Formal Theory for Security Protocol Analysis of Distributed Denial of Service

RUI JIANG
Southeast University
and
BHARAT BHARGAVA
Purdue University

Distributed Denial of Service (DDoS) attack is a great threat to the Internet. Generally, the research in this area focuses on the behaviors of the network, which can not fundamentally solve the problem. In fact, the main reason for the DDoS attack is the loss of security in the communication protocol, therefore what needs to be done is the security protocol analysis. In this paper, a novel formal theory for security protocol analysis of DDoS is proposed. Based on the strand space model, the novel formal theory extends the strand space model with the weighted graph, the state functions of the nodes and a new penetrator model. Then, two kinds of DDoS test models are proposed with the goal of anti-DDoS attack. The DDoS test 1 states that, when an incoming message is received, if it can be authenticated by the receiver, the cost to the sender of preparing it should be greater than the cost to the recipient of authenticating it. The DDoS test 2 states that, when a message is received, if its sender cannot be determined, then the cost to prepare its reply should be negligible, and no state should be needed to complete the session. To show the correctness of the formal theory, two example protocols, which are the Internet key exchange (IKE) and the efficient DoS-resistant secure key exchange protocol (JFK), are formally analyzed. It is proved that the IKE easily suffers from the DDoS attacks, and the JFK is resistant against DDoS attack for the server, respectively. The new formal theory is concise and straightforward, and can keep all the merits of the original strand space model.

Keywords: Distributed denial of service, security protocol analysis, formal theory, strand space model, internet key exchange

1. INTRODUCTION

Distributed Denial of Service (DDoS) attack is a great threat to the Internet, and the research about DDoS is done worldwide. However, all research focuses on the behaviors of the network and mainly deals with two kinds of problem [1, 2], which are the control of information flow and the differentiation of information flow. The control of information flow can deal with the attacks to bandwidth, and the differentiation of information flow can distinguish the attackers from the regular users. Therefore, a series of methods to address the issue is proposed, which are the detection for DDoS attacks, tracking attack sources, differentiation of DDoS attack traffic, graphical authentication, prevention with a firewall, a filter-based DoS defense system, a distributed prevention approach, and the system providing preferential service.

Focusing on the detection for application-layer DDoS attacks, a scheme based on document popularity is introduced [3]. An Access Matrix is defined to capture the spatial-temporal patterns of a normal flash crowd and an anomaly detector based on hidden semi-Markov model is proposed to describe the dynamics of Access Matrix and to detect the attacks. By using a novel distributed divide-and-conquer approach, the authors [4] design a data dissemination architecture that efficiently tracks attack sources, which include attack tree construction, attack path frequency detection and packet to path association. In order to trace DDoS attack, Sowmyadevi et al [30] propose the cyclical deterministic packet marking (CDPM) method, which implements an identification and classification algorithm on Border gateway, to identify an attack source and

This work is supported by National Natural Science Foundation of China under contract No. 61202448, and the Key Laboratory Program of Information Network Security of Ministry of Public Security (No.C14610).

multicast the information to an edge router. To differentiate DDoS flooding attack traffic from legitimate self-similar traffic in the network [5], the authors use the theory of network self-similarity. They develop a neural network detector trained by DDoS prediction algorithm to detect attack traffic during transit and to filter it. Also, the artificial neural networks (ANN) is employed to estimate number of zombies involved in a DDoS attack [31]. The method does not depend on the frequency of attack and hence solves the problem of low detection precision and weak detection stability of ANN which occurs when used for low frequent attack estimation. By using graphical tests for authentication, the authors [6] present the design and implementation of Kill-Bots, a kernel extension to protect Web servers against DDoS attacks. Kill-Bots uses an intermediate stage to identify the IP addresses, sends a test and checks the clients answer without allowing unauthenticated clients access to sockets and worker processes, and combines authentication with admission control. Based on a firewall [7], the authors propose a scheme to detect and prevent the DDoS attacks from the first packet itself. The firewall can distinguish the attack packets from the packets sent by legitimate users based on the marking value on the packet, and thus filter out most of the attack packets. A filter-based DoS defense system named StopIt is designed and implemented in [8]. The StopIt can block the attack traffic from a few millions of attackers within tens of minutes with the bounded router, and can prevent legitimate communications from being disrupted by various DoS flooding attacks. In [9], a distributed approach to detecting DDoS flooding attacks at the traffic-flow level is presented. The defense system is suitable for efficient implementation over the core networks operated by Internet service providers (ISPs). The authors develop a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The security coverage of the defense system is wide enough to safeguard most ISP core networks from real-life DDoS flooding attacks. The authors [10] propose systems using capabilities to provide preferential service to selected flows as a defense against large-scale network DoS attacks. The authors prove that a legitimate sender can establish a capability with high probability regardless of an attackers resources or strategy.

According to the previous research, it is really difficult to deal with the DoS problem if the basic framework of the Internet is not changed. However, it is impossible to change the Internet framework. Therefore, the DoS attack cannot be solved by the method of analyzing the behaviors of the network.

In fact, the reason for the DoS attack on the Internet and any other communication system is the loss of security for the communication protocol [11]. Only because the protocols on the Internet are always short of security requirements, is it possible for the DoS attack. Therefore, the formal theory for the security protocol is necessary to address the DoS attack. Formal theory as a potential tool for security protocol analysis was actually done by Dolev and Yao[12]. Later, most of this work used some type of state exploration techniques such as NRL Protocol Analyzer [13], and others were based on the belief logic such as BAN[14]. Then, the research has been focused on state exploration tools and theorem proving techniques based on the Dolev-Yao model, which was to use a general-purpose model checker such as FDR [15]. More recently, Thayer et al.[16] developed a graph-theoretic interpretation of the Dolev-Yao model, called the strand space model, it has been used as a basis for new special-purpose tools and a framework in which to express theoretical results. However, all these formal theories and methods only focus on the confidentiality and authenticity of the protocol analysis, and lack DoS analysis, which is one of the emerging areas of research [11].

Meadows [17] presented a formal framework for network DoS, and showed some principles to indicate that existing cryptographic protocol analysis tools such as formal methods on belief logics and state exploration techniques could be modified to operate within the formal framework. However, she did not present the definite theory and method to analyze whether the protocol would suffer from the DoS attack or not. She only analyzed the station-to-station protocol of Diffie, van Oorschot, and Wiener, which was designed with message economy rather than denial of service, and pointed out some weaknesses. Moreover, she even did not address the SYN flood

attack problem in the paper. Abadi et el.[29] used the Pi Calculus to formally analyze the JFK protocol[22] and proved it could withstand the DoS attack. However, the whole analysis procedure, which included two lemmas and one theorem, seemed only a special way for JFK rather than the general approach for a protocol to deal with the DoS attack. In addition, the formal analysis seemed actually not to work effectively for the DoS attack. The theorem expressed that the responder committed session-specific resources only once an initiator has established round-trip communication, which was depended only on the responder controlling the emission of token and the attacker being not able to eavesdrop it from message 2. But it will inevitably cost a lot of resource such as calculation and memory for the responder to make sure whether the initiator has established round-trip communication or not, and this will inevitably cause the DoS attack. In fact, the active attacker can fake IP address in message 1, reuse the token part in message 2, and randomly forge the other parts of message 3. Then the responder should consume a lot of calculation to recognize the forged message 3, and will suffer from the DoS attack in this way. Unfortunately, the theorem 1 cannot address this kind of problem with Pi Calculus. In 2009, Basagiannis et al.[18] introduce probabilistic model checking as an efficient tool-assisted approach for systematically quantifying DoS security threats. The authors model a security protocol with a fixed network topology using probabilistic specifications for the protocol participants and analyze a serious DoS threat, for which they provide probabilistic estimates, as well as results for the associated attacker and participants costs. However, they did not propose the exact theory to deal with the DoS attack. In our early work [19], we propose a novel theory to deal with the DoS attack and can prove whether the protocol is DoS-resistant or not. In this paper, we will make further concernswhich introduce the state function of the nodes, to extend the strand space model, and propose two new DoS Tests to deal with the DDoS attack.

