IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURE COMMUNICATION FOR THE NEXT GENERATION 5G AND IOT NETWORKS

Received November 6, 2019, accepted November 27, 2019, date of publication December 4, 2019,
date of current version December 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2957565

An Authentication Scheme to Defend Against UDP DrDoS Attacks in 5G Networks

HAIOU HUANG[1,2], LIANG HU[1], JIANFENG CHU[1], AND XIAOCHUN CHENG[3], (Senior Member, IEEE)

[1]College of Computer Science and Technology, Jilin University, Changchun, China
[2]College of Electronic and Information Engineering, Jilin Agricultural Science and Technology University, Jilin, China
[3]Department of Computer Communications, Middlesex University, London NW4 4BT, U.K.

Corresponding authors: Jianfeng Chu (chujf@jlu.edu.cn) and Xiaochun Cheng (x.cheng@mdx.ac.uk)

This work was supported in part by the National Key Research and Development Plan of China under Grant 2017YFA0604500, and in part by the National Sci-Tech Support Plan of China under Grant 2014BAH02F00.

ABSTRACT 5th generation wireless systems are coming. While we are excited about the delay-free high speeds 5G will bring, security problems are becoming more and more serious. Increasingly rampant Distributed Denial of service (DDoS) attacks, particularly Distributed Reflection Denial of Service (DrDoS) attacks with User Datagram Protocols (UDPs) have developed into a global problem. This article presents a design, implementation, analysis, and experimental evaluation of an authentication scheme, a defense against UDP DrDoS attacks, by which attackers cleverly use rebound server farms to bounce a flood of packets to a target host. We call our solution IEWA because it combines the concepts of increasing expenses and weak authentication. In this paper, we apply IEWA to Network Time Protocol (NTP). First, we simulate and compare the original and improved protocols. Next, we verify the effectiveness of our proposed scheme. We show that our improved scheme is safer than the original scheme. Finally, we compare our solution with existing state-of-the-art schemes, using indicators such as communication overhead, server storage costs, client storage costs, computation costs of server and computation costs of client. We find that our scheme improves system stability and security, reduces communication overhead, server storage cost and computational costs. Our solution not only improves the NTP protocol to mitigate DrDoS attacks, but also strengthens other UDP protocols that are vulnerable to DrDoS attacks. Therefore, our solution can be used as a solution to UDP DrDoS attacks in 5G Networks.

INDEX TERMS Authentication, distributed reflection denial of service (DrDoS), network time protocol (NTP), user datagram protocol (UDP), 5G.

I. INTRODUCTION

Along with the increasingly prosperous development of the Internet of things (IoT) [1], [2], intelligent services and mobile services [3]–[5], the 5th generation wireless systems (in short 5G) is coming gradually [6], [7]. Today, IoT and 5G are two of the biggest hypes in telecom [8], 5G brings us higher speeds and lower latency [9], [10], but it also brings us a cadre of security issues.

Several telecon insiders report that ''Security is a top concern for 5G operators, almost equal to increasing capacity and throughput,'' and ''Opportunities and Challenges await a 5G Connected Economy.'' Many industry leaders report that 94% of respondents expect the growth of 5G to increase security and reliability concerns for 5G mobile operators [11].

Distributed Denial-of-Service (DDoS) [12] is considered one of the most serious threats since it prevents the user from gaining access to network services [13], [14]. The rollout of 5G will almost certainly expand the trend of significant increases in the largest attacks increasing significantly in size, every year, to the point where we can surely expect the first 10 terabits per second attacks sometime soon [15]. Even more frightening, the new advanced 5G network can be paralyzed by someone renting DDoS-for-hire service for tens of dollars, which exploit the power of botnets that they are unwittingly providing the connectivity for [15]!

DDoS attacks have increased rapidly in both quantity and severity within the last few years. Furthermore, there are

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

TABLE 1. DDoS Attack Statistics, First Quarter Of 2018 [17].

Types of DDoS Attacks	Percent of all DDoS attacks
IP Fragment Attacks	6%
TCP Based	26%
UDP Based	50%
Layer 7	6%
Other	12%

four alarming Trends according to the Full Year 2018 DDoS Trends Report [16]:

1) REPEAT ATTACKS

DDoS victims have a 1 in 5 chance (22%) of being attacked again within 24 hours. There is a significant probability that victims will suffer a repeat attack, causing more service outages.

2) LOW-VOLUME ATTACKS DOMINATE

98% of Corero-mitigated DDoS attacks were less than 10Gbps. Low-volume attacks often go undetected and unmitigated by manual/legacy DDoS solutions.

3) MAJOR ATTACKS DOUBLED

100% Increase in DDoS attacks over 10Gbps.

The percentage of attacks over 10Gbps doubled in 2018 compared to 2017.

4) DAILY ATTACKS INCREASING

The average number of attacks per customer in 2018 increased 16% over 2017.

5) SHORT DURATION ATTACKS CONTINUE

Short duration attacks, which often go unmitigated by traditional DDoS solutions, are increasingly common. 81% in 2018 lasted less than 10 minutes, up from 71% in 2017.

A review of DDoS Amplification sources during 2018 reveals that the availability of vulnerable UDP servers continues to be a worldwide problem. From [16] we can see that different geographical locations host a variety of amplifiers that can be harnessed by DDoS attackers from anywhere in the world. These include open DNS resolver, monlist NTP server, Windows CLDAP server, SSDP/uPnP server, and more.

Additionally, [17] points out that 50% of new DDoS attacks use User Datagram Protocol (UDP) flood attacks (TABLE 1).

The concern is that with 5G, a new advanced network, such attacks will be faster and more damaging.

So why are the Distributed Reflection Denial of Service (DrDoS) attacks through UDP favored by attackers? By design, a UDP is a connectionless protocol that does not validate source Internet Protocol (IP) addresses [18], [19]. Unless the application-layer protocol contains countermeasures, such as session initiation in the Voice over Internet Protocol, an attacker can easily forge the IP packet datagram (a basic transfer unit associated with a packet-switched network) to include an arbitrary source IP address. While many UDP packets impersonate its victim's IP address, the destination server (or amplifier) responds to the victim instead of the attacker – this creates a reflected denial-of-service (DoS) attack [20]. Certain application-layer protocols that rely on UDPs (e.g., DNS, NTP, SSDP) have been identified as potential attack vectors. In [21], we can refer all the UDP protocols prone to Distributed Reflection Denial-of-Service (DrDoS) attacks and associated BAFS(Bandwidth Amplification Factors).

