $\bar{q}$ and the vector $\bar{c}$ is very high. Moreover, vector $\bar{c}$ is transmitted in wireless environments and is likely to be exposed to attackers. Therefore, if the correlation between two vectors is high, the possibility of estimating the vector $\bar{q}$ from the vector $\bar{c}$ is also high. In order to solve this vulnerability, the proposed scheme rearranges the element position of the vector $\bar{q}$ in a way that is defined beforehand among member nodes, and finally obtains the mutation address vector, $\bar{v}$. This can greatly reduce the correlation between the two vectors.

These processes are performed independently in each hierarchical network, and the leader node mutually shares the result of address change. Also, each node shares the mutated IP address of the member nodes receiving the same reference information vector. Algorithm 1 shows the IP address change procedure of the proposed scheme.

Algorithm 1 address mutation algorithm of the proposed scheme, which is conducted in a fully distributed manner by all network members.

$\bar{t}=P\cdot\bar{r}$

for i = 1 to n

$q_i=\underset{uIP_j \in U}{\operatorname{argmin}}(t_i-uIP_j)^2$

$q_i=\operatorname{argmin}(t_i-uIP_j)^2$

end for

$\bar{v} = rearrange(\bar{q})$

3.3 Data Transmission to Internal Network Members

As described in Sect. 3.2, nodes know the mutated address information of member nodes in the same network. When node *i* transmits data to node *j* in the same network, the source IP is set to vIP_i and the destination IP is set to vIP_j. That is, instead of using a fixed IP address for data transmission, only the mutated IP address is used. Moreover, the IP address used for data transmission is periodically mutated. Therefore the effect of the scanning attack can be reduced.

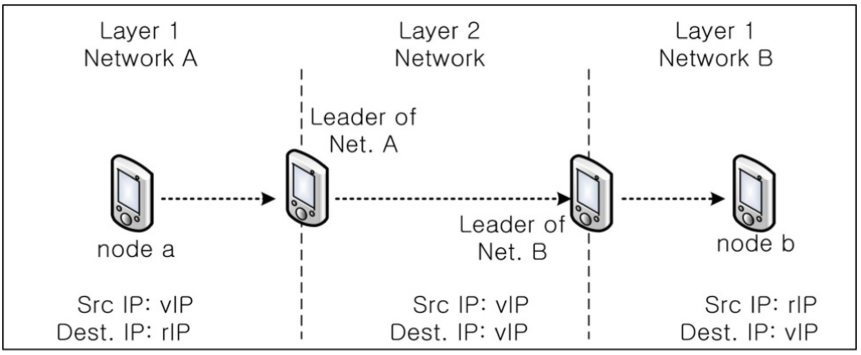

Fig. 2. Source and destination IP address in external communication

3.4 Data Transmission to External Network Members

Figure 2 shows the type of source and destination IP address when transmitting data to external network members in the proposed scheme. At the time of data transmission, the source IP is set to *vIP* and converted to *rIP* by the leader node of the destination. On the other hand, the destination IP is set to *rIP* and converted to the *vIP* by the leader

node of the source network. *rIP* is used only for the network of the sender and receiver, and not for the intermediate network.

In order to transmit data to the external network, frequency conversion must be performed via the leader node because different frequencies are used for each network. The leader node discards the packet if the source address of the received data is not an element of the vector $\bar{v}$. Therefore, the attacker must acquire the *vIP* of the internal member first in order to scan the external member node. However, since the IP address information of the internal member is not only mutated but also the address of the external member node is periodically mutated, the effect of the scanning attack on the external member node is reduced. Table 2 show parameters and its values for performance analysis.

Table 2. Parameters and its value for performance analysis

T	Mutation period
S	Scanning attack trial rate
M	Address mutation rate
$n(U)$	Number of available addresses, 200
$n(V)$	Number of nodes in a network, 1–100
$R\ (= S \times T)$	Number of scanning attack during time T, 1–50

4 Performance Analysis

To analyze the performance of the proposed scheme, I define the address leakage probability, P_L which is the ratio the number of addresses assigned to a network member to the number of addresses leaked by the scanning attack within time T. For ease of analysis, it is assumed that $n(U)$ and $n(V)$ are the same, and P_L for the internal scanning attack and the external scanning attack are respectively examined.