The main contributions of this paper are described as follows. First, we introduce state functions of the nodes, concept of weighted graph, and a new penerator model to extend the strand space model, which can connect the weighted graph with the functions. Secondly, based on the extended strand space model, we propose two principles, which are called two DDoS tests, to formally analyze the DDoS attack. The first principle is, when an incoming message is received, if it can be authenticated by the receiver, the cost to the sender of preparing it should be greater than the cost to the recipient of authenticating it. The second principle is, when a message is received, if its sender cannot be determined, then the cost to prepare its reply should be negligible, and no state should be needed to complete the session. Finally, we formally demonstrate our theory with two example protocols, which are the Internet Key Exchange (IKE) protocol [21] and the efficient DoS-resistant secure key exchange protocol (JFK) [22], to differentiate whether the protocol can withstand the DDoS attack or not. We formally prove the IKE is DDoS-stop, and the JFK is DDoS-resistant.

In this paper, we first introduce the state function of the nodes, the concept of weight graph and a new penatrator model to extend the strand space model. Then we propose two DDoS test model with the conception of DDoS-stop protocol based on the fail-stop protocol [20]. Finally, we apply our formal theory to analyze the two example protocols, which are the Internet Key Exchange (IKE) protocol [21] and the efficient DoS-resistant secure key exchange protocol (JFK) [22]. We prove the IKE is DDoS-stop, and the JFK is DDoS-resistant. The rest of this paper is organized as follows. Based on the original strand space model, we extend the strand space model in Section 2. In Section 3, we propose our novel formal theory for protocol analysis of DDoS attack. Then in Section 4, we apply our formal theory to analyze two example protocols, which are the IKE protocol and the JFK protocol, and prove the IKE is DDoS-stop, and the JFK is DDoS-resistant. The Conclusion is made in Section 5.

2. EXTENDED STRAND SPACE MODEL

In this section, based on the strand space model [16], we introduce concept of weighted graph, state functions of the nodes and a new penerator model to extend the strand space model. The

extended strand space model is a new formal model which includes weighted graph, nodes state functions, new bundles, new term, new encryption and new penetrator model.

2.1 Basic Notions

Consider a set A, the elements of which are the possible messages that can be exchanged between principals in a protocol. The set A is constrained further below in Section 2.3. We refer the element of A as terms t, $t_1 \in t$ denotes t_1 is a subterm of t. where the subterm relation will be defined in Section 2.3. We will represent sending a term as the occurrence of that term with positive sign, and receiving a term as its occurrence with a negative sign.

Definition 2.1 A signed term is a pair $\langle \sigma, a \rangle$ with $a \in$A and σ one of the symbols $+, -$. We will write a signed term as $+t$ or $-t$. $(\pm A)^*$ is the set of finite sequences of signed terms. We will denote a typical element of $(\pm A)^*$ by $\langle \langle \sigma_1, a_1 \rangle, ..., \langle \sigma_n, a_n \rangle \rangle$.

Definition 2.2 An extended strand space is a set $\sum'$ with a trace mapping tr: $\sum' \to (\pm A)^*$, and has a function mapping fu: $\sum' \to R$, in which all the elements of the real set R is positive, i.e. r$\in R$ and r≥ 0.

Fix an extended strand space $\sum'$.

(1) W is an ordered weighted graph with quintuple $\langle V, E, H, F, G \rangle$, where V is a set of nodes, $E = E_0 \cup E_1$ in which E_0 is a set of edges $'' \to''$, and E_1 is a set of edges $'' \Rightarrow''$. Define H to be $fu(V)$ as a mapping: $V \to R$, F to be $fu(E_0)$ as a mapping: $E_0 \to R$, and G to be $fu(E_1)$ as a mapping: $E_1 \to R$.

(2) A node is a pair $\langle s, i \rangle$, with $s \in \sum'$ and i an integer satisfying $1 \leq i \leq length(tr(s))$. The set of nodes is denoted by V. We say the node $\langle s, i \rangle$ belongs to the E-strand s. Clearly, every node belongs to a unique E-strand.

(3) If $n = \langle s, i \rangle \in V$ then index $(n) = i$ and strand $(n) = s$. Define term (n) to be $(tr(s))_i$, i.e. the i th signed term s in the trace of . Similarly, uns term (n) is $((tr(s))_i)_2$, i.e. the unsigned part of the i th signed term in the trace of i.

(4) If $n = \langle s, i \rangle \in V$ then index $(n) = i$ and strand $(n) = s$. Define $h(n)$ the state function value at node n, which is an element of the range $H(V)$, i.e., $h(n) \in H(V) \subseteq R$. The state function value $h(n)$ denotes the weight on node n .

(5) If $n_1, n_2 \in V$, $n_1 \xrightarrow{f_a} n_2$ means term $(n_1) = +a$ and term with the function value f_a, which is an element of the range $F(E_0)$, i.e., $f_a \in F(E_0) \subseteq R$. It means that node n_1 sends the message a, which is received by n_2, creating a casual link between their E-strands. The function value f_a denotes the weight of the corresponding edge $'' \to''$.

(6) If $n_1, n_2 \in V$, then $n_1 \overset{g_a}{\Rightarrow} n_2$ means n_1, n_2 occur on the same E-strand with index (n_1)=index(n_2)-1 and the function value g_a, which is an element of the range $G(E_1)$, i.e., $g_a \in G(E_1) \subseteq R$. It expresses that n_1 is an immediate causal predecessor of n_2 on the E-strand. The function value g_a denotes the weight of the corresponding edge $'' \Rightarrow''$.

(7) An unsigned term t occurs in $n \in V$ if $t \in$ term (n).

(8) An unsigned term t originates on $n \in V$ if: term (n) is positive; term (n); and whenever n' precedes n on the same E-strand, $t \notin$term(n').

(9) An unsigned term t is uniquely originating if t originates on a unique $n \in V$.

To extend the strand space model, we apply the conceptions of Clause 2, 3, 7, 8 and 9 from the reference [16], which can make our new model completely be compatible to the original strand space model and hold all the merits of it.

2.2 Weighted E-bundles

A weighted E-bundle is a finite subgraph of this weighted graph, for which we can regard the nodes with the state function value $H(V)$, and regard the edges as expressing the causal dependencies

of the nodes, where the elements of the range $F(E_0)$ and $G(E_1)$ as expressing the weights on the corresponding edges.

Definition 2.3 Let β be a set of edges, let $F(E_0)$ and $G(E_1)$ be sets of corresponding function values for relating edges respectively, let V_B be the set of nodes incident with any edge in β , and let $H(V_B)$ be sets of state function values for these nodes, β is a weighted E-bundle if:

(1) β is finite.

(2) If $n_1 \in V_B$, then there is state function value $h(n_1)$, where $h(n_1) \in H(V_B)$.

(3) If $n_1 \in V_B$ and term(n_1) is negative, then there is a unique such that $n_2 \xrightarrow{f_a} n_1 \in \beta$, where $f_a \in F(E_0)$.

(4) If $n_1 \in V_B$ and $n_2 \overset{g_a}{\Rightarrow} n_1$, then $n_2 \overset{g_a}{\Rightarrow} n_1 \in \beta$, where $g_a \in G(E_1)$.

(5) β is acyclic.

Definition 2.4 A node n is in a weighted E-bundle β, written $n \in \beta$, if $n \in V_B$; a strand s is in a E-bundle if all of its nodes are in V_b.

Definition 2.5 If β is a weighted E-bundle and $s \in \Sigma'$, then the β-height of s, denoted height $_B(s)$, is the largest $i \leq length(tr(s))$ such that $s \in \Sigma'$ and $\langle s, i \rangle \in \beta$. β contains s if height $_B(s)$= $length(tr(s))$.

