IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS

Received August 5, 2018, accepted September 3, 2018, date of publication September 10, 2018, date of current version October 8, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2869399

Dynamic Defense Strategy Against DoS Attacks Over Vehicular Ad Hoc Networks Based on Port Hopping

YINGMO JIE[1,2], MINGCHU LI[2,3], CHENG GUO[2,3], AND LING CHEN[1,2]

[1]School of Mathematical Sciences, Dalian University of Technology, Dalian 116024, China
[2]School of Software Technology, Dalian University of Technology, Dalian 116620, China
[3]Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, Dalian 116620, China

Corresponding author: Cheng Guo (guocheng@dlut.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61501080, Grant 61572095, Grant 61871064, and Grant 61877007.

ABSTRACT To fight against denial of services (DoS) attacks on vehicular ad hoc networks, which can cause congestion over networks and degrading the user's experience, a lot of detective techniques and schemes have been proposed. However, the complex ones cannot keep pace with the growth of vehicle networks. In this paper, we propose a simple but effective defense strategy scheme inspired by the port-hopping mechanism, which advantage is manifested in that the detection and filtering off of malicious packets launched by attackers can be achieved without any change in existing protocol. First, we design a dynamic defense strategy scheme to puzzle a DoS attacker, where the specific defense strategy will change according to a scheme of time. To mitigate the losses caused by an attacker whose goal is to probe the vulnerable services' ports contained in the UDP/TCP headers between vehicle-to-vehicle or vehicle-to-infrastructure, we add some security services' ports that are valueless to attackers. Second, we give the specific construction of such a defense strategy scheme reflected as a matrix and a security analysis with respect to detecting the probed ports. At last, in comparison with the non-strategy defense scheme, simulations considering some parameters are conducted, which can show that our scheme is an effective defense scheme used for protecting VANETs.

INDEX TERMS Dynamic defense, denial-of-service attacks, port hopping, detection, vehicular ad hoc networks.

I. INTRODUCTION

With the aid of the dedicated short-range communication (DSRC) system, the traditional communication between vehicle and roadside infrastructure provided by vehicular ad hoc networks (VANETs), a type of mobile ad hoc network, has been extended to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications under a highly dynamic topology. Although people have witnessed that VANET offers a lot of convenience, it also triggers some crucial security problems. As the demand for real-time and reliability information transmitted on V2V and V2I communications increases, the channels used to accomplish such communications along with the privacy preservation issue have become quite important. However, such an internet connecting to a large number of vehicles and roadside infrastructure often suffers from more network attacks and threats, which can bring about a series of security problems of VANET. For example, a malicious attacker may affect other vehicles by using a vehicle to send fake messages which may cause harm to road safety if the attacker intercepts private data used to profile users. Moreover, to break the real-time property of VANETs, DoS attackers can unscrupulously consume the available communication bandwidth by injecting a mass of malicious messages, which results in the congestion of networks. In view of the character of DoS attacks, the probe phase before launching attacks plays an important role in the entire procedure. Therefore, many techniques and schemes are proposed to mitigate DoS attacks.

Among other sophisticated techniques, authentication has drawn significant public attention and has been studied comprehensively [1]–[6]. However, with the burgeoning development of vehicle networks, the VANETs have become

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

increasingly pervasive, resulting in an increasing number of devices connected to such networks by wireless technologies. However, the more pervasive the connection, the more vulnerable the devices will become. On the other hand, due to frequent attacks and complex vehicle networks, the cost required to perform authentication for V2V and V2I is quite huge. Hence, the designation of simple but effective techniques used to address the current dilemma is a matter of great urgency.

Recently, a new mechanism named port hopping [7] has been proposed to mitigate DoS attacks over VANETs, which can guarantee that an acceptable level of quality of service can be obtained. The main core of this mechanism is that if the port numbers probed by attackers can be successfully detected, then fake messages contained in malicious packets sent by malicious vehicles can be directly filtered off by checking the relevant port numbers contained in UDP/TCP headers. On the other hand, to increase the difficulty for attackers with respect to probing ''valuable'' ports providing vulnerable services, named vulnerable services' ports, some so-called security services' ports are added, e.g., idle ports and working ports. These have no vulnerable services added. In other word, lots of ports, which numbers are different and usually vary from 0 to 65535, are exposed to attackers. Initially, the ''values'' of these ports are uncertain and need to be probed by attackers. However, considering the observation ability of attackers, static ports can enable attackers to learn the character of each port as time goes on. Hence, different from traditional techniques [8] in which the port numbers are fixed, the vulnerable services' port numbers should vary as a scheme of time. Here, the advantages of port-hopping are simple but feasible, and the existing protocols can be employed for it. Thus, the redundancy of VANETs caused by DoS attacks can be relieved significantly with the help of a port-hopping mechanism.

It is well known that the Internet of things (IoT) security [9]–[11] has consistently been a matter of significance. Although it is difficult to resolve security performance thoroughly in a perfect way, lots of contributions have been proposed. In particular, as one important item of vehicle networks [12]–[13], VANET has received significant attention because the transmissions of real-time and credible messages on V2V and V2I are safety-critical but risk exposure under an open-access situation. Protecting such networks from privacy leakage and malicious attacks is an ongoing issue for current research. Liu *et al.* [14] applied distributed computing to propose a proxy-based authentication used to verify a huge number of vehicles emerging in some areas, but covered only one roadside. The key of this authentication is a verification function that can help proxy vehicles to authenticate multiple messages simultaneously. Considering the privacy preservation of various data, such as a vehicle's or patient's unique identity, position, medical register, and so on, Guo *et al.* [15] employed the ciphertext-policy attributed-based encryption technique to encrypt some important private data, which can guarantee specificity with respect to acquiring private information. To balance the computation efficiency and transmission overhead, a pairing-free certificate-less authentication scheme with batch verification was proposed by Gayathri *et al.* [16].

Moreover, to achieve better performance with respect to privacy preservation, an effective technique [17] used to forward reliable messages was provided. Inspired by a cooperative authentication method, Jo *et al.* [18] proposed an anonymous authentication protocol without demand for extra-mode synchronization. The designation of a key update tree can correct some previous protocols' practical shortcomings. Different from existing symmetric searchable encryption methods such as single keyword search, conjunctive keyword search, multiple keyword search, etc. used to retrieve keywords over encrypted data without decryption, a dynamically multi-phrase-ranked search over encrypted cloud data [19] was introduced. The goal was to search for keywords effectively with little cost as well as considering the case of adding or deleting files.

Besides privacy preservation, another important factor in cloud security is malicious attack detection on vehicle networks for cloud-edge computing [20]. With the objectives of protecting vehicular routes from security threat and considering frequent updated routes, Waraich and Batra proposed a mechanism [21] to calculate the solutions with respect to security routes under the situations of V2V and V2I. Alheeti *et al.* [22] presented an anomaly detection system to delete malicious packets injected by DoS attacks, which can guarantee stability of (semi) self-driving based on real-time communications among vehicles and roadside units. Considering the malicious attacks that manipulate the IEEE 802.11 DCF standards and deceive users who follow the protocol standards, a lightweight technique [23] was proposed to detect the DoS behavior. In particular, this technique can detect and identify the malicious nodes among all nodes in the IEEE 802.11 network under a distributed environment. Compared with some traditional techniques that resist DoS attacks at the cost of consuming many resources used for detecting and filtering malicious packets, a novelty mechanism named port-hopping was proposed. Some schemes [24]–[26] were designed based on such a mechanism and have obtained superb results. However, few of them specifically quantified the performance of resisting DoS attacks in terms of a theoretical perspective; that is what we propose to study here.