TABLE 2. UDP protocols prone To DrDoS attacks and associated BAFs [21].

Protocol	Bandwidth Amplification Factor
NTP	556.9
DNS	28 to 54
SSDP	30.8
SNMPv2	6.3
NetBIOS	3.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS(mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP[22]	56 to 70

The BAF of the Network Time Protocol (NTP) DDoS can reach up to 556.9 (as seen in TABLE 2). A significant DDoS NTP reflection attack occurred on February 11, 2014. This attack was reported to hit a record-breaking 400 Gbit/s (33% larger than the previous year's attack against Spamhaus). This incident was one of the five most notable DDoS attacks in history [23].

This paper uses the NTP DDoS as an example to explore the defense against UDP DDoS attacks. Our contributions can be summarized as follows.

1) The overall state of DDoS susceptibility is characterized by analyzing nearly two years of DDoS attack reports.

2) Extant countermeasures to DDoS attacks are assessed and shortcomings within them are defined.

3) A defense against DrDoS is proposed and its security is verified.

4) A detailed comparison between the proposed scheme and similar existing schemes is provided.

The rest of this paper is organized as follows. Section II provides background information about NTP protocols and NTP DDoS Attacks. Section III introduces existing DDoS attack countermeasures, four strategies from principle: packet filtering, source-side control, source-side tracing, and router dynamic monitoring and control. Section III also considers four schemes to strengthen UDP protocols: Stateless Connections, Cookie, Falling-together, and client Puzzle. Section IV proposes an authentication scheme to defend against UDP DrDoS, reports and its implementation in the laboratory. The security of the proposed scheme is analyzed by using the stochastic model of semi-markov process. Section V provides a further comparison between the proposed countermeasure

and the four countermeasures introduced in Section III. The evaluation parameters include communication overhead, server computation costs, client computation costs, server storage costs, and client storage costs. Section VI contains a brief summary and conclusion.

II. MOTIVATIONS

The NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. The NTP uses the UDP 123 port for communication and is the most common way that GNU/Linux software clocks are synchronized with the Internet time server [24]. It is designed to mitigate the effects of variable network latency, which can typically be kept within tens of milliseconds on the public Internet. LAN accuracy is even higher, at up to 1 ms 0 [25].

A. DrDoS ATTACKS

In 2012, there was a significant increase in the use of a specific DDoS methodology known as Distributed Reflection Denial-of-Service (DrDoS). DrDoS techniques usually involve multiple victim host machines that unwittingly participate in a DDoS attack on the attacker's primary target. Requests to the victim host machines are redirected (or reflected) from the victim hosts to the target [26]. DrDoS attacks have been a persistent and effective type of DDoS attack for more than 10 years. The technique shows no signs of subsiding; it continues to grow in effectiveness and popularity among attackers.

Reflective DDoS attacks are favored by attackers for two main reasons: first, attacks can be carried out by forging addresses to hide the source of attacks, and second, most reflection attacks carry amplification effects, which can magnify attack traffic by tens or even hundreds of times. For example, the average amplification factor of NTP DrDoS attacks is 556.9 [21]. Protocols associated with reflective attacks currently include NTP, Chargen, SSDP, DNS, RPC portmap, and others.

DrDoS attacks are a type of DDoS attack. And the attacks through UDP discussed in this article refer to DrDoS attacks.

B. A NTP DrDoS ATTACK

UDP-based NTP protocol can be abused to amplify DoS attack traffic. The attacker uses spoofing source IP addresses to generate a large number of UDP packets to the NTP server's port 123, saturating the target of the NTP reply. Some NTP installations also support the MONLIST command, which is mainly used to monitor the NTP server. When an NTP server responds to the MONLIST, it returns the IP of the last 600 clients that have been synchronized with the NTP server. The response packet is divided into 6 IP-groups that contain a maximum of 100 response packets. In other words: only a small request packet needs to be sent to trigger a large number of continuous UDP response packets containing IP address information [27]. Consider a malicious teenager calling a restaurant and saying, ''I'll have one of everything on the menu – please call me back and read back my whole order.'' When the restaurant asks for a callback number, the prankster gives a target victim's phone number. The target then receives a call from the restaurant with a lot of cumbersome, time-consuming information that they did not request.

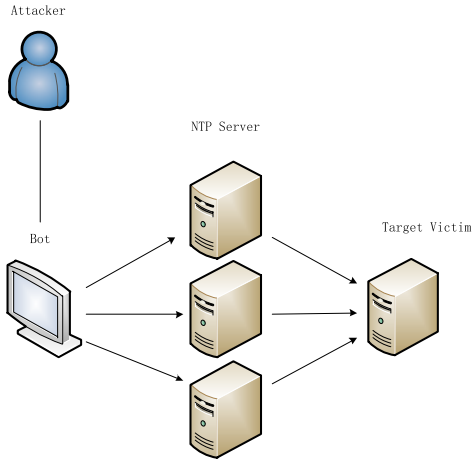

FIGURE 1. NTP amplification attack (DDoS attack) diagram.

An NTP amplification attack can be broken down into four steps:

1) The attacker uses a botnet to send UDP packets with spoofed IP addresses to an NTP server, which has an enabled MONLIST command. The spoofed IP address for each packet points to the victim's real IP address.

2) Each UDP packet makes a request to the NTP server using its MONLIST command, resulting in a large response.

3) The server then spoofs the address with the resulting data response.

4) The target IP address receives the response and the surrounding network infrastructure is overwhelmed by a large amount of traffic, resulting in denial of service.

The NTP amplification attack process is shown schematically in FIGURE 1.

The abuse of the MONLIST request is not new, but has become particularly trendy in recent years.

III. RELATED WORK

There are many existing countermeasures against DDoS attacks. In principle, there are four ways to deal with DoS attacks: packet filtering, source-side control, source-side traceability, and router dynamic monitoring and control.

Packet filtering [28] works by filtering, or discarding, specific traffic to avoid attacks. The packet filtering scheme needs the network administrator of each ISP to cooperate artificially. Thus, the work intensity is large and time-consuming to implement, making the scheme altogether difficult to carry out. Certain forms of source-side filtering can reduce or eliminate fake IP addresses. This may help to prevent DoS attacks, and indeed, more and more routers now support source-side filtering. However, source-side filtering does not completely eliminate IP address impersonation. There are many ways

to trace the source side of an attack. For example, extant methods assume that there is a source of the address spoofing (i.e., an attempt to suppress the attack at its source while identifying said malicious source). Unfortunately, during the actual tracing process, the harm caused by the attack cannot be controlled in real time; furthermore, the attack cannot be effectively traced when the source is scattered.