Definition 2.6 If s is a E-strand and β a weighted E-bundle, the β-trace of s, denoted tr $_B(s)$, is the restriction of tr(s) to the integer interval $\{1, ..., height_B(s)\}$.

From the above definitions, we can know, for a protocol with corresponding principals and whole session exchange course, there is a definite bundle β which includes the definite messages, definite nodes, definite edges, definite state function of the nodes, and definite weights functions on the corresponding edges.

2.3 Terms, Encryption and Authentication Code

We now specialize the set of terms A. We assume given:

A set $T \subset A$ of texts (representing the atomic messages).

A set of names $\mathbf{T}_{names} \subseteq \mathbf{T}$. We will use principal variables such as C (client), S (server) to range over T_{name}.

A set K $\subset$ A of cryptographic keys disjoint from T, equipped with a unary operator inv: $K \to K$. We assume that inv maps each member of a key pair for an asymmetric cryptosystem to the other, and that it maps a symmetric key to itself.

Three binary operators:

$$\text{encr and sig: } \mathbf{K} \times A \to A$$
$$\text{mac and keyed hash: } \mathbf{K} \times A \to A$$
$$\text{join: } A \times A \to A$$

As usual, we write inv(K) as K^{-1}, encr(K, m) and sig(K, m) as $\{|m|\}_K$ that means message m encrypted or signed by key K, mac(K, m) and hash(K, m) as $\{|m|\}^K$ that means message m created authentication code or hashed by key K, and join(a, b) as ab.

Definition 2.7 The subterm relation $\in$ is defined inductively, as the smallest relation such that $a \in a$; $a \in \{|g|\}_K$ if $a \in g$, $a \in gh$; if $a \in g$ or $a \in h$.

2.4 Extended Penetrator Model

We extend the penetrators E-strand with $Au.$ strand that means the penetrator can forge the authentication code and the keyed hash, and extend the definitions of E. strand and D. strand so that the two strands will include the signature and verification respectively. Therefore, the definition of extended penetrator is described as follows:

Definition 2.8 An extended penetrator strand is one of the following:

M: Text message: $\langle +t \rangle$ where $t \in T$.

F: Flushing: $\langle -l \rangle$.
T: Tee: $\langle -l, +l, +l \rangle$.
C: Concatenation: $\langle -l, -h, +lh \rangle$.
S: Separation into components: $\langle -lh, +l, +h \rangle$.
K: Key: $\langle +K \rangle$ where $\langle +K \rangle$.
E: Encryption and Signature: $\langle -K, -h, +\{|h|\}_K \rangle$.
D: Decryption and Verification: $\langle -K^{-1}, -\{|h|\}_K, +h \rangle$.
Au: Authentication code and keyed hash:$\left\langle -K, -h, +\{|h|\}^K \right\rangle$.

Definition 2.9 An infiltrated E-strand space is a pair ($\sum'$,P) with $\sum'$ an extended strand space and $P \subseteq \sum'$ such that $tr(P)$ is a penetrator trace for all $p \in P$. A E-strand $s \in \sum'$ is a penetrator strand if it belongs to P, and a node is a penetrator node if the E-strand it lies on is a penetrator strand. Otherwise we will call it a regular E- strand or node.

3. FORMAL THEORY FOR ANALYSIS OF DISTRIBUTED DENIAL OF SERVICE

In this section we propose our formal theory for analysis of DDoS based on the extended strand space model. We first introduce the notion of fail-stop protocol to define the DDoS-stop protocol, then we define the goal of anti-DDoS property. Finally, we propose two kind of DDoS tests models to create our new formal theory for analysis of DDoS.

3.1 Goal of anti-DDoS property

The conception of the fail-stop protocol was first proposed in [20]. The authors organize the messages of a protocol into an acyclic directed graph where each arc represents a message and each directed path represents a sequence of messages. In a fail-stop protocol, if a message actually sent is in any way inconsistent with the protocol specification, then all those messages that are behind this altered message on some path in the graph (i.e., they are causally after the altered message) will not be sent. Therefore, we can define the DDoS-stop protocol as follows:

Definition 3.1 A protocol is DDoS-stop if any DDoS attack launched and interfering with a regular message sent in one step will cause all following messages in the next step or later not to be sent. The goal of DDoS-stop property for a protocol has a logical form of a sentence:

$$\forall \beta \forall s \exists s'. tr_B(s) = i \cap \Phi(s) \rightarrow tr_B(s') = j \cap \Omega(s, s')$$

β is a weighted E-bundle, s, s' are E-strands. $tr_B(s) = i < height_B(s)$ and $tr_B(s') = j < height_B(s')$. The hypothesis $\Phi(s)$ typically says what type of E-strand s is, such as an initiator E-strand or a responder E-strand. It typically contains assumptions that certain values are uniquely originating and that certain keys are uncompromised. The conclusion $\Omega(s, s')$ typically says the assertion that what type of corresponding E-strand s' is, such as a responder E-strand or an initiator E-strand, and always entails that s' is regular. It will also say the protocol must stop at the i th step and j th step for s and s', respectively, to avoid the DDoS attack.

In definition 3.1, the meaning of interfering with a regular message is the message recipient in the protocol cannot easily distinguish the regular message from the forged messages. The easily means the recipient should cost less resource and calculation to distinguish the regular message than that of the attacker to make the forged messages. Based on the conception of DDoS-stop protocol, we can define the goal of anti-DDoS property with the extended strand space model as follows:

Definition 3.2 The goal of anti-DDoS property for a protocol has a logical form in common. It takes the form of a sentence:

$$\forall \beta \forall s \exists s'. height_B(s) = i \cap \Phi(s) \rightarrow height_B(s') = j \cap \Psi(s, s')$$

β is a weighted E-bundle, s, s' are E-strands. The hypothesis $\Phi(s)$ typically says what type of E-strand s is, such as an initiator E-strand or a responder E-strand. It typically contains assumptions that certain values are uniquely originating and that certain keys are uncompromised.

The conclusion $\Psi(s, s')$ typically says what type of E-strand s' is, such as a responder E-strand or an initiator E-strand, and always entails that s' is regular. It will also say which data values must be shared between s and s'.

3.2 DDoS Test Model

In order to define the DDoS test model, we now introduce the notion of cost set and define three cost function values. The first cost function value $h(n)$ describes the cost of the node n to maintain the state such as memory and pre-calculation, the second cost function value f_a describes the cost of a principals generating and sending a message in the protocol, and the third cost function value g_a describes the cost of a principals authenticating the received message in one E-strand.

Definition 3.3 The positive real set R is constrained into a cost set C_0, i.e. $C_0 \subseteq R$, in which every element of the set C_0 is the cost of resources and calculation for message processing in a protocol. Then the range of mapping H is constrained into sets of cost C_V, i.e., $C_V \subseteq H(V)$, in which every element of the set C_V is the cost of maintaining state of a node in V. The range of mappings F and G are constrained into sets of cost C_{E_0} and C_{E_1}, i.e., $C_{E_0} \subseteq F(E_0)$ and $C_{E_1} \subseteq G(E_1)$, in which every element of the set C_{E_0} and C_{E_1} is the cost of resources and calculation for message processing in weights on E_0 and E_1 respectively.

Definition 3.4 The function value $h(n)$, which is the element of C_V, i.e. $h(n) \in C_V$, and expresses the weight on node n with the cost of maintaining node state, is called a node state cost value.

In definition 3.4, function value $h(n)$ means the cost of maintaining node state such as memory and pre-calculation at a node n in weighted bundle β.

Definition 3.5 The function value f_a, which is the element of C_{E_0}, i.e. $f_a \in C_{E_0}$, and expresses the weight on E_0 with the cost of sending message , is called a E-strand linking cost value. The function value g_a, which is the element of C_{E_1}, i.e. $g_a \in C_{E_1}$, and expresses the weight on E_1 with the cost of receiving message a, is called a E- strand cost value.