In this paper, we design a new port-hopping defense strategy scheme to detect and filter malicious packets for VANET based on singular linear space. While preserving advantages inherited from port-hopping, we also consider the security performance of our scheme in terms of theoretical analysis and experimental simulations. The main contributions of this paper are as follows:

1. A series of novelty Anzahl formulas for special singular linear space used to implement and design a defense strategy scheme.
2. A port-hopping defense strategy scheme used to resist DoS attacks for VANET based on singular linear space.

3. Security analysis with respect to mitigating DoS attacks associated with our scheme.
4. Superb security performance reflected by a simulation comparing our scheme with a random non-strategy scheme.

The rest of this article is organized as follows. In section 2, we introduce some preliminaries employed in this paper. Then, in section 3, we describe the motivation for our paper in detail. Following that, we propose the specific construction of the defense strategy scheme and the relevant security analysis in section 4. Then, we compare our strategy with other methods to show the superiority of ours in section 5. Finally, in section 6, we briefly draw our conclusions with respect to this paper.

II. PRELIMINARIES

In this section, we will introduce some basic definitions used in this paper. Particular, some novelty Anzahl formulas associated with subspaces of type (m, g) in singular linear space [27] are demonstrated by some lemmas.

Definition 1: [28] Let Φ be a $o \times c$ matrix. If there exists a constant $\delta_k \in (0, 1)$, such that for any $k-$ sparse vector $x \in R^c$, we have

$$(1-\delta_k)\|x\|_2^2 \le \|\Phi x\|_2^2 \le (1+\delta_k)\|x\|_2^2, \tag{1}$$

then the matrix Φ is said to satisfy the restricted isometry property (RIP) of order k, and the smallest nonnegative number δ_k in eq. (1) is called restricted isometry constant of order k.

Definition 2: [29] Let Φ be a matrix with columns $u_1, u_2, \cdots, u_c$, the coherence of Φ is defined as

$$\mu(\Phi) = \max_{i \ne j} \frac{| < u_i, u_j > |}{\|u_i\|_2 \cdot \|u_j\|_2}, \quad \text{for } 1 \le i, j \le c. \tag{2}$$

Lemma 3: [30] Suppose Φ is a matrix with coherence μ. Then the RIP of order k associated with Φ satisfies $\delta_k \le \mu(k-1)$, whenever $k < 1/\mu + 1$.

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. Given n and l denoted as two non-negative integers, $\mathbb{F}_q^{n+l}$ represents the $(n+l)-$dimensional row vector space over $\mathbb{F}_q$. The form of

$$\begin{pmatrix} M_{11} & M_{12} \\ 0 & M_{22} \end{pmatrix}$$

represents a $(n+l)\times(n+l)$ nonsingular matrix over $\mathbb{F}_q$, where M_{11} and M_{22} are nonsingular matrices with $n \times n$ and $l \times l$, respectively. Then a group under matrix multiplication named the singular general linear group of degree $n+l$ over $\mathbb{F}_q$ and denoted as $GL_{n+l,n}(\mathbb{F}_q)$ is formed by the set of all above-mentioned $(n+l) \times (n+l)$ nonsingular matrices over $\mathbb{F}_q$. In particular, $GL_{n,n}(\mathbb{F}_q) = GL_n(\mathbb{F}_q)$ or $GL_{l,0}(\mathbb{F}_q) = GL_l(\mathbb{F}_q)$ can be regarded as the general linear group of degree n or l when $l = 0$ or $n = 0$ [31].

Suppose that P is a $m-$dimensional subspace of $\mathbb{F}_q^{n+l}$, which also can be defined as a $m \times (n+l)$ matrix of rank m whose rows span the subspace P. Here, an action of $GL_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{n+l}$ can be defined as follows

$$\mathbb{F}_q^{n+l} \times GL_{n+l,n}(\mathbb{F}_q) \to \mathbb{F}_q^{n+l},$$

$((x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+l}), M) \to (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+l})M$. Note that an action on the set of subspaces of $\mathbb{F}_q^{n+l}$ can be induced by the above action, a subspace P can be derived by $M \in GL_{n+l,n}(\mathbb{F}_q)$ the subspace PM. Therefore, the $(n+l)-$ dimensional singular linear space over $\mathbb{F}_q$ can be constituted by the vector space $\mathbb{F}_q^{n+l}$ together with the above-mentioned group action. Given a row vector represented as $e_i (1 \le i \le n+l)$ in $\mathbb{F}_q^{n+l}$ whose i^{th} coordinate is 1 and all others are 0, the $l-$ dimensional subspace of $\mathbb{F}_q^{n+l}$ denoted as E can be generated by $e_{n+1}, e_{n+2}, \cdots, e_{n+l}$. A $l-$dimensional subspace P of $\mathbb{F}_q^{n+l}$ can be called a subspace of type (m, h) if $\dim(P \cap E) = h$. For $0 \le m \le n$, the attenuated space can be defined as the collection of all subspaces of types $(m, 0)$ in $\mathbb{F}_q^{n+l}$ [32].

Let s_1, s_2 be two integers, the Gaussian coefficient is

$$\begin{bmatrix} s_2 \\ s_1 \end{bmatrix}_q = \frac{\prod_{i=s_2-s_1+1}^{s_2} (q^i - 1)}{\prod_{i=1}^{s_1} (q^i - 1)}, \tag{3}$$

where $\begin{bmatrix} s_2 \\ 0 \end{bmatrix}_q = 1$ for all integer s_2 and $\begin{bmatrix} s_2 \\ s_1 \end{bmatrix}_q = 0$ whenever $s_1 < 0$ or $s_2 < s_1$. According to [31], we know that $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is the number of $m-$dimensional subspaces of $\mathbb{F}_q^n$.

Lemma 4: Suppose that P is the subspace of type (m, h) over $\mathbb{F}_q^{n+l}$. Given a subspace W of type $(m-d, h-f)$ contained in P, the set of all subspaces U of type (r, g) contained in P satisfying $U+W = P$ is represented as $R(r, g; d, f; m, h)$ whose size is denoted as $N(r, g; d, f; m, h)$. Then we can obtain

$$N(r, g; d, f; m, h) = q^{(d-f)(n-r+g)} \begin{bmatrix} n-d+f \\ r-g-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g \end{bmatrix}_q. \tag{4}$$

Proof: Based on the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$ above the set of (P, W), the forms can be assumed as the equation can be derived, as shown at the top of the next page.