The main assumption of router dynamic monitoring and control is that we can identify the flow aggregation through the router by analyzing the packet loss history. If a router recognizes high-bandwidth stream aggregates, it can ask the upstream router sending the aggregates to limit its delivery rate. However, whether this mechanism can be realized in an actual network is uncertain due to issues such as monitoring standards, fairness mechanisms, and efficient implementation or overall operation management problems.

The very high frequency, and increasingly high severity of UDP DDoS attacks, suggest that defects in the UDP protocol remain problematic. To resolve DDoS attacks at the root, it is critically important to strengthen the UDP protocol. Current methods taking this approach include stateless connection, increasing expense, and weak authentication.

Stateless Connections methods can be used to solve DoS problems by reducing the memory resource load of the responder [29]. After receiving an initial request from the initiator, the responder executes the protocol without saving the status information related to the protocol; this is accomplished by sending status information to the initiator as part of the response information. Then, the initiator returns the status to the responder in the next message [30], [31]. Although this method does not deplete memory resources, computational resources are still affected. If confidentiality and integrity of the state are required, the consumption of computational resources will rapidly increase. Additionally, an attacker can replay Msg3 to launch a replay attack.

The Falling-together method was established by Matsuura and Imai [32]. It works by minimizing the number of calculations required by the responder. In this way, the number of calculations required by the initiator is greater than or equal to that of the responder when both parties have comparable computing power [33]. When an attacker attempts a DoS attack on a responder, the attacker may first run out of its own computing resources before the responder runs out of computing resources [34], [35]. The Falling-together approach ensures the initiator and responder have a comparable computation level, while the responder is stateless. This method can only prevent a single-attacker DoS attack – it is rendered ineffective by a DDoS or DrDoS.

Dwork and Naor developed the Proof of the Work concept [36], while Jules and Brainard proposed the Client Puzzle method currently utilized by Aura [37]. In these methods, when a request is received and agreed upon, the responder does not save any state but rather asks a sponsor a password problem, then waits for the sponsor to solve the problem to continue the agreement [38]–[40]. The Client Puzzle method is highly vulnerable to replay attacks. Additionally, setting up sufficiently challenging password problems to ensure the method's efficacy can be difficult.

The basic working principle of the Cookie method is a stateless weak authentication mechanism [41]. The initiator initiates a request and receives a cookie (returned by the responder) that may only be made or verified by the responder. The initiator connects to the responder again and provides the cookie, then the responder verifies whether the cookie is correct. If the test is passed, the responder initially believes that the initiator is not an attacker and begins to provide resources for the operation of subsequent parts of the agreement [42]. However, if an attacker uses a real IP address to obtain the cookie, he can use the real IP address to launch an attack.

As far as we know, our study is the only quantitative and empirical study on UDP DDoS attacks thus far.

IV. IEWA SCHEME AND ANALYSIS

An IEWA scheme is a scheme that combines increasing expense and weak authentication. In this part, the implementation process and rules of the IEWA scheme are introduced in detail at first. Then, the correctness of the scheme is verified in the laboratory (according to the comparison of experimental results without and with IEWA). Finally, the security of the method is verified.

A. IEWA SCHEME

The IEWA scheme:

Step 1: (Initialization) Assume that no client has sent a request to the server. The server defines all variables, including the IP address of $client_i$ CIP_i. The two hashes obtained by md5 algorithm are H_{i1} and H_{i2}. A random number SN_j is generated every 12 hours. $Client_i$ defines a variable H'_{i2} that stores a verification code.

Step 2: The server initializes SN_j.

Step 3: $client_i$ makes a request to the server.

Step 4: The server computes the value of

$$H_{i1}(SN_j||CIP_i) \tag{1}$$

and sends

$$SN_j||H_{i1}(SN_j||CIP_i) \tag{2}$$

to $client_i$.

Step 5: $client_i$ computes

$$H'_{i2}(SN_j||H_{i1}) \tag{3}$$

and sends it (along with $Request_{i1}$) to the server.

Step 6: The server computes the value of

$$H_{i2}(SN_j||H_{i1}) \tag{4}$$

and determines whether H'_{i2} and H_{i2} are equivalent. If H'_{i2} equals H_{i2}, then the server satisfies the $client_i$'s request, otherwise, we go to Step 2.

A flow diagram depicting the IEWA algorithm flow when the client sends the first request to the server within 12 hours is shown in FIGURE 2.

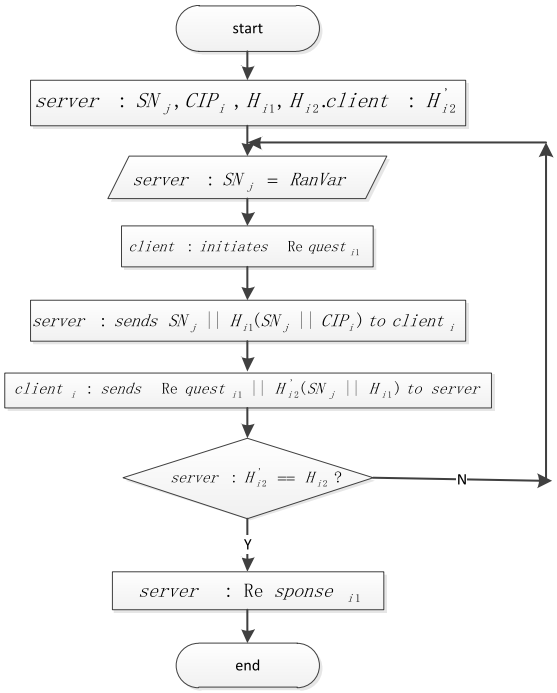

FIGURE 2. Algorithm flow of IEWA (when client i sends the first request to the server within 12 hours).

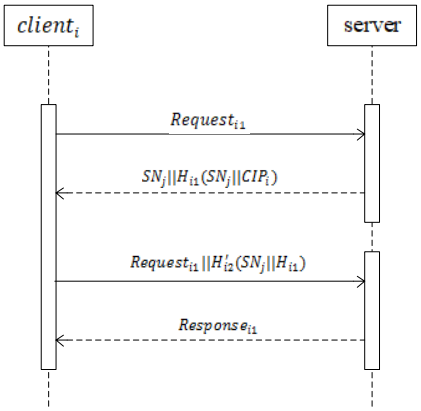

FIGURE 3. Initial connection establishment in IEWA.