I analyze the overhead caused by the proposed scheme and investigate the correlation between the reference information vector that is transmitted by the leader node and the mutation address vector that is calculated by each member. And I discuss the advantages of the proposed scheme.

4.1 Leakage Probability by Internal Scanning Attack

In the proposed scheme, the address is mutated every time T. It means that the mutation address is valid only for time T. The random variable X represents the number of addresses leaked by the scanning attack during time T. The mutation rate per unit time is $1/T$. If the scan rate per unit time is S, then the number of scanning attacks during time T, R, can be expressed as the product of S and T. Assuming that the attacker knows the information about the address range assigned to the specific network, the probability that the attacker obtains more than one address information during time T is as follows

$$P(X > 0) = 1 - \prod_{i=0}^{R-1} \left(1 - \frac{n(V)}{n(U) - i}\right), \quad n(U) \geq n, R. \tag{4}$$

If the attacker does not know the information about U (that is, there is no information about the address range), the probability of obtaining address information by the scanning attack sharply decreases. This is because the value of $n(U)$ becomes very large. On the other hand, the expected value of the random variable X is calculated as follows

$$\mathrm{E(X)} = \sum_{\mathrm{i}=1}^{\mathrm{n(V)}} \mathrm{i} \times \mathrm{P(X = i)}. \tag{5}$$

The attacker will not scan more than twice for the same IP address during time T. Therefore, scanning addresses is a sampling without replacement problem. In the viewpoint of a specific node, the probability of leakage by internal attack, $\mathrm{P_L^{(I)}}$, is the value of $E(X)$ divided by $n(V)$ in Eq. (5).

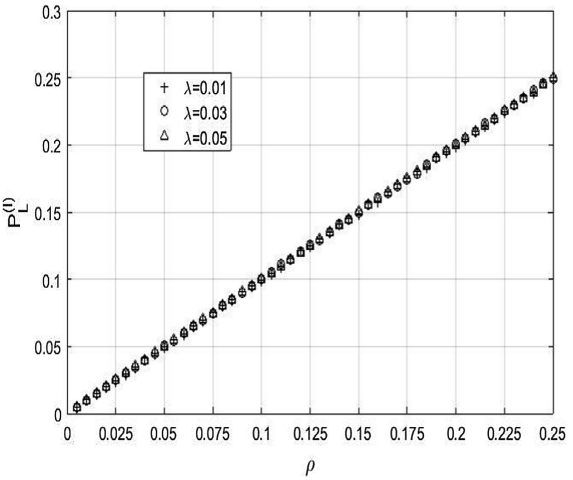

Fig. 3. Address leakage probability according to λ and ρ in internal scanning attack

Figure 3 represents $\mathrm{P_L^{(I)}}$ with the variation of ρ and λ. ρ is the ratio of the number of available addresses ($n(U)$) to the number of scanning attacks (R) during time T, and λ is the ratio of the number of available addresses ($n(U)$) to the number of assigned addresses ($n(V)$). Intuitively, as R increases, the number of leaked addresses increases, and as $n(U)$ increases, the number of leaked addresses decreases because more addresses need to be scanned. Therefore, as shown in Fig. 3, $\mathrm{P_L^{(I)}}$ increases as ρ increases. However, there is no influence by λ. It is a natural result because the number of assigned IP in a network is not related to the leakage probability in the viewpoint of a specific node.

4.2 Leakage Probability by External Scanning Attack

In order to attempt a scanning attack on the external network, the address information of the internal member node should be acquired first. Therefore, it is assumed that the attacker attempts to scan the external member node after the scanning attack on the internal network is successful. Figure 4 represents the probability of leakage by an external scanning attack, $P_L^{(E)}$, with the variation of ρ and λ.

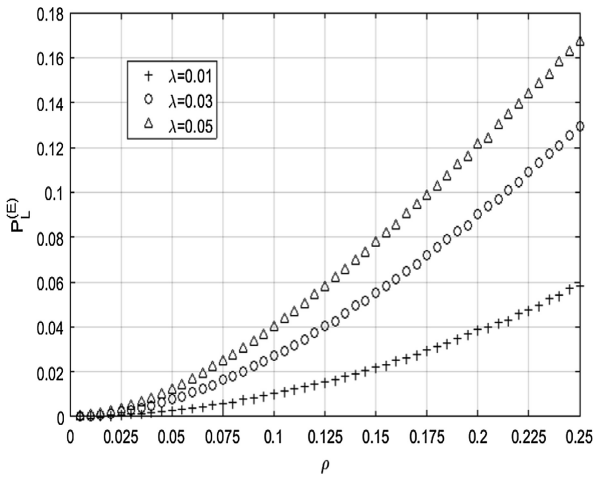

Fig. 4. Address leakage probability according to λ and ρ in external scanning attack