Akin to the above-mentioned, U can also be represented as the form

$$U = \begin{pmatrix} M_1^{(r-g-d+f,\, n-d+f)} & 0 & 0 & 0 \\ M_2^{(d-f,\, n-d+f)} & I^{(d-f)} & M_3^{(d-f,\, h)} & M_4^{(d-f,\, l-h)} \\ 0 & 0 & M_5^{(g,\, h)} & 0 \end{pmatrix},$$

where M_1 is a $(r-g-d+f) \times (n-d+f)$ matrix of rank $(r-g-d+f)$ and M_5 is a $g \times h$ matrix of rank g. The number of choices for M_1 is $\begin{bmatrix} n-d+f \\ r-g-d+f \end{bmatrix}_q$ and M_5 is $\begin{bmatrix} h \\ g \end{bmatrix}_q$ [31]. With the help of the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$, we may get

$$M_1 = \begin{pmatrix} I^{(r-g-d+f)} & 0^{(r-g-d+f,\, n-r+g)} \end{pmatrix},$$

$$P = \begin{pmatrix} I^{(m-h)} & 0^{(m-h,n-m+h)} & 0 & 0 \\ 0 & 0 & I^{(h)} & 0^{(h,l-h)} \end{pmatrix},$$
$$W = \begin{pmatrix} I^{(m-d-h+f)} & 0^{(m-d-h+f,n-m+d+h-f)} & 0 & 0 \\ 0 & 0 & I^{(h-f)} & 0^{(h-f,l-h+f)} \end{pmatrix}.$$

and

$$M_5 = \begin{pmatrix} I^{(g)} & 0^{(g,h-g)} \end{pmatrix}.$$

Then, U has the unique matrix representation of the form

$$U = \begin{pmatrix} I^{(r-g-d+f)} & 0^{(r-g-d+f,n-r+g)} & 0 & 0 & 0 \\ 0 & A_1^{(d-f,n-r+g)} & 0^{(d-f)} & 0 & 0^{(d-f,l-g)} \\ 0 & 0 & 0 & I^{g} & 0 \end{pmatrix}.$$

Hence

$$N(r,g;d,f;m,h) = q^{(d-f)(n-r+g)} \begin{bmatrix} n-d+f \\ r-g-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g \end{bmatrix}_q.$$

Lemma 5: Suppose that P is the subspace of type (m,h) over $\mathbb{F}_q^{n+l}$ and W is a subspace of type $(m-d, h-f)$ contained in P. Given a subspace U_2 of type (r_2,g_2) contained in P satisfying $U_2+W=P$, the number of subspaces U_1 of type (r_1,g_1) contained in P satisfying $U_1+W=P$ and $U_1 \subseteq U_2$ denoted as $N(r_1,g_1;r_2,g_2;d,f;m,h)$ is

$$q^{(d-f)(r_2-r_1+g_1)} \begin{bmatrix} r_2-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q.$$

Proof: Fixing W, as the subgroup $GL_{n+l,n}(\mathbb{F}_q)_W$ associated with $GL_{n+l,n}(\mathbb{F}_q)$ acts transitively on the set $\{U | U+W=P, \dim U = r_2\}$, $N(r_1,g_1;r_2,g_2;d,f;m,h)$ only depends on r_1 and r_2. By lemma 4 and eq. (4), we can get

$$N(r_1,g_1;r_2,g_2;d,f;m,h) = q^{(d-f)(r_2-r_1+g_1)} \begin{bmatrix} r_2-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q. \quad (5)$$

Lemma 6: Suppose that P is the subspace of type (m,h) over $\mathbb{F}_q^{n+l}$ and W is a subspace of type $(m-d, h-f)$ contained in P. Given a subspace U_1 of type (r_1,g_1) contained in P satisfying $U_1+W=P$, the number of subspaces U_2 of type (r_2,g_2) contained in P satisfying $U_2+W=P$ and $U_1 \subseteq U_2$ is

$$N'(r_1,g_1;r_2,g_2;d,f;m,h) = q^{(d-f)(h_1-g_1)} \begin{bmatrix} n-r_1+g_1 \\ r_2-g_2-r_1+g_1 \end{bmatrix}_q \begin{bmatrix} h-g_1 \\ g_2-g_1 \end{bmatrix}_q. \quad (6)$$

Proof: Let S be a set satisfying

$$S = \left\{ (U_1,U_2) \,\middle|\, \begin{matrix} U_1 \in R(r_1,g_1;d,f;m,h), \\ U_2 \in R(r_2,g_2;d,f;m,h), \\ U_1 \subseteq U_2 \end{matrix} \right\}.$$

Here, we compute the size of S in terms of two ways. First, given a fixed subspace U_1 of type (r_1,g_1), the number of subspaces U_2 of type (r_2,g_2) containing U_1 is $N'(r_1,g_1;r_2,g_2;d,f;m,h)$. Based on lemma 4, we get

$$|S| = N'(r_1,g_1;r_2,g_2;d,f;m,h) \cdot N(r_1,g_1;d,f;m,h). \quad (7)$$

Then, given a fixed subspace U_2 of type (r_2,g_2), the number of subspaces U_1 of type (r_1,g_1) contained in U_2 is $N(r_1,g_1;r_2,g_2;d,f;m,h)$. Based on lemma 4, we can also get

$$|S| = N(r_1,g_1;r_2,g_2;d,f;m,h) \cdot N(r_2,g_2;d,f;m,h). \quad (8)$$

Hence, combining eqs. (4), (5), (7) and (8), (6) holds.

Lemma 7: Given integers $0 \le g_1 \le g_2 \le h \le l$ and $0 \le m-d-h+f \le m-h \le n-l$, the sequence $N(r,g;d,f;m,h)$ is unimodal and gets its peak at $r_2 = \left\lfloor \frac{n+1}{2} \right\rfloor - g$.

Proof: According to lemma 4, let $r_1 < r_2$, then we can get

$$\begin{aligned} \frac{N(r_1,g;d,f;m,h)}{N(r_2,g;d,f;m,h)} &= \frac{q^{(d-f)(n-r_1+g)} \begin{bmatrix} n-d+f \\ r_1-g-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g \end{bmatrix}_q}{q^{(d-f)(n-r_2+g)} \begin{bmatrix} n-d+f \\ r_2-g-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g \end{bmatrix}_q} \\ &= q^{(d-f)(r_2-r_1)} \cdot \frac{\prod_{i=r_1-g-d+f+1}^{r_2-g-d+f} (q^i-1)}{\prod_{i=n-r_2+g+1}^{n-r_1+g} (q^i-1)} \\ &= \frac{(q^{r_1-g+1}-q^{d-f}) \cdots (q^{r_2-g}-q^{d-f})}{(q^{n-r_2+g+1}-1) \cdots (q^{n-r_1+g}-1)} \\ &= \frac{q^{r_1-g+1}-q^{d-f}}{q^{n-r_1+g}-1} \cdots \frac{q^{r_2-g}-q^{d-f}}{q^{n-r_2+g+1}-1}. \end{aligned}$$

$$\frac{q^{r_1-g+1}-q^{d-f}}{q^{n-r_1+g}-1} < \frac{q^{r_1-g+2}-q^{d-f}}{q^{n-r_1+g-1}-1} < \cdots < \frac{q^{r_2-g}-q^{d-f}}{q^{n-r_2+g+1}-1} < 1$$

can be obtained when $r_1 < r_2 \le \left\lfloor \frac{n+1}{2} \right\rfloor - g$, i.e., $\frac{N(r_1,g;d,f;m,h)}{N(r_2,g;d,f;m,h)} < 1$. Reversely, $1 < \frac{q^{r_1-g+1}-q^{d-f}}{q^{n-r_1+g}-1} < \frac{q^{r_1-g+2}-q^{d-f}}{q^{n-r_1+g-1}-1} < \cdots < \frac{q^{r_2-g}-q^{d-f}}{q^{n-r_2+g+1}-1}$ can be got when $\left\lfloor \frac{n+1}{2} \right\rfloor -$

$g \leq r_1 < r_2$, i.e., $\frac{N(r_1,g;d,f;m,h)}{N(r_2,g;d,f;m,h)} > 1$. Hence, the desired results follows.