FIGURE 3 shows the first time a client sends a request to and successfully establishes a connection with the server. After that, if $client_i$ has a request and as long as the value of c [i] is not greater than N, $client_i$ simply sends H_{i2} (and the request) to the server without introducing additional communication time.

B. IEWA SCHEME IMPLEMENTATION

We applied the IEWA scheme to the NTP protocol in our laboratory to verify its security.

1) EXPERIMENTAL SETTINGS

When setting up the experimental environment, we used a virtual machine as the NTP server: Windows 7 (64-bit) (Windows 7 virtual machine under VMware 12 pro). The script file was run under Ubuntu-12.04.5.

Time	Source	Destination	Protocol
5.833159	172.16.93.122	172.16.93.123	NTP
5.834589	172.16.93.123	172.16.93.122	NTP
7.892640	172.16.93.123	172.16.93.122	NTP
9.960139	172.16.93.123	172.16.93.122	NTP
12.024335	172.16.93.123	172.16.93.122	NTP
14.095085	172.16.93.123	172.16.93.122	NTP
16.173122	172.16.93.123	172.16.93.122	NTP
18.242261	172.16.93.123	172.16.93.122	NTP
20.272215	172.16.93.123	172.16.93.122	NTP
22.343957	172.16.93.123	172.16.93.122	NTP
24.407171	172.16.93.123	172.16.93.122	NTP
26.450337	172.16.93.123	172.16.93.122	NTP
28.509464	172.16.93.123	172.16.93.122	NTP
30.578328	172.16.93.123	172.16.93.122	NTP
32.647256	172.16.93.123	172.16.93.122	NTP
34.698450	172.16.93.123	172.16.93.122	NTP
36.756385	172.16.93.123	172.16.93.122	NTP
38.814248	172.16.93.123	172.16.93.122	NTP
40.894952	172.16.93.123	172.16.93.122	NTP
42.953512	172.16.93.123	172.16.93.122	NTP
45.024193	172.16.93.123	172.16.93.122	NTP
47.096762	172.16.93.123	172.16.93.122	NTP
49.168622	172.16.93.123	172.16.93.122	NTP

FIGURE 4. One request from 172.16.93.122 responded to 172.16.93.123 by 22 (without IEWA).

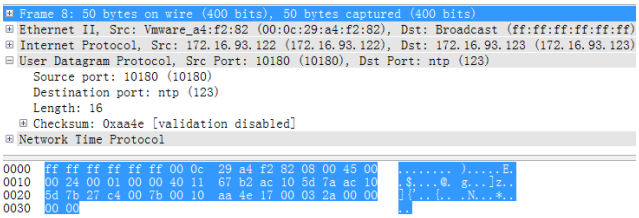

FIGURE 5. A request in which 172.16.93.122 sends to 172.16.93.123 (without IEWA).

2) RESULTS AND ANALYSIS

First, we simulated a NTP DrDoS attack in our laboratory. The experimental results are shown in FIGURE 4-6. In FIGURE 4, client 172.16.93.122 initiated a request to NTP server 172.16.93.123. Next, the server responded to the client with 100 packets. We calculated the specific amplification factor as follows: the client initiates a request using 50 bytes (as shown in FIGURE 5) but 64 bytes are transmitted [43]. The server responds to the data packets with 410 bytes (as shown in FIGURE 6) per packet and 100 data packets, sending out a total of 41000 bytes; thus, the amplification factor is 410 * 100/64 = 641. In fact, the amount of data returned by a MONLIST request is related to the number of clients interacting with the NTP server over time. If the NTP server interacts with a large number of clients, the attack traffic amplification factor increases.

We ran an experimental verification of the IEWA scheme according to the algorithm flow detailed in A of Section IV. In the first iteration, we did not limit the quantity of client requests (see FIGURE 7). We found that, although client 172.16.93.122 did not pass the verification, server 172.16.93.122 did not respond. This suggested that there was no DrDoS attack; but, in reality, as the client initiated the request, the server was too busy to consider the reasonable request to be normal and a DoS attack did occur.

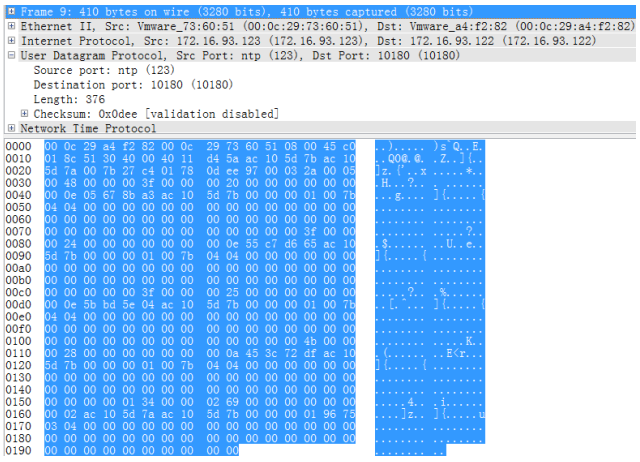

FIGURE 6. A response in which 172.16.93.123 replies to 172.16.93.122 (without IEWA).

Time	Source	Destination	Protocol
0.000000	172.16.93.122	172.16.93.123	NTP
0.002197	172.16.93.122	172.16.93.123	NTP
0.004415	172.16.93.122	172.16.93.123	NTP
0.006563	172.16.93.122	172.16.93.123	NTP
0.009804	172.16.93.122	172.16.93.123	NTP
0.012172	172.16.93.122	172.16.93.123	NTP
0.014429	172.16.93.122	172.16.93.123	NTP
0.017128	172.16.93.122	172.16.93.123	NTP
0.019457	172.16.93.122	172.16.93.123	NTP
0.028711	172.16.93.122	172.16.93.123	NTP
0.031606	172.16.93.122	172.16.93.123	NTP
0.033900	172.16.93.122	172.16.93.123	NTP
0.036038	172.16.93.122	172.16.93.123	NTP
0.038918	172.16.93.122	172.16.93.123	NTP
0.041528	172.16.93.122	172.16.93.123	NTP
0.044198	172.16.93.122	172.16.93.123	NTP
0.046358	172.16.93.122	172.16.93.123	NTP
0.048729	172.16.93.122	172.16.93.123	NTP
0.050878	172.16.93.122	172.16.93.123	NTP
0.053243	172.16.93.122	172.16.93.123	NTP
0.055500	172.16.93.122	172.16.93.123	NTP
0.057942	172.16.93.122	172.16.93.123	NTP
0.060250	172.16.93.122	172.16.93.123	NTP
0.062539	172.16.93.122	172.16.93.123	NTP
0.064963	172.16.93.122	172.16.93.123	NTP

FIGURE 7. Unlimited quantity of requests from 172.16.93.122 to 172.16.93.123 (with IEWA).