As shown in the Fig. 4, as ρ increases, $P_L^{(E)}$ increases because attacker makes more attack attempts. However, contrary to the internal scanning attack, the probability of leakage increases as λ increases. Large λ means that there are many addresses assigned to the network. Note that a specific IP address in the internal network is not required for the external scanning attack. Any assigned IP address can be used for the external scanning attack. Therefore, an attacker's internal scanning attack can be terminated earlier as the λ is larger, and more attempts can be made for an external scanning attack. For this reason, as shown in Fig. 4, $P_L^{(E)}$ increases as λ increases. On the other hand, Figs. 3 and 4 show that $P_L^{(E)}$ is always smaller than $P_L^{(I)}$ when ρ and λ are the same. This is a natural result because an external scanning attack is possible after an internal scanning attack succeeds.

The performance analysis results show that increasing *n(U)* or shortening time *T* can mitigate the effect of an attacker's internal and external scanning attacks. Since the address information is mutated after time *T*, even if the address information is leaked, the leaked address information can be utilized only by the attacker for a maximum time *T*. That is, since the attacker must repeatedly attempt to scan at every time *T*, it is possible to effectively respond to the scanning attack by using the address mutation scheme.

4.3 Overhead Analysis

The proposed scheme incurs the overhead that the leader node periodically transmits the reference information vector. Therefore, the overhead depends on the size of the reference information vector, the generation period, and the number of leader nodes. The size of the reference information vector increases in proportion to the number of network members, but the number of transmissions does not increase because only the leader node transmits the reference information vector.

On the other hand, the shorter the generation period of the reference information vector is, the more the number of transmission increases, although the size of the vector does not change. As the number of leader nodes increases, the number of messages to be shared among the leader nodes increases. In order to exchange data, an additional overhead due to the communication protocol occurs. Therefore, an increase in the number of transmissions leads to a larger overhead rather than an increase in the size of the reference information vector.

Consider the case of m sub-networks consisting of n members and $2m$ sub-networks consisting of $n/2$ members. Let the former be network A and the latter be network B. The number of members in both networks is equal to $n \times m$. Assume that the address range available to the networks is the same. As we have seen, $P_L^{(E)}$ is smaller as the number of network members is smaller. Therefore, it can be said that network B is safer against scanning attack than A. However, network B has a relatively large number of transmissions between leader nodes as compared with network A because the number of leader nodes is large in network B. That is, the overhead is greatly increased. Therefore, the performance and the overhead of address mutation are in a trade-off relationship and should be appropriately selected in consideration of network size, security threat, and security demand level.

4.4 Similarity Analysis Between Vectors

The reference information vector $\bar{c}$ is transmitted periodically in wireless environment by the leader node. Therefore, if the reference information vector is not encrypted, it can be easily obtainable by an attacker. If an attacker can easily infer mutation address vector $\bar{v}$ from vector $\bar{c}$, it could be a serious security threat. The proposed scheme obtains the vector $\bar{t}$ by projecting the fixed address vector $\bar{r}$ to the reference information vector $\bar{c}$. Then, the vector $\bar{q}$ is obtained by mapping the elements of the vector $\bar{t}$ to the available addresses, the element positions of the vector $\bar{q}$ are rearranged, and finally the mutation address vector $\bar{v}$ is obtained.

The Pearson correlation coefficient was calculated to measure the similarity between these vectors. The Pearson correlation coefficient has a range of -1 to 1, 1 if the two vectors are the same, 0 if they are completely different, and -1 if they are the opposite. Table 3 shows the average of the absolute value of the correlation coefficient between $\bar{c}$ and $\bar{t}$, $\bar{v}$, $\bar{q}$.