In definition 3.5, function value f_a means the cost of resources and calculation for generating and sending message a at a node in weighted bundle β. Likewise, function value means the cost of resource and calculation for authenticating the received message a at a node in weighted bundle β.

Definition 3.6 Suppose that the message a cannot be authenticated on the edge in set E_1, then the E-strand cost value is $+\infty$, i.e., $g_a = +\infty$. Suppose that the node is positive, then the E-strand cost value on the following strand is $g = 0$. The node n is stateless only when the state cost value on it is $h(n) = 0$.

In definition 3.6, if the message a cannot be authenticated on the edge in set E_1, then $g_a = +\infty$. It means the subterm of message a cannot construct one of the tests between the outgoing test and the incoming test, which are described in reference [28]. Therefore, whatever the cost of resources and calculation the receiver spends, he cannot authenticate the identity that sends the message a. The E-strand cost value $g = 0$ implies the node is positive and the principal costs nothing on resource and calculation at the following strand. The node is stateless means the principal will cost nothing on resource and calculation in this node, i.e., the weight of the node in set V is zero.

We now describe the DDoS test model which includes two DDoS tests. The fact of the DDoS attack is the adversary sends as many bogus messages as possible to the victim server through the distributed network, then the victim server exhausts its resources to authenticate these messages or to maintain the establishment of communication so as to deny the legitimate users. So, each initiator may be an attacker before authenticated by the server. Therefore, we should take into account both the authentication and the cost of resources and calculation to deal with the problem, and propose two principles to address the DDoS attack. The first one is that the server will allocate its own resources only after he can authenticate the client or can determine the identity of the legitimate client. The other is that the client (initiator) should always commit

its more resources first and then the server (responder) will allocate its own resources, which is consistent with [23,24,25]. We will combine two principles and propose two DDoS tests based on the outgoing test and incoming test [28].

DDoS test 1 Let β be a weighted bundle in $\sum'$ with nodes $n, n' \in \beta$, and let $n \Rightarrow n'$ be an outgoing test or an incoming test for message a or subterm of a. Then:

(1) There exist regular nodes $m, m' \in \beta$ such that $n \xrightarrow{f_a} m \in \beta$ and $m \overset{g_a}{\Rightarrow} m' \in \beta$.

(2) Suppose in addition that $f_a \geq \alpha g_a$, where $\alpha \in R$ and $\alpha > 1$. Then the node m' can connect the next ordered edges $m' \xrightarrow{f_{a'}} n'$ and $m' \overset{g=0}{\Rightarrow} m''$ with message a'. In addition, the nodes $n, n', m, m'\pi$ are regular and $n \prec m \prec m' \prec n'$.

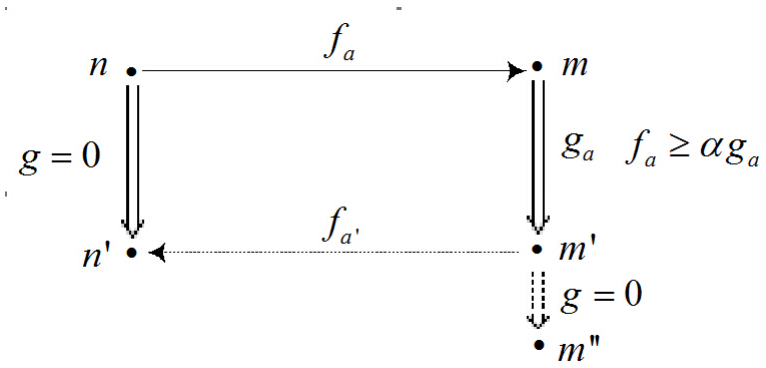

Figure. 1: Distributed denial of service test 1.

This assertion is illustrated in Figure 1. In this diagram, if the message a can be authenticated by the responder, which means the message a or subterm of a could construct one of the tests between the outgoing test and the incoming test, which are described in reference [28], then there exit regular nodes m and m'. In addition, if $f_a \geq \alpha g_a$ is qualified, which means the initiator commits more resources and calculation for generating and sending message a than that of the responder for receiving and authenticating the message, then the protocol can continue to perform correctly and withstand the DDoS attack. Furthermore, the nodes are ordered $n \prec m \prec m' \prec n'$ in the causal ordering. For example, if the receiver can authenticate the message a in a step of a running protocol, then he will check whether the cost of producing a is not less than α times of the cost for verifying a. Only when the check is OK, can the protocol run further.

DDoS test 2 Let β be a weighted bundle in $\sum'$ with regular nodes $n, m \in \beta$,and edge $n \xrightarrow{f_a} m \in \beta$. Then:

(1) There exists regular node $m' \in \beta$, such that $m \overset{g_a}{\Rightarrow} m' \in \beta$.

(2) Suppose in addition that $g_a = +\infty$ and $h(m') = 0$, then the node m' can connect the next ordered edges $m' \xrightarrow{f_{a'}} n'$ and $m' \overset{g=0}{\Rightarrow} m''$, where message a' should be pre-generated or easily generated, and there exists regular node $n' \in \beta$. In addition, the nodes n, n', m, m' are regular and $n \prec m \prec m' \prec n'$.

DDoS test 2 is illustrated in Figure 2. We show that, if $g_a = +\infty$, which means the responder cannot authenticate the message a, then the protocol should be performed stateless at this point to avoid DDoS attack. In addition, the nodes are ordered $n \prec m \prec m' \prec n'$ in the causal ordering. The stateless node m' means the protocol will cost nothing on resources and calculation at this point, i.e., $h(m') = 0$. To pre-generate or easily generate message a' means the value of $f_{a'}$ is negligible. For example, if the receiver can not authenticate the message a in a step of a running protocol, he can run the protocol further only when he will cost nothing in the following step.

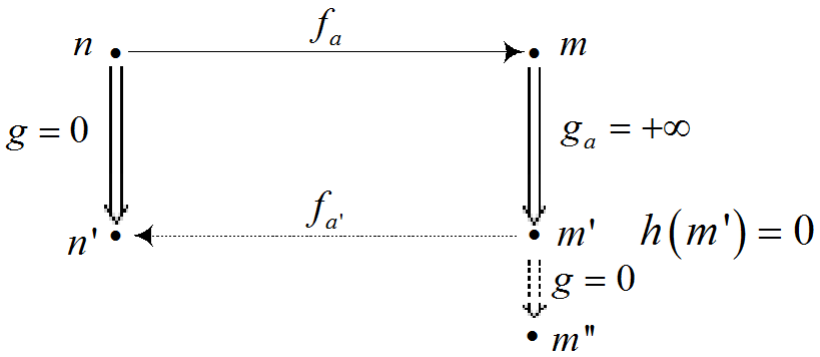

Figure 2: Distributed denial of service test 2.

Lemma 3.1 Let β be a weighted bundle. Suppose regular nodes $n, n' \in \beta$, $n \Rightarrow n'$ is an outgoing test or an incoming test for message a. If $f_a \geq \alpha g_a$, where $\alpha \in R$ and $\alpha > 1$. Then there exist regular edges $m \overset{g_a}{\Rightarrow} m'$, $m' \overset{f_{a'}}{\rightarrow} n'$ and $m' \overset{g=0}{\Rightarrow} m''$ with message a'. Also there exist regular nodes $n \prec m \prec m' \prec n'$.