Conversely, when we limited the number of client requests to N = 10 in a minute (see FIGURE 8), although the client made continuous service requests to the server, it did not constitute a DoS attack. The IEWA scheme in this case successfully resisted both the DrDoS attack and DoS attack.

C. SECURITY PROOF

Reference [44] indicated that the safety evaluation index is not absolute. For different network systems, people are interested in different evaluation indicators; therefore, attributes in some specific systems do not need to be involved. For DDoS attacks discussed in this article, we did not find it necessary to analyze the confidentiality and integrity of the system. In contrast, people are more concerned about the steady-state

Time	Source	Destination	Protocol
0.000000	172.16.93.122	172.16.93.123	NTP
0.002207	172.16.93.122	172.16.93.123	NTP
0.005139	172.16.93.122	172.16.93.123	NTP
0.007325	172.16.93.122	172.16.93.123	NTP
0.009656	172.16.93.122	172.16.93.123	NTP
0.011922	172.16.93.122	172.16.93.123	NTP
0.014171	172.16.93.122	172.16.93.123	NTP
0.017235	172.16.93.122	172.16.93.123	NTP
0.019397	172.16.93.122	172.16.93.123	NTP
0.021588	172.16.93.122	172.16.93.123	NTP

FIGURE 8. Requests from 172.16.93.122 to 172.16.93.123 while Number of requests limited to 10 in a minute (with IEWA).

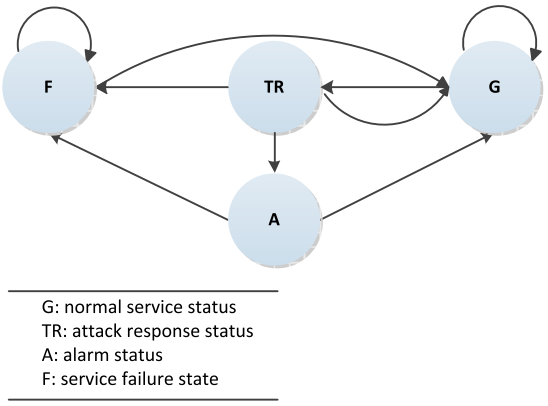

FIGURE 9. Network system state under DDoS attack.

availability of the system. Therefore, the security analysis in this paper mainly analyzes the steady-state availability after using the IEWA protocol.

A stochastic model based on state can analyze a network system under attack given the transfer relationship between the distributed states, the original states, and applications based on the original states. In the Angle of attack method, the network attack model ignores unknown details that do not affect the safety evaluation index. In addition, unknown attacks can be described and recognized from the perspective of the attack influence [44].

As described in [45] and [46], the process of the network system under attack (by DDoS) is characterized by four states {G,A,TR,F} (see FIGURE 9). If the TR state is entered, the server may recover, fail, or enter an alert state. In the alert state, the user can either manually restore the server or the server fails. A chance of recovery remains after a server failure, but the server is far less alert and is not in a state where it can counteract or respond to an attack.

The security quantitative analysis method is based on Semi-Markov Process (SMP). SMP is adopted to analyze the security of our IEWA. Model parameters include the transition probability matrix $P_{ij}\,(i, j \in \{G, A, TR, F\})$ between states and the average residence time $\mathrm{h} = (h_G, h_A, h_{TR}, h_F)$ of states. The discrete-time Markov chain (DTMC) [47] corresponding to FIGURE 9 is shown in FIGURE 10. First, the probability distribution of the stable state, of the discrete-time Markov chain $\mathrm{v} = (v_G, v_A, v_{TR}, v_F)$, is calculated. Then, the steady state probability of the Semi-Markov Process

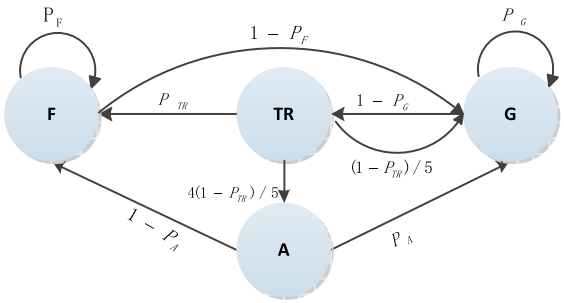

FIGURE 10. DTMC process under DDoS attack.

model can be expressed as:

$$\pi_i = \frac{v_i h_i}{\sum_j v_j h_j}, \quad i, j \in \{G, A, TR, F\} \tag{5}$$

The steady-state availability of the system is defined as:

$$A_s = 1 - \pi_F \tag{6}$$

According to FIGURE 10, the state transition formula of DTMC in DDoS attack

$$v_G = p_G v_G + p_A v_A + \frac{1}{5}(1 - p_{TR})\, v_{TR} + (1 - p_F)\, v_F \tag{7}$$

$$v_{TR} = (1 - p_G) v_G \tag{8}$$

$$v_A = \frac{4}{5}(1 - p_{TR}) v_{TR} \tag{9}$$

$$v_F = p_{TR} v_{TR} + p_F v_F + (1 - p_A) v_A \tag{10}$$

The following is the numerical analysis of the security indicators for the original NTP protocol, the improved IEWA protocol and of the initialization of the model parameter values.

The state transition probability P: p_G is defined when the model is at a normal service state G or the attack failure model remains in server state. The parameter p_A is the probability of successful alarm, p_{TR} is the probability of responding to an attack, and p_F is the probability of a successful attack. Before NTP protocol improvement, we set $p_G = 0.9, p_A = 0.1, p_{TR} = 0.12, p_F = 0.2$. After improving the protocol, there is an authentication stage in the IEWA protocol. At this stage, the attack difficulty is upgraded, so $p_F = 0.001$ after improving the protocol.

The average residence time h_i: is determined by the random time that state i completes the corresponding interaction process (according to the protocol). In the SMP model of this paper, the residence time of the four states satisfies the exponential distribution and each time unit is 1. Before implementing the improvement of the NTP protocol, $h_G = h_F = h_A = 0.5$. Since the attack response state time will be long, $h_{TR} = 1$.

After the protocol is improved, the average residence time of the authentication phase is increased, so set $h_G = 1$.