Since the vector $\bar{t}$ is the result of projecting the vector $\bar{r}$ onto the vector $\bar{c}$, the correlation coefficient with the vector $\bar{c}$ is always 1. The correlation coefficient between vector $\bar{q}$ that is the result of mapping vector $\bar{t}$ to an available address, is somewhat lower than 1, but its influence is almost negligible, and the degree of lowering of the

correlation coefficient depends on the distribution of available addresses. On the other hand, the correlation coefficient between vector $\bar{c}$ and vector $\bar{v}$, which rearranged the positions of the elements irregularly, was significantly lowered to 0.3 or less. That is, it is not easy to predict the vector $\bar{v}$ even if the attacker obtains the vector $\bar{c}$. Also, since a vector $\bar{c}$ is newly generated every time T, it is difficult for an attacker to obtain a meaningful vector $\bar{v}$.

Table 3. Average absolute Pearson correlation coefficients between vectors

Vectors	$\bar{c}$, $\bar{t}$	$\bar{c}$, $\bar{q}$	$\bar{c}$, $\bar{v}$
Correlation coefficient	1	0.998	0.2744

4.5 Advantage of the Proposed Scheme

The proposed scheme has two advantages over the existing scheme. First, the addresses of all communication entities required for data transmission are mutated. In the case of the existing research [5, 6, 8], the address of the DNS or the authentication server for processing the query of the communication opponent's mutated address information is not changed. Communication entities that perform this function become the weakest part of the address mutation network. If an attacker can exploit the vulnerability of this communication entity, the entire network operation is restricted. However, since the proposed scheme can easily share the mutation address information for internal member nodes and the mutation address information of the external member nodes is distributed and managed by the leader nodes, the problem of single point of failure can be mitigated.

Second, the address of the internal node is needed to scan the external member nodes. If the source address is not the address of the internal node, the leader node does not forward the data to the outside. In other words, the defense against scanning attacks is multi-stepped, and the success probability of a scanning attack is greatly reduced.

5 Conclusion

In this paper, I proposed an address mutation scheme using a projection matrix in a tactical wireless network, in which it has a hierarchical structure. A node can acquire mutated address information for all the network members at once including the leader node by projecting the address information vector to the reference information vector that is transmitted by the leader node. Unlike the existing scheme, address information of all communication entities directly involved in data transmission is mutated. Each node can effectively respond to an attacker's internal and external scanning attacks by using mutated address information. Even if the address information used by the attacker's scanning attack is leaked, the address information is periodically mutated, so that the leaked information becomes meaningful information for the attacker only for a certain period of time.

As a result of analyzing the leakage probability and overhead of the proposed scheme, it was confirmed that the larger the available address range and the smaller the address to be assigned, the better the performance. On the other hand, the overhead caused by the amount of reference information vector transmitted by the leader node, and the number of network members and leader nodes is the tradeoff relationship with the performance on the proposed scheme. Therefore, the network should be designed with the consideration these factors.

References

1. Beraud, P., Cruz, A., Hassell, S., Meadows, S.: Using cyber maneuver to improve network resiliency. In: 2011 - MILCOM 2011 Military Communications Conference, Baltimore, MD, pp. 1121–1126 (2011)
2. Carroll, T.E., Crouse, M., Fulp, E.W., Berenhaut, K.S.: Analysis of network address shuffling as a moving target defense. In: 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, pp. 701–706 (2014)
3. Wang, S., Zhang, L., Tang, C.: A new dynamic address solution for moving target defense. In: 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, pp. 1149–1152 (2016)
4. Tang, H., Sun, Q.T., Yang, X., Long, K.: A network coding and DES based dynamic encryption scheme for moving target defense. IEEE Access **6**, 26059–26068 (2018)
5. Cai, G.-L., Wang, B.-S., Hu, W., Wang, T.-Z.: Moving target defense: state of the art and characteristics. Front. Inf. Technol. Electron. Eng. **17**(3), 1122–1153 (2016)
6. Sun, J., Sun, K.: DESIR: Decoy-enhanced seamless IP randomization. In: IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, pp. 1–9 (2016)
7. Luo, Y.B., Wang, B.S., Wang, X.F., Hu, X.F., Cai, G.L., Sun, H.: RPAH: random port and address hopping for thwarting internal and external adversaries. In: 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, pp. 263–270 (2015)
8. Wu, J.: Meaning and vision of mimic computing and mimic security defense. Telecommun. Sci. **30**(7), 17 (2014)
9. Jafarian, J.H., Al-Shaer, E., Duan, Q.: An effective address mutation approach for disrupting reconnaissance attacks. IEEE Trans. Inf. Forensics Secur. **10**(12), 2562–2577 (2015)