Proof. If $n, n' \in \beta$ and $n \Rightarrow n'$ is an outgoing test or an incoming test for message a, then there exist regular nodes $m, m' \in \beta$ and transforming edge $m \overset{g_a}{\Rightarrow} m'$. Also there exist regular nodes $n \prec m \prec m' \prec n'$(Authentication Test 1 or 2 in [28]). Suppose $f_a \geq \alpha g_a$, according to DDoS test 1, there exist regular edges $m' \overset{f_{a'}}{\rightarrow} n'$ and $m' \overset{g=0}{\Rightarrow} m''$ with message a'. □

Lemma 3.2 Let β be a weighted bundle. Suppose regular nodes $n, m \in \beta$ and edge $n \overset{f_a}{\rightarrow} m \in \beta$. There exists regular node $m' \in \beta$ such that $m \overset{g_a}{\Rightarrow} m' \in \beta$. If $g_a = +\infty$, $h(m') = 0$ and message a' could be pre-generated or easily generated, then there exist regular edges $m' \overset{f_{a'}}{\rightarrow} n'$, $m' \overset{g=0}{\Rightarrow} m''$ and regular node $n' \in \beta$. Also, the nodes are $n \prec m \prec m' \prec n'$.

Proof. In a weighted bundle β, if $n, m \in \beta$ and $n \overset{f_a}{\rightarrow} m \in \beta$, then there exists regular node $m' \in \beta$ such that $m \overset{g_a}{\Rightarrow} m' \in \beta$(DDoS test 2). Suppose $g_a = +\infty$, $h(m') = 0$ and message a' be pre-generated or easily generated, according to DDoS test 2, then there exist regular edges $m' \overset{f_{a'}}{\rightarrow} n'$, $m' \overset{g=0}{\Rightarrow} m''$ and regular node $n' \in \beta$. Therefore, the regular nodes are $n \prec m \prec m' \prec n'$. □

Definition 3.7 A DDoS-resistant protocol is non-DDoS-stop, which means all steps of the protocol should obey the Lemma 3.1 or Lemma 3.2 and run to the end. Otherwise, it is DDoS-stop.

4. SHOWING PROTOCOL AGAINST DDOS ATTACKS

In this section we apply the theory of Section 3 to two examples. They are the Internet Key Exchange (IKE) protocol [21] and the efficient DoS-resistant secure key exchange protocol (JFK) [22]. We do so to illustrate how to use our formal theory for protocol analysis of DDoS. We will prove the IKE is DDoS-stop, and the JFK is DDoS-resistant.

4.1 Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) protocol [21] is designed to exchange keying material and negotiate security associations for secure communication. It works in two phases. Phase 1 establishes an ISAKMP SA and derives shared secrets that will be used to protect phase 2 exchange. Phase 2 negotiates SA_S for IPSEC and generates fresh keying material. In addition, the IKE protocol defines three basic modes of exchanges: main mode and aggressive mode used

in phase 1, and quick mode used in phase 2. We give a detailed exposition on the main mode protocol with pre-shared key for DoS test, so that the reader can see just how our method works. The method is also fit for other mode protocols. The brief description of the pre-shared key main mode protocol is as follows:

(1) $I \rightarrow R : HDR_1, SA_i$
(2) $R \rightarrow I : HDR_2, SA_r$
(3) $I \rightarrow R : HDR_3, KE_i, N_i$
(4) $R \rightarrow I : HDR_4, KE_r, N_r$
(5) $I \rightarrow R : HDR_5^*, ID_i, HASH_I$
(6) $R \rightarrow I : HDR_6^*, ID_r, HASH_R$

There are six steps of exchanges between the initiator I and the responder R in the protocol. The first two steps negotiate the ISAKMP SA, the next two steps exchange Diffie-Hellman public values, and the last two steps authenticate the ISAKMP SA and the Diffie-Hellman Exchange.

$HDR_j(j = 1, 2, ..., 6)$ is an ISAKMP header which includes the cookie (CKY). HDR_j^* indicates that all payload following HDR_j are encrypted. SA_i and SA_r are security association payloads. KE_i and KE_r are Diffie-Hellman public key exchange payloads. N_i and N_r are nonce payload. ID_i and ID_r are ISAKMP identification payload, where i and r represent the initiator and the responder, respectively. $HASH_I$ and $HASH_R$ are authenticators generated by the initiator and the responder, respectively.

At the end of step 4, the newly shared secret $SKEYID$ can be derived as follows:

$$SKEYID = prf(pre - shared - key, N_i\_b \| N_r\_b)$$

where prf is a keyed pseudo-random function, $pre - shared - key$ is a key pre-shared between the initiator and the responder, N_i_b and N_r_b are nonce payload excluding their generic payload heads, and ||represents concatenation.

Meanwhile, a set of cryptographic keys are generated as follows:

$$SKEYID_d = prf\,(SKEYID, g^{x_i x_r} \| CYK_I \| CKY_R \| 0\ )$$

$$SKEYID_a = prf\,(SKEYID, SKEYID_d \| g^{x_i x_r}\ \| CYK_I \| CKY_R \| 1\ )$$

$$SKEYID_e = prf\,(SKEYID, SKEYID_a \| g^{x_i x_r}\ \| CYK_I \| CKY_R \| 2\ )$$

where g^{x_i} and g^{x_r} are Diffie-Hellman public values included in KE_i and KE_r, and $g^{x_i x_r}$ is Diffie-Hellman shared secret. CKY_I and CKY_R are cookies generated by the initiator I and the responder R. $SKEYID_d$ will be used to derive keying material for IPSEC SA_S. $SKEYID_a$ will be used to authenticate IKE exchanges. $SKEYID_e$ will be used to protect the confidentiality of IKE exchange.

In step 5 and 6, the initiator and the responder authenticate their exchanges by sending the authenticators $HASH_I$ and $HASH_R$, which are defined as follows:

$$HASH_I = prf\,(SKEYID, g^{x_i} \| g^{x_r} \| CKY_I \| CKY_R \| SA_i\_b \| ID_i\_b\ \ )$$

$$HASH_R = prf\,(SKEYID, g^{x_r} \| g^{x_i} \| CKY_R \| CKY_I \| SA_i\_b \| ID_r\_b\ \ )$$

where SA_i_b is the initiators security association payload excluding its generic payload head. ID_i_b and ID_r_b are identification payloads excluding their generic payload heads. Although, the definitions of $HASH_I$ and $HASH_R$ have security shortage, which is analyzed in [26], it does not affect our analysis of DDoS attack. So, in this paper, we still use above definition.

At the end of the protocol, the SA_r is accepted as an ISAKMP SA by the negotiation peers.

We now apply our two DDoS tests to check whether the main mode protocol of IKE with pre-shared key can get over the DDoS attack. In the form we consider, the protocol involves two types of regular E-strands and is depicted in Figure 3.

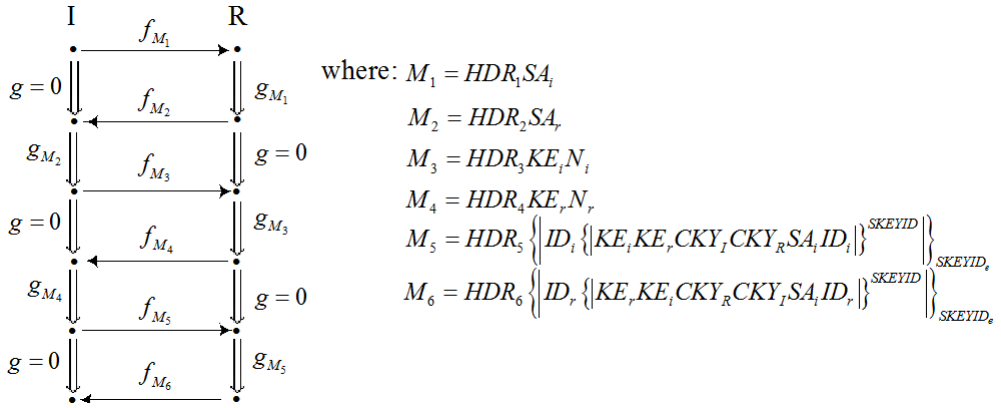

Figure 3: Regular weighted bundle in pre-shared key protocol of IKE.