III. MOTIVATIONS

In this section, we will describe DoS attacks on vehicle networks and introduce the effective mechanism called port-hopping used to detect such attacks.

A. DOS ATTACKS

As one of the main threats to Internet security during the era of Big Data [33]–[34], DoS attacks have been noted for their high frequency and ubiquity [35]. Before launching attacks, attackers first will probe some ports to determine whether or not they are the vulnerable services' ports attackers seek. This can be called the reconnaissance phase. Generally, the port number varies from 0 to 65535, and space 0 through 1023 are well-known for providing standard services. For example, port 25 is used for simple mail transfer protocol and port 69 is employed for trivial file transfer protocol. In fact, ports under such exemplifications are vulnerable to being probed out and then attacked in terms of malicious packets, which are difficult to detect and filter out reliably. However, most of the existing techniques used to address such attacks are complex due to the growth of Internet systems such as vehicle networks. Hence, proposing a simple scheme to successfully fight against DoS attacks has become more and more crucial.

Here, in order to design a simple but effective scheme employed to address DoS attacks, we will introduce such attacks in terms of mathematics. Specifically, the total number of ports is c, which include the vulnerable services' ports and secure services' ports—such as ports not in use or ports that are active but not associated with providing vulnerable services. On the other hand, compared to the total number of ports, the attacker—whose objective is to discover the vulnerable services' ports and then launch DoS attacks against the relevant ports—expects to use k resources to probe k ports from all these ports. Hence, a $k-$attack can be denoted as a vector $x \in R^c$ whose nonzero entries size is $k < c$, i.e., the size of the support set associated with x is k. Given an attack x, if the attacker probes a port, the value of the corresponding entry belonging to x is nonzero, and vice versa.

B. PORT HOPPING

Port hopping is proposed as an uncomplicated method to address the vulnerability of ports. Specifically, in this method, different from traditional ones such as UDP and TCP protocols wherein the port numbers are fixed, the server's port numbers change dynamically as a function (schedule) of time. A cryptographic key is shared between the server, who keeps some ports open to provide network services, and the user. At any time, the port number will be decided by the user who owns the key, which will guarantee that the attackers cannot learn the current valid port number. Then, the illegitimate packets can be easily filtered off by the server in terms of inspecting the port numbers contained in the UDP/TCP headers.

In this paper, we add a secure and trustworthy third part-administrator to directly design a defense strategy scheme, i.e., a function (schedule) of time used to decide the port number for any time. Hence, the key used to determine the port number can be neglected. In the next section, we will demonstrate this strategy in detail.

IV. DESIGN AND ANALYSIS

In this section, we will provide the specific construction of a defense strategy scheme inspired by a port-hopping mechanism against DoS attacks, and the relevant security analysis.

A. DESIGN PRINCIPLE

Before proposing the designation of a defense strategy scheme, we will explain the principle inspired by the port-hopping and sensing matrix associated with singular linear space. First of all, to satisfy the demand for the dynamic property of port hopping, service time can be divided into o slots, and for any slot i, $1 \leq i \leq o$, the administrator needs to provide a defense strategy, which can be formulated as a binary vector $y \in \{0, 1\}^c$, where the entry with "1" can be interpreted that the corresponding port is used to provide vulnerable services; otherwise, such a port can be viewed as a secure services' port. Here, we assume that the number of ports employed to provide vulnerable services for any slot is fixed as s, i.e., the size of support set of y is equal to s. Therefore, the defense strategy of all slots can be constructed as a matrix whose size is $o \times c$, where each row represents a defense strategy corresponding to a slot and each column represents an available port. Note that based on the above-mentioned information, the number of nonzero associated with each row is equal to s. On the other hand, to guarantee the balance of utilization associated with each port used to provide vulnerable services, we assume that the number of nonzero associated with each column is also the same and denoted by t. Considering the actual situation, compared with the number of available ports, that of the slots is smaller, which means that $o < c$ should be satisfied. Hence, such a matrix can be regarded as a defense strategy scheme that we will propose in the next subsection.

After demonstrating the formation of a defense strategy scheme, we need to explain the corresponding working principle of it. Given a defense strategy scheme denoted as a matrix $\Phi_{o\times c}$, which is unknown to attackers, a detective vector $z = \Phi x \in R^o$ contains the attack information when an uncertainty probe attack x is launched. The goal of the administrator is to learn the specific ports probed by the attacker, i.e., attack x. Hence, what the administrator should do is to reconstruct the original probe attack x with $z = \Phi x$, although it is an underdetermined linear system for $o < c$. Fortunately, the problem had been solved by Donoho [36] and Candes *et al.* [37], a solution which can be described as finding the sparsest solution of linear equations $z = \Phi x$ such

that

$$\min_{x\in R^c} \|x\|_0 \text{ s.t. : } \Phi x = z. \tag{9}$$

Although this l_0 – minimization, named a combinatorial minimization problem, is regarded as NP-hard [38], a greedy algorithm, called orthogonal matching pursuit (OMP) [39], can be employed to solve eq. (9). Given the above, the objective of this paper is to study the construction of matrix $\Phi_{o\times c}$ and analyze its security performance. It was pointed out by Candes and Tao [40] that the performances is tied to the RIP mentioned by definition 1.

B. CONSTRUCTION AND SECURITY ANALYSIS

In this subsection, we will provide the specific designation of defense strategy matrix Φ with size of $o \times c$ as well as the corresponding analysis of security performance. To make it more intuitive and straightforward, some special cases of defense matrices will also be shown.

Construction 8: Given integers $0 \le g_1 \le g_2 \le h \le l, 0 \le r_1 - g_1 \le r_2 - g_2 \le \min\{\lfloor \frac{n+1}{2} \rfloor, m-d-h+f\}$ and $m-d-h+f < m-h \le n-l$, let Φ be the binary matrix with rows indexed with $\Re(r_1, g_1; d, f; m, h)$, and columns indexed with $R(r_2, g_2; d, f; m, h)$ such that $\Phi(i, j) = 1$ if and only if j^{th} subspace U_2 of type (r_2, g_2) contains i^{th} subspace U_1 of type (r_1, g_1), where $U_1 \in R(r_1, g_1; d, f; m, h)$ and $U_2 \in R(r_2, g_2; d, f; m, h)$.