With IEWA, the attacker can't implement a DrDoS attack, the attack may be downgraded to a DoS attack. While, the DoS attack needs to be implemented before the other attack to defraud the server authentication, e.g., Man-in-the-middle attack. However, to carry out a man-in-the-middle attack, ARP spoofing is often necessary. Thus, to implement this attack, the difficulty of the DoS attack must increase greatly, which also consumes a lot of time. Therefore, the attack response time is greatly extended. The h_{TR} parameter adds verification time, ARP spoofing time, and man-in-the-middle attack time to the original protocol. Therefore, we set $h_{TR} = 4$.

According to the parameters and eqs. (5-10) described in this section:

The original protocol:

$$v_G = 0.79, \quad v_A = 0.056, \; v_{TR} = 0.084, \; v_F = 0.074,$$
$$\pi_F = 0.07, \quad A_s = 0.93$$

Protocol with IEWA:

$$v_G = 0.55, \quad v_A = 0.039, \; v_{TR} = 0.055, \; v_F = 0.041,$$
$$\pi_F = 0.02, \quad A_s = 0.98$$

After the protocol is improved, the steady-state availability of the system increases from 0.93 to 0.98, indicating that the IEWA scheme proposed in this paper has a higher steady-state availability than the original NTP protocol under analysis (via the random model based on the semi-Markov process).

V. COMPARISON AND ANALYSIS

We simulated NTP (adds IEWA before and after) DrDoS attacks in our laboratory and verified the effectiveness of the proposed IEWA scheme in section IV. Then, we compared the four countermeasures mentioned in the Related Work section with IEWA scheme in terms of communication overhead, server computation costs, client computation costs, server storage costs, and client storage costs. In TABLE 3-(a) and TABLE 3-(b), Co, *Scc*, *Ccc*, *Ssc*, *Csc* stand for communication overhead, server computation costs, client computation costs, server storage costs, and client storage costs, respectively.

A. COMPARISON

Original protocols have 2N communication overhead when the client initiates N requests. The co-rows of TABLE 3-(a) and TABLE 3-(b) show that, when compared to the original protocol, if the client makes N requests, the IEWA scheme adds two session times. Alternatively, the other four schemes all add 2N requests. In this regard, IEWA scheme outperforms the others.

Row Ccc shows the Computation cost to the client. Next, we verify if the server and the client have communicated N times. In an IEWA scheme request, the client needs a hash function to begin calculations. The Stateless Connections and Failing-together methods require several computation iterations (N-times Encryption, N-times Decryption and N-times Encryption, N-times Decryption, N times Hash, respectively). The Client Puzzle method needs an N-times PHC puzzle solution, while the cookies method does not

TABLE 3. (a) Communication overhead of N client requests to Server. (b) Communication overhead of N client requests to Server.

(a)

Index	Stateless Connections[30],[31]	Cookie[41],[42]	Client Puzzle[37],[38]
Co	2n	2n	2n
Scc	^{N}MAC(or HMAC), ^{2N}Encryption, ^{N}Decryption	^{N}HMAC	^{N}Hash
Ccc	^{N}Encryption, ^{N}Decryption	None	^{N}PHC puzzle solution
Ssc	$K_a, K_b^{-1}, K_{ba}, K_{be}, K_{bm}$	secret, K_{HMAC}	N_s,b
Csc	K_b,K_a^{-1},K_{be}	HMAC, context, IP-I	None

(b)

Index	Falling-together[32]	IEWA scheme
Co	2n	2
Scc	^{2N}Encryption,^{N}Hash	^{2N}Hash
Ccc	^{N}Encryption, ^{N}Decryption, ^{N}Hash	^{1}Hash
Ssc	K_{ba}, K_a, K_{be}	SN_j
Csc	$K_{ab}, K_b, K_a^{-1}, K_{be}$	H'_{i2}

Note: in TABLE III-I and III-II, *Co* , *Scc* , *Ccc* , *Ssc* , *Csc* stand for communication overhead, server computation costs, client computation costs, server storage costs, and client storage costs, respectively.

require any computation from the client. The key point of a DoS attack is to consume a huge amount of the target's computational resources with low cost [48]. So increasing the cost of launching a DrDoS attack properly may reduce the likelihood of launching an attack. So the IEWA scheme is a more appropriate choice in this respect.

The key to server storage cost-efficiency in the Cookie method is maintaining at least 64 bits of encryption strength [49], but the secret length of a Cookie is uncertain. Therefore, the server storage costs of the Cookie method is: 64 + an uncertain length (unknown). Ns is 64-bits + length(b), but the length of b is uncertain, so the server storage costs of the Client Puzzle method is 64 + length(b). If b is more than 8 bits, the PHC problem is unanswerable. The Falling-together and Stateless Connection methods both use the Diffie-Hellman algorithm. Thus, the default secret key length is 1024. Therefore, the server storage costs of the Falling-together and Stateless Connection method are, respectively, 1024 * 3 = 3072bits and 1024 * 5 = 5120 bits. The server storage costs of IEWA are Length $(SN_j) = 64$ bits. Thus, IEWA outperforms the other methods.

The client storage costs of IEWA are 128 bits. The Stateless Connections are 3072 bits. The Cookie are 288 bits (context is minimum at 128 bits and Cookie uses the MD5 algorithm). The Falling-together method has 4094 bits. The Client Puzzle method has none. Therefore, the storage requirements of the client are moderate for IEWA scheme.

B. ANALYSIS

First, we find that the steady-state availability of the system has been improved by 5 percent. This is based on analysis of the Security Proof.

Second, as shown in FIGURE 3, communication overhead with the IEWA assumes that the client requests to the server only occur one N at a time. Only at the first request, two communications are added, including the server sending the random number, the hash function value of the random number and the client IP to the client and the client sending the request and verification code to the server. For other N-1 requests, the client just attaches the verification code to the request to initiate requests without an increase in communication time (That is to say two communications are added when the client issues N requests to the server). Therefore, the increased communication overhead does not break the lightweight nature of the UDP protocol.

As we have shown, the computational cost of the client and the server includes the calculation of the hash function, which is only added to the client once and to the server twice (this is based on the client's original protocol). Additionally, from the storage cost analysis of the client and server, compared to the original protocol, the server and the client have increased 64 bits and 128 bits respectively. For a vulnerable protocol like NTP, too much or too little computation and storage on the client side is not good, because too much computational and storage cost reduces the availability of NTP, while too little reduces the cost of launching a DrDoS attack. So our scheme does not affect the availability of an NTP protocol, but increases the cost of launching a DrDoS attack.

Based on the analysis in this section, the availability of NTP is not affected by IEWA. Similarly, as with IEWA, the other UDP protocols are not vulnerable to DrDoS attacks.