(1) Initiator I E-strands with trace:$\langle +M_1, -M_2, +M_3, -M_4, +M_5, -M_6\rangle$, where $ID_i, ID_r \in T_{name}$, $HDR_j, CKY_I, CKY_R \in T, (j = 1, 2, ..., 6)$, $N_i, N_r, KE_i, KE_r, SA_i, SA_r \in T$, $pre-shared-key, SKEYID, SKEYID_e \in K$, $Init\,[N_i, N_r, KE_i, KE_r, ID_i, ID_r, SA_i, SA_r, CKY_I, CKY_R]$ will denote the set of all strands with the trace shown.

(2) Responder R E-strands with trace: $\langle -M_1, +M_2, -M_3, +M_4, -M_5, +M_6\rangle$, where $ID_i, ID_r \in T_{name}$, $HDR_j, CKY_I, CKY_R \in T, (j = 1, 2, ..., 6), N_i, N_r, KE_i, KE_r, SA_i, SA_r \in T$, $pre-shared-key, SKEYID, SKEYID_e \in K$, $Resp\,[N_i, N_r, KE_i, KE_r, ID_i, ID_r, SA_i, SA_r, CKY_I, CKY_R]$ will denote the set of all strands with the trace shown.

In general, we should only concern about whether the responder (server) can get over the DDoS attack. The meaning of this analysis is illustrated in Figure 4. For convenience, Let β be a weighted bundle and we denote the initiator E-strand with s and the responder E-strand with s'. We can know the nodes $\langle s, 1\rangle, \langle s', 1\rangle \in \beta$ and $\langle s, 1\rangle \overset{f_{M_1}}{\rightarrow} \langle s', 1\rangle \in \beta$, according to Lemma 3.2, there exists regular node $\langle s', 2\rangle \in \beta$ such that $\langle s', 1\rangle \overset{g_{M_1}}{\Rightarrow} \langle s', 2\rangle \in \beta$. For the responder R cannot authenticate message M_1 at all after receiving it, then $g_{M_1} = +\infty$. According to Lemma 3.2, if $h(\langle s', 2\rangle) = 0$, then there will exist next node and edges. Actually, in addition to sending message M_2, the responder at this point should keep the information of CKY_I and CKY_R. However, the cost is negligible, so $h(\langle s', 2\rangle) \approx 0$. Strictly, it violates the Lemma 3.2 at this step, for it should be stateless at the node and $h(\langle s', 2\rangle) = 0$. Therefore, an attacker may make DDoS attack at this step.

For we only concern about the DDoS attack on the responder (server), we can skip to the third step. We can know the nodes $\langle s, 3\rangle, \langle s', 3\rangle \in \beta$ and $\langle s, 3\rangle \overset{f_{M_3}}{\rightarrow} \langle s', 3\rangle \in \beta$, according to Lemma 3.2, there exists regular node $\langle s', 4\rangle \in \beta$ such that $\langle s', 3\rangle \overset{g_{M_3}}{\Rightarrow} \langle s', 4\rangle \in \beta$. For the responder R cannot authenticate message M_3 at all after receiving it, then $g_{M_3} = +\infty$. According to Lemma 3.2, if $h(\langle s', 4\rangle) = 0$, then there will exist next node and edges. Unfortunately, in addition to sending message M_4, the responder at this point should execute heavy computation, including four keyed pseudo-random function calculation and one modular exponential calculation, to generate $SKEYD, SKEYD_d, SKEYD_a, SKEYD_e$, and this heavy calculation cannot be pre-generated. Furthermore, the responder should keep much memory information such as $KE_i, KE_r, SA_i, CKY_I, CKY_R$, and etc. So, we can know $h(\langle s', 4\rangle) \gg 0$ at node $\langle s', 4\rangle$, and it violates the Lemma 3.2. Therefore, the protocol should terminate on this point to avoid DDoS attack. The IKE is DDoS-stop according to Definition 3.7.

In fact, if an attack sends as much bogus messages M_1, M_3 as possible to the responder, the responder will easily exhaust its calculation resources and deny the legitimate users, which is similar to the SYN flood attack in [27]. Therefore, the pre-shared key IKE protocol will

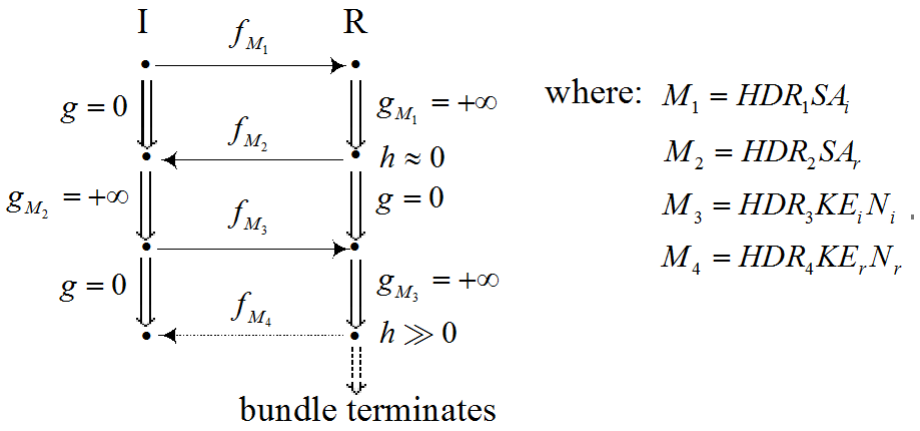

Figure 4: DDoS test on pre-shared key protocol of IKE.

easily suffer from the DDoS attack. It means if the IKE is applied in the Internet or any other communication system, it will cause the DDoS attack.

4.2 Efficient DoS-resistant Secure Key Exchange Protocol

The efficient DoS-resistant secure key exchange protocols [22] are proposed by ATT Labs Research, and called JFK to stand for Just Fast Keying. The JFK is primary designed for use in the IP Security Architecture, and has more advantages over IKE [21]. It has two variants, one is JFK_r that provides identity protection for the responder against active adversaries, the other is JFK_i that provides identity protection for the initiator even against active attacks. In this paper, we use JFK_r as an example.

The JFK_r protocol consists of four messages (two round trips):

(1) $I \rightarrow R : N_I, g^i$

(2) $R \rightarrow I : N_I, N_R, g^r, grp\inf o_R, H_{HK_R}\left(g^r, N_R, N_I, IP_I\right)$

(3) $I \rightarrow R : N_I, N_R, g^i, g^r, H_{HK_R}\left(g^r, N_R, N_I, IP_I\right)$
$\left\{ID_I, ID_{R'}, S_a, S_I\left[N_I, N_R, g^i, g^r, grp\inf o_R\right]\right\}_{K_e}^{K_a}$

(4) $R \rightarrow I : \left\{ID_R, S_a{}', S_R\left[N_I, N_R, g^i, g^r\right]\right\}_{K_e}^{K_a}$

In the above messages, N_I and N_R are nonce of initiator and responder respectively. g^i and g^r are current exponential of initiator and responder respectively. ID_I and ID_R are certificates or public-key identifying information of initiator and responder respectively. $ID_{R'}$ is an indication by the initiator to the responder as to what authentication information the latter should use. IP_I is the initiators network address. S_a is the cryptographic and service properties of the security association (SA) that the initiator wants to establish. $S_a{}'$ is the SA information the responder may need to give to the initiator. $grp\inf o_R$ are all groups supported by the responder, the symmetric algorithms used to protect messages (3) and (4), and the hash function used for key generation. $H_K(M)$ denotes the hash of message M with key K. $S_x[M]$ denotes the digital signature of the message M with the private key belonging to principal x (initiator or responder). $\{M\}_{K_e}^{K_a}$ denotes the message M encrypted by symmetric key K_e, followed with Message Authentication Code (MAC) by symmetric key K_a. HK_R is a transient hash key private to the responder. The keys used to protect messages (3) and (4), K_e and K_a, are computed as $H_{g^{ir}}\left(N_I, N_R, "1"\right)$ and $H_{g^{ir}}\left(N_I, N_R, "2"\right)$ respectively. $H_{HK_R}\left(g^r, N_R, N_I, IP_I\right)$ is used as an encrypted token in the protocol. K_e is used to encrypt the message and K_a is used to produce MAC. The session key passed to IPsec, K_{ir} , is $H_{g^{ir}}\left(N_I, N_R, "0"\right)$.