According to lemmas 4, 5 and 6, Φ is a $o \times c$ binary matrix and each column (row) has the same number of nonzero entries, i.e., the weight of each column (row) is equal and denoted as $t(s)$, where

$$\begin{aligned} o &= N(r_1, g_1; d, f; m, h) \\ &= q^{(d-f)(n-r_1+g_1)} \begin{bmatrix} n-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g_1 \end{bmatrix}_q, \end{aligned} \tag{10}$$

$$\begin{aligned} c &= N(r_2, g_2; d, f; m, h) \\ &= q^{(d-f)(n-r_2+g_2)} \begin{bmatrix} n-d+f \\ r_2-g_2-d+f \end{bmatrix}_q \begin{bmatrix} h \\ g_2 \end{bmatrix}_q, \end{aligned} \tag{11}$$

$$\begin{aligned} t &= N(r_1, g_1; r_2, g_2; d, f; m, h) \\ &= q^{(d-f)(r_2-r_1+g_1)} \begin{bmatrix} r_2-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q, \end{aligned} \tag{12}$$

$$\begin{aligned} s &= N'(r_1, g_1; r_2, g_2; d, f; m, h) \\ &= q^{(d-f)(h-g_1)} \begin{bmatrix} n-r_1+g_1 \\ r_2-g_2-r_1+g_1 \end{bmatrix}_q \begin{bmatrix} h-g_1 \\ g_2-g_1 \end{bmatrix}_q. \end{aligned} \tag{13}$$

Lemma 7 guarantees the demand for $o < c$, the reason behind this demand is that compared with the number of time slots, that of total ports is quite larger in terms of practical applications.

Construction 9: Given the matrix Φ constructed by construction 8, it can be used as a defense strategy scheme when the numbers of slots, total ports, and vulnerable services' ports are o, c, and s, respectively.

Next, we will provide the security performance of our defense strategy scheme in terms of theoretic analysis. The security analysis of this scheme, reflected by the above-constructed matrix, will be explored by theorem 11 in this subsection. Practically, the security analysis is mainly used to consider the ability of the scheme to detect the probed ports vulnerable to DoS attackers. Mathematically, we will study the reconstruction of attack x with defense matrix Φ.

Lemma 10: Suppose that $0 \le g_1 \le g_2 \le h \le l$, $0 \le r_1 - g_1 \le r_2 - g_2 \le \min\{\lfloor \frac{n+1}{2} \rfloor, m-d-h+f\}$ and $m-d-h+f < m-h \le n-l$, then the coherence of matrix Φ is $\mu(\Phi) = \frac{q^{r_2-r_1+g_1}-1}{q^{r_2}-q^{d-f}}$, which can guarantee that the RIP of order k with $\delta_k \le \frac{(k-1)(q^{r_2-r_1+g_1}-1)}{q^{r_2}-q^{d-f}}$, can be satisfied, whenever $k \le \left\lfloor \frac{q^{r_2}-q^{d-f}}{q^{r_2-r_1+g_1}-1} + 1 \right\rfloor$, where $\left\lfloor \frac{q^{r_2}-q^{d-f}}{q^{r_2-r_1+g_1}-1} + 1 \right\rfloor$ is defined as the lower bound of k.

Proof: Construction 8 illustrates that the number of nonzero entries for each column of Φ is the same and equals to

$$w = q^{(d-f)(r_2-r_1+g_1)} \begin{bmatrix} r_2-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q,$$

which can be regarded as the constant value of the denominator in eq. (2). Therefore, the calculation of coherence μ of Φ can be turned to calculate the maximum value of $| < u_i, u_j > |$. As the description of construction 8, the columns of Φ are indexed by the subspaces U_2^j, where $U_2^j \in \Re(r_2, g_2; d, f; m, h)$, $1 \le i \le N(r_2, g_2; d, f; m, h)$. Note that any two different columns U_2^j and $U_2^{j'}$ can be formulated as any two distinct subspaces of type (r_2, g_2). Hence, our objective is to calculate the maximum value of $| < U_2^j, U_2^{j'} > |$, i.e., the maximum number of $U_1^i \in \Re(r_1, g_1; d, f; m, h)$ which are contained in U_2^j and $U_2^{j'}$ formulated as $U_1^i \subseteq U_2^j$, $U_1^i \subseteq U_2^{j'}$ simultaneously. As the intersection of two subspaces is also a subspace, then let $U_2 = U_2^j \cap U_2^{j'}$ be a subspace whose rank is $r_2 - 1$ and the intersection with E is g_2. Hence, the maximum value of $| < U_2^j, U_2^{j'} > |$ equals to the number of subspaces of type $(r_2 - 1, g_2)$, which can be formulated as

$$v = q^{(d-f)(r_2-1-r_1+g_1)} \begin{bmatrix} r_2-1-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q.$$

Based on definition 2, then

$$\begin{aligned} \mu(\Phi) &= \frac{q^{(d-f)(r_2-1-r_1+g_1)} \begin{bmatrix} r_2-1-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q}{q^{(d-f)(r_2-r_1+g_1)} \begin{bmatrix} r_2-d+f \\ r_1-g_1-d+f \end{bmatrix}_q \begin{bmatrix} g_2 \\ g_1 \end{bmatrix}_q} \\ &= \frac{q^{r_2-r_1+g_1}-1}{q^{r_2}-q^{d-f}}. \end{aligned} \tag{14}$$

By lemma 3, Φ satisfies the RIP of order k with $\delta_k \le \frac{(k-1)(q^{r_2-r_1+g_1}-1)}{q^{r_2}-q^{d-f}}$, whenever $k \le \left\lfloor \frac{q^{r_2}-q^{d-f}}{q^{r_2-r_1+g_1}-1} + 1 \right\rfloor$.

Theorem 11: Given the matrix Φ with the RIP of order k, then the defense strategy matrix Φ can fight against any DoS attack with probe resources no more than the lower boundary

of k, i.e., any DoS attack x cannot be successful when the support set of x denoted by $S(x)$ satisfies

$$S(x) \leq \left\lfloor \frac{q^{r_2} - q^{d-f}}{q^{r_2-r_1+g_1} - 1} + 1 \right\rfloor. \tag{15}$$

Proof: From lemma 10, we know that the matrix Φ owns the RIP of order k, which can be simply read as: the RIP of order k corresponding to Φ can be defined as the ability to learn about any unknown attack x. When the size of x's support set is smaller than the lower boundary of k, then x can be exactly learned, i.e., we can successfully fight against such DoS attacks. Otherwise, we cannot guarantee the truth of x.

Next, we will provide several special cases for our defense strategy matrices and the relevant defense ability against DoS attacks.

Case 1: Let q be a large prime power. Given the parameters with $d = f$, $g_1 = g_2 = 0$, $n = 2r_2 = 4r_1$, then we can obtain an $o_1 \times c_1$ matrix Φ_1 with

$$o_1 = \begin{bmatrix} 4r_1 \\ r_1 \end{bmatrix}_q, \quad c_1 = \begin{bmatrix} 4r_1 \\ 2r_1 \end{bmatrix}_q, \; t_1 = \begin{bmatrix} 2r_1 \\ r_1 \end{bmatrix}_q,$$
$$s_1 = \begin{bmatrix} 3r_1 \\ r_1 \end{bmatrix}_q, \quad \mu(\Phi_1) = \frac{1}{q^{r_1} + 1}.$$

Φ_1 satisfies the RIP of order $k_1 \leq q^{r_1} + 1$ and has sparsity order with $k = \Theta(s^{1/2})$, i.e., given the number of vulnerable services' ports s, the ability to protect these ports is measured by $k = \Theta(s^{1/2})$.