VI. CONCLUSION

5G not only brings high speed and low latency online experience to everyday network users, but also provides a faster and more convenient attack channel for UDP DrDoS attacks. That is to say, in a 5G network, UDP-based DrDoS will become more and more dangerous. In the face of 5G, the abuse of UDP for amplification Denial of Attack is a threat that needs to be mitigated urgently.

UDP flooding can be deployed for DrDoS attack has advantages in terms security by which a large number of UDP packets are sent to a target server in order to overwhelm the device's processing capability and responsiveness. The UDP protocols are vulnerable to DrDoS attacks because spoofing a UDP packet is easier than spoofing a TCP packet [50]. A UDP does not establish an initial connection (also known as a handshake) because there is no virtual connection between the two communicating systems. Thus, the services associated with UDP are under serious threats of attacks. Therefore, all UDP protocols listed in TABLE 2 are vulnerable to DrDoS attacks for similar reasons.

In this study, we design IEWA scheme for NTP. We analyzed and compared five defense countermeasures in terms of

security, communication overhead, server computation costs, client computation costs, server storage costs, and client storage costs. The proposed IEWA scheme has advantages in terms of security, communication load, server storage costs, and client computation costs. The method also performs well on all the metrics we tested. Security, communication and computation overheads are important aspects of network communication. Thus, IEWA is a feasible countermeasure to NTP DrDoS attacks. With IEWA, we can strengthen other UDP protocols that are prone to DrDoS attacks.

REFERENCES

[1] F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Social behaviometrics for personalized devices in the Internet of Things era," *IEEE Access*, vol. 5, pp. 12199–12213, 2017.

[2] L. Li, G. Xu, L. Jiao, X. Li, H. Wang, J. Hu, H. Xian, W. Lian, and H. Gao, "A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems," *IEEE Trans. Ind. Informat.*, to be published.

[3] Y. Yin, L. Chen, Y. Xu, J. Wan, H. Zhang, and Z. Mai, "QoS prediction for service recommendation with deep feature learning in edge computing environment," *Mobile Netw. Appl.*, pp. 1–11, Apr. 2019.

[4] H. Gao, W. Huang, Y. Duan, X. Yang, and Q. Zou, "Research on cost-driven services composition in an uncertain environment," *J. Internet Technol.*, vol. 20, no. 3, pp. 755–769, 2019.

[5] Y. Yin, J. Xia, Y. Li, Y. Xu, W. Xu, and L. Yu, "Group-wise itinerary planning in temporary mobile social network," *IEEE Access*, vol. 7, pp. 83682–83693, 2019.

[6] I. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh, and H. T. Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities," *Comput. Netw.*, vol. 145, pp. 207–218, Nov. 2018.

[7] K. Cabaj, M. Gregorczyk, W. Mazurczyk, P. Nowakowski, and P. Żórawski, "Network threats mitigation using software-defined networking for the 5G Internet of radio light system," *Secur. Commun. Netw.*, vol. 2019, Feb. 2019, Art. no. 4930908.

[8] M. Schachter. DDoS & 5G: The bigger the Pipe, the Stronger the Threat. Allot Secure. Accessed: Jun. 26, 2018. [Online]. Available: https://www.allot.com/blog/ddos-5g-the-bigger-the-pipe-the-stronger-the-threat/

[9] I. A. Ridhawi, M. Aloqaily, Y. Kotb, Y. A. Ridhawi, and Y. Jararweh, "A collaborative mobile edge computing and user solution for service composition in 5G systems," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 11, 2008, Art. no. e3446.

[10] I. A. Ridhawi, N. Mostafa, Y. Kotb, M. Aloqaily, and I. Abualhaol, "Data caching and selection in 5G networks using F2F communication," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.

[11] M. Bacon. DDoS Attacks Among Top 5G Security Concerns. TechTarget SearchSecurity. Accessed: May 13, 2019. [Online]. Available: https://searchsecurity.techtarget.com/feature/DDoS-attacks-among-top-5G-security-concerns

[12] W. Mazurczyk, K. Szczypiorski, and B. Jankowski, "Towards steganography detection through network traffic visualisation," in *Proc. 4th Int. Congr. Ultra Modern Telecommun. Control Systems.*, Oct. 2012, pp. 947–954.

[13] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842, doi: 10.1016/j.adhoc.2019.02.001.

[14] B. Lipiński, W. Mazurczyk, K. Szczypiorski, and P. Śmietanka, "Towards effective security framework for vehicular ad-hoc networks," *J. Adv. Comput. Netw.*, vol. 3, no. 2, pp. 134–140, 2015.

[15] S. Newman, "5G will increase DDoS attack risk," *CORERO/Netw. Secur. Trends*, Dec. 2018. [Online]. Available: https://www.corero.com/blog/905-5g-will-increase-ddos-attack-risk.html

[16] CORERO. (2019). *Full Year 2018 DDoS Trends Report*. [Online]. Available: https://www.corero.com/resources/infographics/full-year-2018-ddos-trends-report-key-highlights-/

[17] VERISIGN. (2018). *Verisign Distributed Denial of Service Trends Report, Volume 5, Issue 1—1st Quarter*. [Online]. Available: https://www.verisign.com/en_GB/security-services/ddos-protection/ddos-report/index.xhtml

[18] J. Postel, *User Datagram Protocol*, document RFC 768, Aug. 1980.

[19] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Vice over IP," *IEEE Spectr.*, vol. 47, no. 2, pp. 42–47, Feb. 2010.

[20] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," *ACM Trans. Comput. Syst.*, vol. 24, no. 2, pp. 115–139, May 2006, doi: 10.1145/1132026.1132027.

[21] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, Feb. 2014, pp. 23–26.