In the form we consider, the JFK_r involves two types of regular E-strands and is depicted in Figure 5.

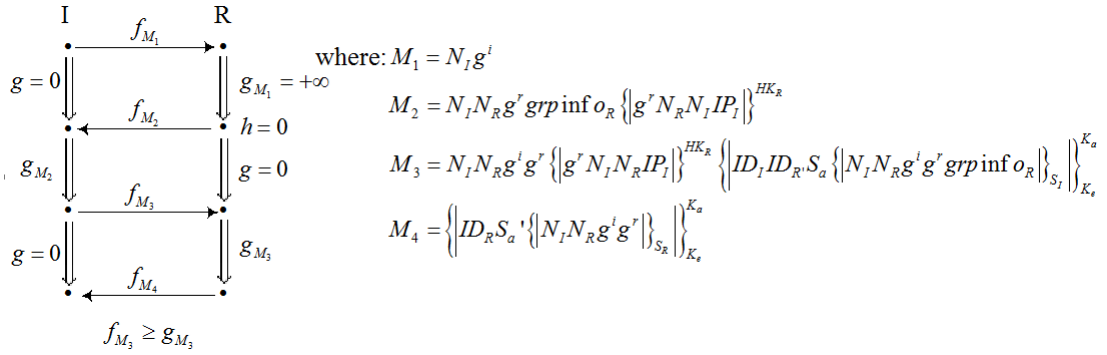

Figure 5: Regular weighted bundle for DDoS test in JFK_r.

(1) Initiator E-strands with trace: $\langle +M_1, -M_2, +M_3, -M_4 \rangle$, where $ID_I, ID_R \in T_{name}$, N_I, N_R, $g^i, g^r, S_a, S_a{}' \in T$, $N_I, g^i, S_a \notin T_{name}$, $S_I, S_R, HK_R \in K$ are the private keys, $K_a, K_e \in K$ are the symmetric keys. $Init\left[N_I, N_R, g^i, g^r, ID_I, ID_R, S_a, S_a{}'\right]$ will denote the set of all strands with the trace shown.

(2) Responder E-strands with trace: $\langle -M_1, +M_2, -M_3, +M_4 \rangle$, where $ID_I, ID_R \in T_{name}$, N_I, N_R, $g^i, g^r, S_a, S_a{}' \in T$ but $N_R, g^r, S_a{}' \notin T_{name}$, $S_I, S_R, HK_R \in K$ are the private keys, $K_a, K_e \in K$ are the symmetric keys. $Resp\left[N_I, N_R, g^i, g^r, ID_I, ID_R, S_a, S_a{}'\right]$ will denote the set of all strands with the trace shown.

We now prove the responder can withstand the DDoS attack. If the JFK_r protocol can obey the Lemma 3.1 or Lemma 3.2 in each message exchanging for the responder and run to the end, then we are sure this protocol can withstand DDoS attack for the responder. Otherwise, the protocol will fail to stop when any message exchanging fail to pass the DDoS test, and the responder will not waste its resources and calculation to the DDoS attacker.

Theorem 4.1 Let β be a weighted bundle in $\sum'$. Assume $S_I, S_R, HK_R \notin K_P$, suppose $N_I \neq N_R$, $i \neq r$, and N_I, N_R, i, r are uniquely originating, then there is a regular responder E- strand $s \in Resp\left[N_I, N_R, g^i, g^r, ID_I, ID_R, S_a, S_a{}'\right]$ with β-height 4 and the regular initiator E-strand $s \in Init\left[N_I, N_R, g^i, g^r, ID_I, ID_R, S_a, S_a{}'\right]$ with β-height 4.

Proof. In figure 5, we know first the nodes $\langle s', 1\rangle, \langle s, 1\rangle \in \beta$ and $\langle s', 1\rangle \overset{f_{M_1}}{\rightarrow} \langle s, 1\rangle \in \beta$, according to Lemma 3.2, there exists regular node $\langle s, 2\rangle \in \beta$ such that $\langle s, 1\rangle \overset{g_{M_1}}{\Rightarrow} \langle s, 2\rangle \in \beta$. For the responder has not any information to verify who sends the message M_1, then $g_{M_1} = +\infty$. According to Lemma 3.2, if $h(\langle s, 2\rangle) = 0$, then there will exist next node and edges. Fortunately, the responder at this point need not keep any memory information and execute any calculation except sending message M_2, so $h(\langle s, 2\rangle) = 0$. Then there exist regular edges $\langle s, 2\rangle \overset{f_{M_2}}{\rightarrow} \langle s', 2\rangle, \langle s, 2\rangle \overset{g=0}{\Rightarrow} \langle s, 3\rangle$ and regular node $\langle s', 2\rangle \in \beta$.

Although the nodes $\langle s, 2\rangle, \langle s', 2\rangle, \langle s', 3\rangle, \langle s, 3\rangle$ and corresponding edges compose the DDoS test 2, it only tests the DDoS attack for initiator, which is not concerned in this protocol, the protocol should continue at node $\langle s', 3\rangle$.

We know then the nodes $\langle s', 3\rangle, \langle s', 4\rangle \in \beta$ and $\langle s', 3\rangle \Rightarrow \langle s', 4\rangle$ is an incoming test for subterm of message M_3. Because $\left\{\left|N_I N_R g^i g^r grp \inf o_R\right|\right\}_{S_I}$ in message M_3 is a test for N_R, g^r and $grp \inf o_R$ according to Definition 13 in [28], checking the assumption $S_I \notin K_P$, then it follows that $\langle s', 3\rangle \Rightarrow \langle s', 4\rangle$ is an incoming test for N_R, g^r and $grp \inf o_R$ according to Definition 14 in [28]. According to Lemma 3.1, then there exist regular nodes $\langle s, 3\rangle, \langle s, 4\rangle \in \beta$ such that

$\langle s', 3\rangle \overset{f_{M_3}}{\rightarrow} \langle s, 3\rangle \in \beta$ and $\langle s, 3\rangle \overset{g_{M_3}}{\Rightarrow} \langle s, 4\rangle \in \beta$. Furthermore, if $f_{M_3} \geq \alpha g_{M_3}$, then there exist regular edge $\langle s, 4\rangle \overset{f_{M_4}}{\rightarrow} \langle s', 4\rangle$ with message M_4 and regular nodes $\langle s', 3\rangle \prec \langle s, 3\rangle \prec \langle s, 4\rangle \prec \langle s', 4\rangle$. Fortunately, we know $f_{M_3} \geq g_{M_3}$, because the calculation of encrypting and decrypting the same message M_3 with symmetric key K is generally equivalent, and the calculation of singing the message M_3 is generally greater than or comparative to that of verifying it. So, we can get $f_{M_3} \geq g_{M_3}$. Therefore, there will be a regular responder strand s with β-height 4 and the regular initiator strand s' with β-height 4. □

Theorem 4.1 proves JFK_r protocol can withstand DDoS attack for the responder (server) when the assumptions are satisfied, the protocol can obey the Lemma 3.1 or Lemma 3.2 and run to the end without failing to stop. It means we can use the JFK in the communication system to withstand the DDoS attack.