Case 2: Let q be a large prime power. Given the parameters with $d - f = 1$, $g_1 = g_2 = h$, $n = 2r_2 = 4(r_1 - h)$, then we can obtain an $o_2 \times c_2$ matrix Φ_2 with

$$o_1 = q^{n-r_1+h} \begin{bmatrix} 4r_1 - 4h - 1 \\ r_1 - h - 1 \end{bmatrix}_q,$$
$$c_1 = q^{2r_1-h} \begin{bmatrix} 4r_1 - 4h - 1 \\ 2r_1 - 3h \end{bmatrix}_q,$$
$$t_1 = q^{r_1-h} \begin{bmatrix} 2r_1 - 2h - 1 \\ r_1 - h - 1 \end{bmatrix}_q, \quad s_1 = \begin{bmatrix} 3r_1 - 3h \\ r_1 - 2h \end{bmatrix}_q,$$
$$\mu(\Phi_2) = \frac{1}{q^{r_1-h} + 1}.$$

Φ_2 satisfies the RIP of order $k_2 \leq q^{r_1-h} + 1$ and has sparsity order with $k = \Theta(s^{1/2})$, i.e., given the number of vulnerable services' ports s, the ability to protect these ports is measured by $k = \Theta(s^{1/2})$.

V. PERFORMANCE EVALUATION

To evaluate our method's ability for detecting the DoS attackers' probes, we present our simulations to quantify the likelihood of attacker success in terms of the number of total ports, number of probe ports with respect to attacker, number of vulnerable services' ports, and hopping frequency. We compare our method with other non-strategies to demonstrate its superiority. All computations are run on a machine with 2.3GHz Intel Core i5 with 8 GB memory.

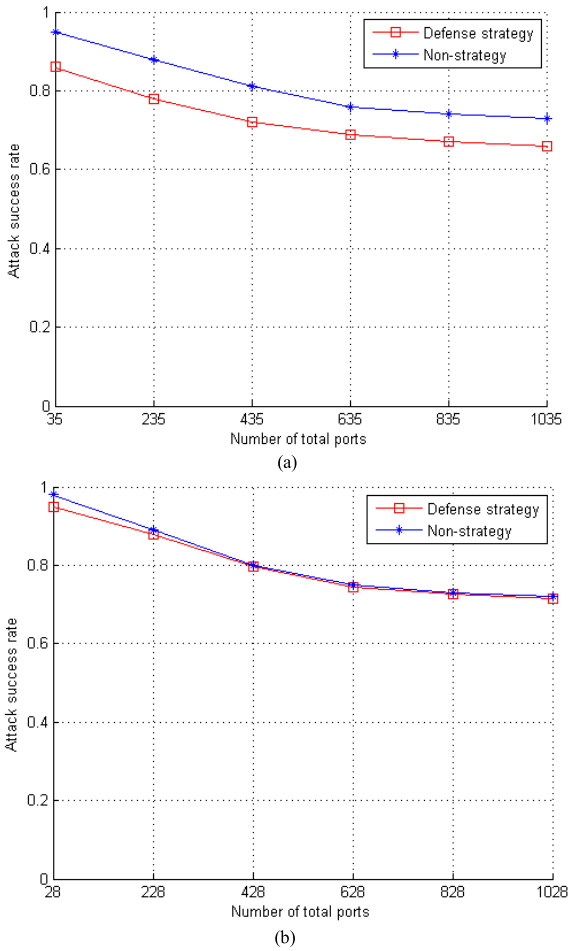


FIGURE 1. The comparison of total ports. (a) Case 1. (b) Case 2.

In the simulations, we test the performance of our strategy in terms of the attack success rate, which can be explained as follows: Given a probe attack x, OMP is used to solve l_0- minimization in eq. (9) and the solution is denoted as x'. Inspired by the idea of reconstructing the signal-to-noise ratio (SNR) [41] defined as

$$\mathrm{SNR}(x) = 10 \cdot \log_{10}\left(\frac{\|x\|_2}{\|x - x'\|_2}\right) dB, \tag{16}$$

we can assume that if $SNR(x)$ is no less than 100 dB, then the recovery of x is perfect, i.e., the probe attack has been detected perfectly. Given the value of k associated with probe attack's ability, we input 5000 random attacks to compute the perfect detecting percentage.

In summary, the main steps for exploring the security performance associated with defense strategy matrices are as follows:

- First of all, based on two cases mentioned in Section 4, we choose the appropriate emerging parameters to achieve various matrices with different rows (slots) os, columns (total ports) cs, weights of rows (vulnerable services' ports) ss and abilities to detect probe ports ks.
- Then, we need to compare our defense strategy matrices with non-strategy matrices, which can be regarded as

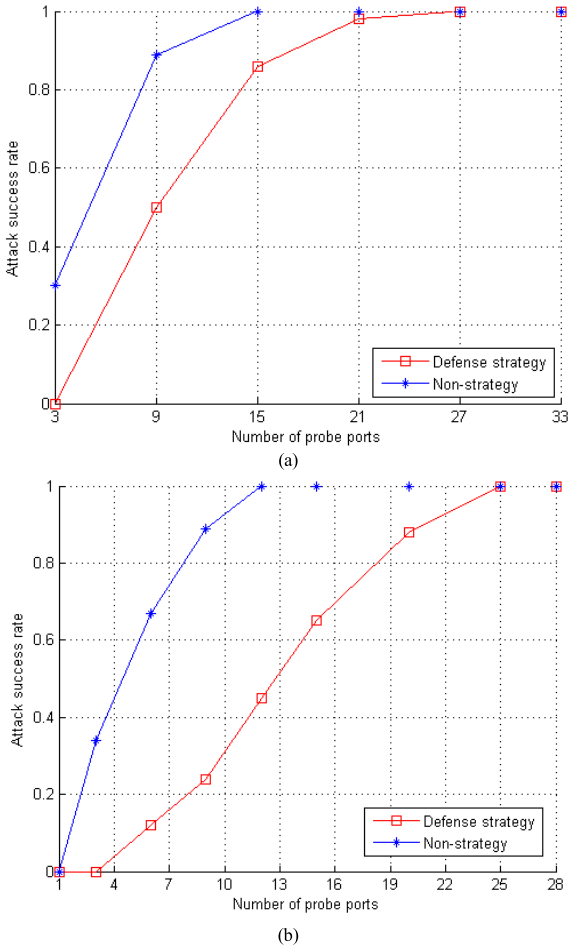


FIGURE 2. The comparison of probe ports. (a) Case 1. (b) Case 2.