[22] Jose Arteaga & Wilber Mejia. *CLDAP Reflection DDoS, Akamai's Threat Advisory*. Accessed: Apr. 3, 2017. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf

[23] L. Constantin. Attackers use NTP Reflection in Huge DDoS Attack. Computerworld. Accessed: Feb. 11,2014. [Online]. Available: https://www.computerworld.com/article/2487573/network-security/attackers-use-ntp-reflection-in-huge-ddos-attack.html

[24] J. Burbank, D. Mills, and W. Kasch, *Network Time Protocol Version 4: Protocol and Algorithms Specification*, document RFC 5906, IETF, Jun. 2010. [Online]. Available: https://tools.ietf.org/html/rfc5905

[25] D. L. Mills. *Network Time Protocol (NTP) General Overview*. Accessed: Aug. 2, 2004. [Online]. Available: http://www.eecis.udel.edu/~mills/database/brief/overview/overview.pdf

[26] E. M. Donner. *Prolexic Releases DNS Reflection Attack White Paper: Popular, Effective Distributed Reflection Denial of Service (DrDoS) Attacks Disrupt the Internet Domain Name System to Target Their Victims*. CISION PRWeb. Accessed: Mar. 19, 2013. [Online]. Available: http://www.prweb.com/releases/prolexic/dos-ddos-mitigation/prweb10544638.htm

[27] Akamai's. *NTP-AMP: Amplification Tactics And Analysis*. Accessed: Mar. 2014. [Online]. Available: http://docplayer.net/19890492-Ntp-amp-amplification-tactics-and-analysis.html

[28] D. Lukan. Packet Filtering. Infosec Resources. InfoSec Institute. Accessed: Sep. 26, 2012. [Online]. Available: https://resources.infosecinstitute.com/packet-filtering/#gref

[29] UTC, Wikipedia. *Stateless Protocol*. Accessed: Jan. 9, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Stateless_protocol

[30] T. Aura and P. Nikander, "Stateless connections," in *Proc. Int. Conf. Inf. Commun. Secur. (ICICS)*, vol. 1334, 1997, pp. 87–97.

[31] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*. Springer, 2013. [Online]. Available: https://www.springer.com/gp/book/9783540431077

[32] K. Matsuura and H. Imai, "Protection of authenticated key-agreement protocol against a Denial-of-service attack," in *Proc. Int. Symp. Inf. Theory Its Appl. (ISITA)*, Oct. 1998, pp. 466–470.

[33] B. Groza and M. Minea, "Formal modelling and automatic detection of resource exhaustion attacks," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur.*, Hong Kong, 2011, pp. 326–333.

[34] L. Jiang, C. Xu, X. Wang, and Y. Zhou, "Analysis and comparison of the network security protocol with DoS/DDoS attack resistance performance," in *Proc. High Perform. Comput. Commun.(HPCC), IEEE 7th Int. Symp. Cyberspace Saf. Secur. (CSS), IEEE 12th Int. Conf. Embedded Softw. Syst. (ICESS), IEEE 17th Int. Conf.*, Aug. 2015, pp. 1785–1790, doi: 10.1109/HPCC-CSS-ICESS.2015.148.

[35] M. R. Valluri, "An identification protocol based on the twisted ring-root extraction problem," in *Proc. World Congr. Ind. Control Syst. Secur. (WCICSS)*, Dec. 2015, pp. 95–97.

[36] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. 12th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, Aug. 1992, pp. 139–147.

[37] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 1999, pp. 151–165.

[38] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 281–310.

[39] S. C. H. Huang, D. MacCallum, and D. Z. Du, Eds., *Network Security*. Springer, 2010, pp. 231–232.

[40] T. Aura, P. Nikander, and J. Leiwo, "DoS-resistant authentication with client puzzles," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 2000, pp. 170–177. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-44810-1_22
[41] P. Karn and W. Simpson, *Photuris: Session-Key Management Protocol*, document RFC 2522, Mar. 1999.
[42] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, *Internet Key Exchange Protocol Version 2 (IKEv2)*, document RFC 7296, Oct. 2014.
[43] W. Mazurczyk and Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking," Feb. 2006, *arXiv:cs/0602042*. [Online]. Available: https://arxiv.org/abs/cs/0602042
[44] C. Lin, Y. Wang, and Q.-L. Li, "Stochastic modeling and evaluation for network security," *Chin. J. Comput.*, vol. 28, no. 12, pp. 1943–1956, 2005.
[45] J. McDermott, "Attack-potential-based survivability modeling for high-consequence systems," in *Proc. 3rd IEEE Int. Workshop Inf. Assurance (IWIA)*, Mar. 2005, pp. 119–130.
[46] K. Goseva-Popstojanova, F. Wang, R. Wang, F. Gong, K. Vaidyanathan, K. Trivedi, and B. Muthusamy, "Characterizing intrusion tolerant systems using a state transition model," in *Proc. DARPA Inf. Survivability Conf. Expo. (DISCEX)*, vol. 2, Jun. 2001, pp. 211–221.
[47] H. Gao, W. Huang, and X. Yang, "Applying probabilistic model checking to path planning in an intelligent transportation system using mobility trajectories and their statistical data," *Intell. Automat. Soft Comput.*, vol. 25, no. 3, pp. 547–559, Jan. 2019.
[48] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.
[49] R. Stewart, *Stream Control Transmission Protocol*, document RFC 4960, Sep. 2007. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc4960.txt.pdf
[50] G. Xu, B. Guo, C. Su, X. Zheng, K. Liang, D. S. Wong, and W. H. Wang, "Am i eclipsed? A smart detector of eclipse attacks for Ethereum," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101604.

HAIOU HUANG was born in Tonghua, Jilin, in 1980. She received the B.S. degree in computer science and technology from the Changchun University of Technology, in 2004, and the master's degree in computer application technology from the Changchun University of Science and Technology, in 2009. She is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Jilin University, Changchun. Her research interests include data security and privacy, and wireless networks.

LIANG HU was born in 1968. He received the B.S. degree from the Harbin Institute of Technology (HIT), Harbin, and the M.S. and Ph.D. degrees from the College of Computer Science and Technology, Jilin University (JLU), Changchun, China. He has been a Professor, since 2002, and has been a Ph.D. Supervisor, since 2003, with Jilin University. His current research interests include distributed computing, network computing and security, data security and privacy, and so on.

JIANFENG CHU received the M.S. and Ph.D. degrees from the College of Computer Science and Technology, Jilin University, Changchun. He is currently a Sub-Professor with the College of Computer Science and Technology, Jilin University. His research interests include network penetration, and data security and privacy.

XIAOCHUN CHENG (SM'04) received the B.Eng. degree in computer software engineering and the Ph.D. degree in computer science from Jilin University, in 1992 and 1996, respectively. He has been a Computer Science EU Project Coordinator with Middlesex University, since 2012. He is currently a member of the IEEE SMC Technical Committee on Enterprise Information Systems, the IEEE SMC Technical Committee on Computational Intelligence, the IEEE SMC Technical Committee on Cognitive Computing, the IEEE SMC Technical Committee on Intelligent Internet Systems, the IEEE Communications Society Communications and Information Security Technical Committee, the BCS Information Security Specialist Group, the BCS Cybercrime Forensics Specialist Group, and the BCS Artificial Intelligence Specialist Group.