5. CONCLUSION

Distributed Denial of Service attack is a great threat to Internet. However, the research always concentrated in the behaviors of the network and can not deal with the problem exactly. In fact, the main reason for the DoS attack is the loss of security for the communication protocol. In this paper, we start from the security analysis of the protocol, then we extend the strand space model and propose a new formal theory to address the problem. First, we introduce the conception of weight graph and the state function of the nodes to extend the strand space model. Then we extend the penatrator model and propose the DDoS-stop protocol based on the fail-stop protocol. Finally, we define the goal of anti-DDoS property, propose two DDoS test model and two Lemmas to create the new formal theory for analysis of DDoS attack. In the end, we apply our new formal theory to analyze the two example protocols, which are the Internet Key Exchange (IKE) protocol and the efficient DDoS-resistant secure key exchange protocol (JFK). We prove the IKE is DDoS-stop, and the JFK is DDoS-resistant. It means if the IKE is applied in the Internet or any other communication system, it will suffer from the DDoS attack. On the contrary, we can use the JFK in the communication system to withstand the DDoS attack. Our novel formal theory model is concise and straightforward, and can keep all the merits of the original strand space model.

REFERENCES

Peng T, Leckie C, Ramamohanarao K, Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Computing Surveys , 2007, 39(1).

Kumar P A R, Selvakumar S,Distributed Denial-of-Service Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback MechanismsIEEE International Conference on Advance Computing 2009IACC 20096-7 March 2009pp.1275 -1280.

Yi Xie, Shun-Zheng Yu, Monitoring the Application-Layer DDoS Attacks for Popular WebsitesIEEE/ACM Transactions on Networking, Vol.17, No.1, 2009, pp.15-25.

Muthuprasanna M, Manimaran G, Distributed divide and conquer techniques for effective DDoS attack defenses, In Proc. IEEE ICDCS, 2008.

Chonka A, Singh J, Wanlei Zhou, Chaos theory based detection against network mimicking DDoS attacksIEEE Communications Letters, Vol.13, No.9, 2009, pp.717-719.

Kandula S, Katabi D, Jacob M, Botz-4-sale : surviving organized DDoS attacks that mimic flash crowds, In Proc. USENIX NSDI, 2005.

Nagaratna M, Prasad V K, Kumar S T, Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking Based Detection and Filtering (EMDAF), International Conference on Advances in Recent Technologies in Communication and Computing 2009 (ARTCom '09), 27-28 Oct. 2009, pp.753-755.

Liu X, Yang X, Lu Y, To filter or to authorize: network-layer DoS defense against multimillion-node botnets. In Proc. ACM SIGCOMM, 2008.

Yu Chen, Kai Hwang, Wei-Shinn Ku, Collaborative Detection of DDoS Attacks over Multiple Network Domains, IEEE Transactions on Parallel and Distributed Systems, Vol.18, No.12, 2007, pp.1649-1662.

Parno B, Wendlandt D, Shi E, Portcullis: protecting connection setup from denial of capability attacks, In Proc. ACM SIGCOMM, 2007.

C. Meadows, Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends, IEEE Journal on Selected Areas in Communications, Vol. 21, No. 1, January 2003, pp.44-54.

D. Dolev and A. Yao, On the security of public key protocols, IEEE Trans. Inform. Theory, vol. ITC29, pp. 198C208, Mar. 1983.

C. Meadows, Applying formal methods to the analysis of a key management protocol, Journal of Computer Security, vol. 1, pp. 5C53, 1992.

M. Burrows, M. Abadi, and R. Needham, A logic of authentication, ACM Trans. Comput. Syst., vol. 8, pp. 18C36, Feb. 1990.

G. Lowe, Breaking and fixing the Needham-Schroeder public-key protocol using FDR, Softw.Concepts Tools, vol. 17, no. 3, pp. 93C102, 1996.

F. T. Fbrega, J. Herzog, and J. Guttman, Strand spaces: Proving security protocols correct, Journal of Computer Security, 7(2/3): 191C230, 1999.

C. Meadows, A formal framework and evaluation method for network denial of service, in Proc. 12th IEEE Computer Security Foundations Workshop, June 1999, pp. 4C13.

Stylianos Basagiannis, Panagiotis Katsaros, Andrew Pombortsis, Nikolaos Alexiou, Probabilistic model checking for the quantification of DoS security threats, Computers Security, Vol.28, No.5, 2009, pp. 450-465.

Rui Jiang, A Novel Formal Theory for Security Protocol Analysis of Denial of Service Based on Extended Strand Space Model, China Communications, Vol.7, No.4, 2010, pp.23-28.

L. Gong and P. Syverson, Fail-stop protocols: An approach to design secure protocols, Dependable Computing for Critical Applications 5, pages 79-100. IEEE Computer Society 1998.

D. Harkins and D. Carrel. (1998) The Internet Key Exchange (IKE). Internet Engineering Task Force. [Online]. Available: http://ietf.org/rfc/rfc2409.txt

W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Loannidis, A. D. Keromytis and O. Reingold, Efficient, DoS-resistant, Secure key exchange for Internet protocols, ACM CCS 02, pages 27-39, Nov. 2002, Washington, DC USA.

A. Juels and J. Brainard, Client puzzles: A cryptographic countermeasure against connection depletion attacks, In Proc. 1999 Network and Distributed Systems Security Symposium (NDSS), pages 151C165, San Diego, CA, February 1999. Internet Society.

T. Aura, P. Nikander, and J. Leiwo, DoS-resistant authentication with client puzzles, Security Protocols Workshop 2000, pages 170-177.

K. Matsuura and H. Imai, Protection of authenticated key-agreement protocol against a denial-of-service attack, In Proceedings of 1998 International Symposium on Information Theory and Its Applications (ISITA 98), pp. 466-470, Oct. 1998.

J. Zhou, Further analysis of the Internet key exchange protocol, Computer Communications, 23, 2000, pp.1606C1612.

C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, and D. Zamboni, Analysis of a Denial of Service Attack on TCP, In Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 208-223. IEEE Computer Society Press, May 1997.

J. D. Guttman and F. J. Thayer Fabrega, Authentication tests and the structure of bundles, Theoretical Computer Science, 283(2): 333-380, 2002.

M. Abadi, B. Blanchet, and C. Fournet, Just Fast Keying in the Pi Calculus, In Proceedings of 13th European Symposium on Programming (ESOP 2004), Barcelona, Spain, March 29-April 2, 2004.

K. Sowmyadevi and T. V. Jenitha, Detect DDoS Attack Using Border Gateways and Edge Routers, International Journal of Computer Applications, Vol. 42, No. 9, 2012, pp. 9-13.

B. B. Gupta, R. C. Joshi, and M. Misra, ANN Based Scheme to Predict Number of Zombies in a DDoS Attack, International Journal of Network Security, Vol. 14, No. 2, 2012, pp. 61-70.

Rui Jiang is now an associate professor at Southeast University, China. He received his Ph D degree at Shanghai Jiaotong University, Shanghai, China in 2005. His current research interests include secure analysis and design of communication protocols, secure mobile cloud computing, secure network and systems communications, mobile voice end-to-end secure communications, and applied cryptography.

Bharat Bhargava a professor of computer science at Purdue University. He is conducting research in security and privacy issues in distributed systems and sensor networks. This involves identity management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. His recent work involves attack graphs for collaborative attacks. Prof. Bhargava has won five best paper awards in addition to the technical achievement award and golden core award from IEEE, and is a fellow of IEEE. He received Outstanding Instructor Awards from the Purdue chapter of the ACM in 1996 and 1998. He has graduated the largest number of Ph.D students in CS department and is active in supporting/mentoring minority students. In 2003, he was inducted in the Purdue's Book of Great Teachers. He has graduated the largest number of women Ph.D students and the first African American student Ph.D in CS department. He is editor-in-chief of three journals and serves on over ten editorial boards of international journals. Professor Bhargava is the founder of the IEEE Symposium on Reliable and Distributed Systems, IEEE conference on Digital Library, and the ACM Conference on Information and Knowledge Management. Bhargava has worked extensively at research laboratories of Air Force and Naval. He has successfully completed several Darpa and Navy STTR proposals. He is working with General Motor Corporation in analyzing use of sensors in cars and other vehicle. He has organized an NSF workshop on V2V wireless network.