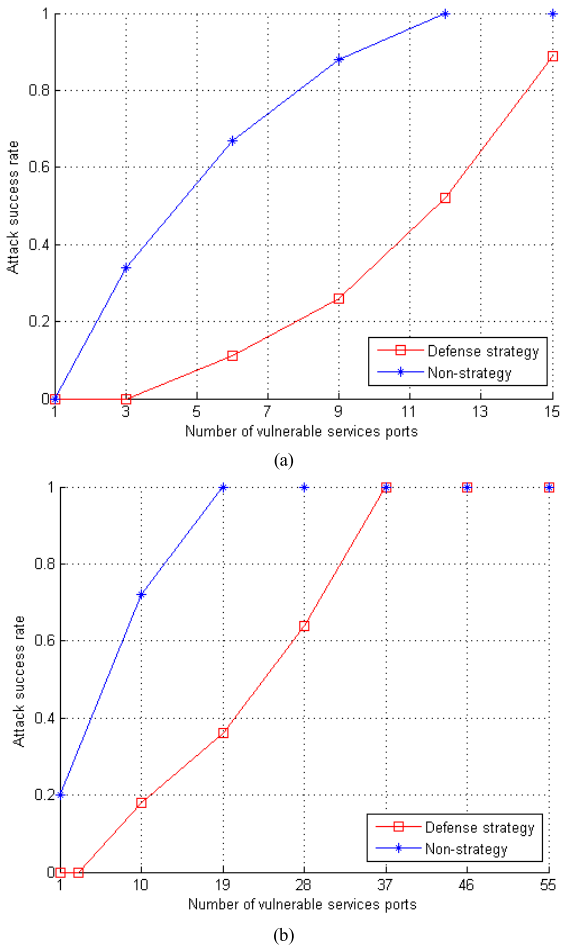


FIGURE 3. The comparison of vulnerable service's ports. (a) Case 1. (b) Case 2.

random Gaussian defense matrices chosen without any strategy. To guarantee the comparability, given a test parameter, we assign these matrices being compared with the same numbers of other ones.

A. NUMBER OF TOTAL PORTS

We compare the security performance of our defense strategy matrices with non-strategy ones by evaluating the number of total ports' influence, denoted as c. The defense strategy matrices simulated in Figs. 1(a) and 1(b) are based on case 1 and case 2, respectively, where the x-axis is the number of total ports, and y-axis is the rate of attack success. Here, we mainly consider the well-known service ports ranging from 0 to 1023. For the random non-strategy matrices, we choose the Gaussian ones to compare with ours under the assumption that both of them have the same number of ports. From the results of Fig. 1, we can observe that although the attack success rate is quite high when the number of total ports is small, it decreases as that of ports increase. Both of the cases are better than random matrices; in particular, the performance of case 1 reduces the rate of attack success by 10% as compared to random non-strategy matrices.

B. NUMBER OF PROBE PORTS

The number of probe ports denoted as k and decided by DoS attackers is also an important factor that influences the attack success rate. In fact, as some existing schemes used to fight against DoS attacks were introduced by the operating systems, the number of probe ports available to attackers is limited. Given other parameters, we test the security performance of case 1 and case 2 by exploring the ability of attackers, reflected by Figs. 2(a) and 2(b), respectively. The x-axis is the number of probe ports and y-axis is the attack success rate. As shown in Fig. 2, the attack success rate against our defense strategy matrices increases at a slower rate compared to that against random non-strategy ones, which increase significantly as the number of probe ports grows. However, the attack success rate is quite high when the number of probe ports is large enough, i.e., the ability DoS of attacker is powerful enough.

C. NUMBER OF VULNERABLE SERVICES' PORTS

As a matter of fact, the number of vulnerable services' ports denoted as s is also a significant factor affecting the attack success rate. The attacker's goal is to probe out at least one

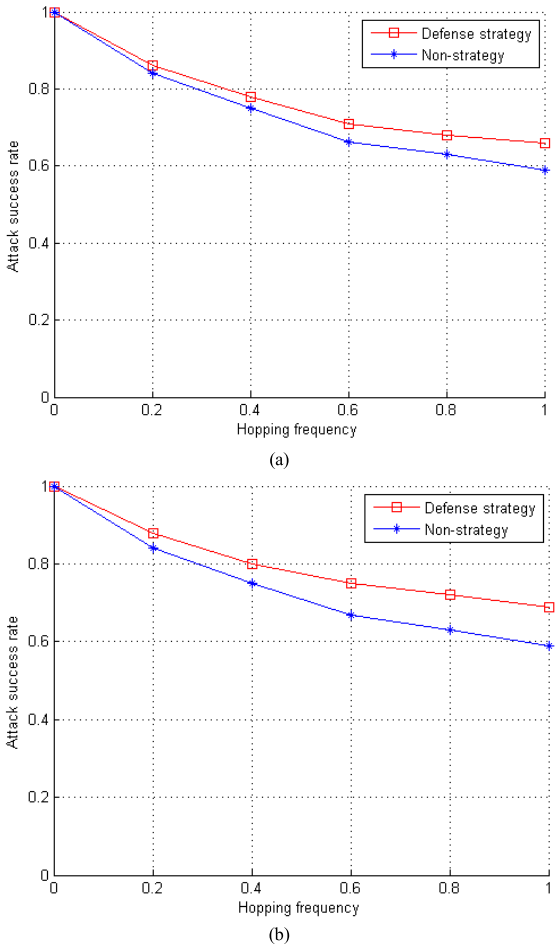


FIGURE 4. The comparison of hopping frequency. (a) Case 1. (b) Case 2.

of the vulnerable services' ports. Thus, Figs 3(a) and 3(b) are used to demonstrate the security performance of our defense strategy matrices by considering the influence of the number of vulnerable services' ports, where the x-axis is the number of vulnerable services' ports and y-axis is the attack success rate. Obviously, the results of Fig. 3 illustrate that our scheme can fight against DoS attacks perfectly when the number of vulnerable services' ports $s \leq 3$. However, with the growth of the number of vulnerable services' ports, the rate of attack success can quickly reach 1. Hence, our defense scheme can be regarded as an effective one when the number of vulnerable services' ports is small.

D. HOPPING FREQUENCY

As another important factor that can influence the attack success rate, the frequency of port hopping will be considered in this part of the simulation. As this paper has mentioned, the service time can be divided into o slots to satisfy the demand for dynamic property of port hopping. For each slot, the defense strategy will make a change. Here, hopping frequency can be defined as the ratio of the number of slots to that of total ports, i.e., o/c. If the defense strategy does not change any more after the first slot, this case can be called a static ports defense strategy, and the value of hopping frequency equals 0. On the other hand, with the constraint $o < c$, the case of near-perfect ports defense strategy can be derived when the value of hopping frequency is close to 1. From the results of Fig. 4, we can see that the attack success rate decreases with the growth of hopping frequency, which proves the importance of port hopping.

VI. CONCLUSION

In this paper, to mitigate DoS attacks on VANETs effectively, we introduce port hopping and singular linear space to propose a simple but effective defense strategy scheme for changing the vulnerable services' ports numbers used to accomplish the communications for V2V and V2I at different service slots. Facing uncertainty of DoS attacks and complex VANETs, a novel scheme manifested as defense strategy matrices is introduced to detect the port numbers probed by DoS attackers. Simulation results demonstrate that our scheme is superior to non-strategy ones, and is a simple but effective defense strategy scheme.

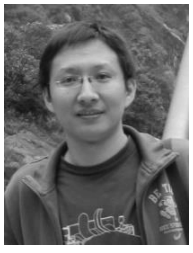
REFERENCES

[1] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.
[2] C. Guo *et al.*, "Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage," *Future Gener. Comput. Syst.*, vol. 84, pp. 190–199, Jul. 2018.
[3] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Inform.*, to be published, doi: 10.1109/TII.2018.2816590.
[4] B. Pooja, M. M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," in *Proc. 4th Asia–Pacific Conf. Comput. Aided Syst. Eng. (APCASE)*, Feb. 2014, pp. 152–157.
[5] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506–2517, Aug. 2018, doi: 10.1109/JIOT.2017.2764259.
[6] C. Guo, R. Zhuang, Y. Jie, K.-K. R. Choo, and X. Tang, "Secure range search over encrypted uncertain IoT outsourced data," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2845106.
[7] H. C. J. Lee and V. L. L. Thing, "Port hopping for resilient networks," in *Proc. IEEE 60th Veh. Technol. Conf. (VTC-Fall)*, vol. 5, Sep. 2004, pp. 3291–3295.
[8] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under denial of service in connected vehicles," in *Proc. Amer. Control Conf.*, May 2017, pp. 4971–4976.
[9] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, Jun. 2018.
[10] M. Asplund and S. Nadjm-Tehrani, "Attitudes and perceptions of IoT security in critical societal services," *IEEE Access*, vol. 4, pp. 2130–2138, 2016.
[11] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 71–79, Jun. 2018.
[12] B. Groza and P. Murvay, "Security solutions for the controller area network: Bringing authentication to in-vehicle networks," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 40–47, Mar. 2018.
[13] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, to be published, doi: 10.1109/MWC.2017.1700441.
[14] Y. Liu, L. Wang, and H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3697–3710, Aug. 2014.

[15] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K.-K. R. Choo, "Fine-grained database field search using attribute-based encryption for E-healthcare clouds," *J. Med. Syst.*, vol. 40, no. 11, p. 235:1-235:8, 2016.
[16] N. B. Gayathri, G. Thumbur, P. V. Reddy, and Z. U. R. Muhammad, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.
[17] X. Wang *et al.*, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, to be published.
[18] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 4, pp. 1065–1079, Apr. 2018.
[19] C. Guo, X. Chen, Y. Jie, F. Zhangjie, M. Li, and B. Feng, "Dynamic multi-phrase ranked search over encrypted data with symmetric searchable encryption," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2017.2768045.
[20] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, "Green and sustainable cloud of things: Enabling collaborative edge computing," *IEEE Commun. Mag.*, to be published, doi: 10.1109/MCOM.2018.1700895.
[21] P. S. Waraich and N. Batra, "Prevention of denial of service attack over vehicle ad hoc networks using quick response table," in *Proc. 4th IEEE Int. Conf. Signal Process., Comput. Control*, Sep. 2017, pp. 586–591.
[22] K. M. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, and A. Fernando, "Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model," in *Proc. IEEE Int. Conf. Consum. Electron.*, Jan. 2016, pp. 502–503.
[23] J. Soryal and T. Saadawi, "DoS attack detection in Internet-connected vehicles," in *Proc. Int. Conf. Connected Vehicles Expo*, Dec. 2013, pp. 7–13.
[24] L. Zhang, Y. Guo, H. Yuwen, and Y. Wang, "A port hopping based DoS mitigation scheme in SDN network," in *Proc. 12th Int. Conf. Comput. Intell. Secur.*, Dec. 2016, pp. 314–317.
[25] Y.-B. Luo, B.-S. Wang, X. Wang, B.-F. Zhang, and W. Hu, "RPAH: A moving target network defense mechanism naturally resists reconnaissances and attacks," *IEICE Trans. Inf. Syst.*, vol. E100-D, no. 3, pp. 496–510, 2017.
[26] Y.-B. Luo, B.-S. Wang, and G.-L. Cai, "Effectiveness of port hopping as a moving target defense," in *Proc. 7th Int. Conf. Secur. Technol.*, Dec. 2014, pp. 7–10.
[27] K. Wang, J. Guo, and F. Li, "Singular linear space and its applications," *Finite Fields Appl.*, vol. 17, no. 5, pp. 395–406, 2011.
[28] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Math.*, vol. 346, nos. 9–10, pp. 589–592, May 2008.
[29] J. A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2231–2242, Oct. 2004.
[30] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, "Explicit constructions of RIP matrices and related problems," *Duke Math. J.*, vol. 159, no. 1, pp. 145–185, 2011.
[31] Z. Wan, "Affine geometry over finite fields," in *Geometry of Classical Groups Over Finite Fields*, 2th ed. Beijing, China: Science, 2002, ch. 1, sec. 1, pp. 14–19.
[32] A. Brouwer, A. Cohen, and A. Neumaier, *Distance-Regular Graphs*. Berlin, Germany: Springer-Verlag, 1989.
[33] W. Hou, Z. Ning, L. Guo, and X. Zhang, "Temporal, functional and spatial big data computing framework for large-scale smart grid," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2017.2681113.
[34] L. Guo, Z. Ning, W. Hou, B. Hu, and P. Guo, "Quick answer for big data in sharing economy: Innovative computer architecture design facilitating optimal service-demand matching," *IEEE Trans. Automat. Sci. Eng.*, to be published, doi: 10.1109/TASE.2018.2838340.
[35] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," in *Proc. 10th USENIX Secur. Symp.*, 2010, pp. 1–14.
[36] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[37] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[38] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM J. Comput.*, vol. 24, no. 2, pp. 227–234, 1995.
[39] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.
[40] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.
[41] D. Needell and J. A. Tropp, "CoSaMP: Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.

YINGMO JIE received the B.S. degree in information and computing science from the Tianjin University of Technology and Education, in 2011, and the M.S. degree in applied mathematics from the Civil Aviation University of China, Tianjin, China, in 2015. She is currently pursuing the Ph.D. degree with the School of Mathematical Sciences, Dalian University of Technology. Her current research interests include information security, resources optimization, and game theory.

MINGCHU LI received the B.S. degree in mathematics from Jiangxi Normal University, in 1983, the M.S. degree in applied science from the University of Science and Technology Beijing, in 1989, and the Ph.D. degree in mathematics from the University of Toronto, in 1997. He was an Associate Professor with the University of Science and Technology Beijing from 1989 to 1994. He was engaged in research and development on information security with Longview Solution, Inc, Compuware, Inc., from 1997 to 2002. In 2002, he was with the School of Software, Tianjin University, as a Full Professor. Since 2004, he has been with the School of Software Technology, Dalian University of Technology, as a Full Professor. His main research interests include theoretical computer science and cryptography.



CHENG GUO received the B.S. degree in computer science from the Xi'an University of Architecture and Technology, in 2002, and the M.S. and Ph.D. degrees in computer application and technology from the Dalian University of Technology, Dalian, China, in 2006 and 2009, respectively. From 2010 to 2012, he held a post-doctoral position with the Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan. Since 2013, he has been an Associate Professor with the School of Software Technology, Dalian University of Technology. His current research interests include information security, cryptology, and cloud security.

LING CHEN received the B.S. degree from the School of Mathematics Statistics, Shandong University, Shandong, China, in 2016. She is currently pursuing the Ph.D. degree with the School of Mathematical Sciences, Dalian University of Technology. Her current research interests include game theory and security game.