ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

ROLE OF DENIAL- OF –SERVICE IN NETWORK SECURITY

Madhava Reddy. CH[1], Srinath Reddy. N[2], Sunil kumar. V.V[3]

Associate Professor, Visvodaya Engineering College, Kavali[1]

Associate Professor, Visvodaya Engineering College, Kavali[2]

Associate Professor, PBRVITS, Kavali[3]

Abstract: We know that in network systems it is not possible to avoid Denial-of-Service attacks. Denial-of-Service attacks will play important role on security as well as on through put. As Security has their own vulnerability to DoS, this paper studies how to avoid the risk of DoS in security and through put. In this context, we begin building attacker capabilities and a basic network to model the actual protocol operation. Secondly we build an advanced model for evaluation of the risk. After defining the intruder capability with a basic model, the risk evaluation model gives the "Risk-Evolution-Factor" (REF) for the Security and through put. The "Risk- Evolution-Factor" is going to presents the amount of computing resources is expected to lose with a specified level of confidence in security and through put. This model can help end users to have a good understanding of the protocols structures, what they are using, and in addition to that provide help developers and designers to examine their developments and designs and get hints to improve the same.

Keywords: DoS, REF, Ad-hoc networks, IKE

I. INTRODUCTION

Significant progress has been made in securing ad hoc networks via the development of secure routing protocols. Moreover, ensuring resilience to misbehaviour and denial-of-service attacks has also been the focus of significant research efforts as such resilience is a critical component of a secure system. Denial-of-Service (DoS) attacks are any malicious actions that degrade networks' intended service to legitimate users. They are threatening both the Internet and resource-constrained ad-hoc sensor networks. One of the most common and devastating types of DoS attack is the resource exhaustion attack, in which an attacker, by initiating a large number of instances of a protocol, causes the victim to deplete resource. These DoS attacks are usually carried out by intruders taking advantage of the vulnerabilities of the protocol that intends to establish or authenticate communications following up. As a result, defences against Denial -of - Service attacks have been built into the Security as much as possible.

Security protocol is an important component of network security. Before data communications between any network entities, a security protocol is executed for entity authentication, key agreement and secure associations establishment. For example, Internet Key Exchange (IKE) protocol uses shared secrets or public key schemes to authenticate the protocol initiator to avoid flooding of unwanted traffics.

After establishing connections, Security can be used to provide data confidentiality and non-repudiation service. For instance, SPINS[1] is proposed for the secure communication in resource-constrained sensor networks, without which the sensor nodes are highly vulnerable to flooding-based DoS attacks. Actually Security are used everywhere in the current Internet and emerging networks; they are widely used for key agreement, entity authentication and secure data transportation. However Security sometimes have DoS vulnerability themselves, because some verification involves resource consuming computations which may cause victims to be exhaustive of resources. Consequently, protocol designers should be alert to this problem and make their protocols robust to DoS attacks.

As Security have their own vulnerability to DoS, it is desirable to evaluate the resilience of Security to DoS attacks. As a saying goes: if you cannot evaluate it, you cannot improve it. Not until we can express in numbers what we are speaking about is our knowledge of something becoming satisfactory. The security protocol is no exception. Although formal methods[2] have achieved great success during the last two decades in evaluating whether or not Security satisfy their security goals, little effort has been made for the risk evaluation of DoS vulnerabilities in Security, the circumstance of which makes the problem of DoS risk evaluation important and urgent.

With protocol analysis, we can only find out certain potential vulnerabilities of a protocol, namely what kind of attackers under what kind of circumstance can intrude the system. Existing studies on DoS Role assessment[3] also focus on the problem of "how many resources are lost or how much the system endures during a certain DoS attack".

But the existence of various forms of attacks complicates this problem. Suppose protocol *PA* performs better than protocol *PB* under a certain attack, but *PA* performs worse than *PB* under another attack. Current studies on DoS Role assessment cannot compare the overall performance of these two protocols. Actually we would like to know how Security perform overall under various attack models, so we introduce risk evaluation of Security in this paper. The notion of risk tries to encapsulate the overall performance of a certain event by evaluating its "uncertainty of outcome". For Security, risk is the uncertainty for them to protect the system. Even with the cost based framework alone proposed by Meadows[4-5], it is difficult to evaluate the risk of protocols. As the first step towards risk evaluation of Security, this study evaluates the risk of Security by introducing a probability model characterizing the likelihood of those security threats turning into realistic losses. Drawing an analogy to the financial risk evaluation model, the risk metric used in this model is called "Risk-Factor"[6] (RF) . In financial risk evaluation, RF aggregates all the risks into a *single number* representing how much money is "at risk" with a given confidence, while in our model, RF of Security characterizes how much computing resources are expected to lose with a given level of confidence. This risk evaluation model indicates the robustness of the protocol to Denial-of - Service attacks and can help designers to make their protocols more effective.

The contributions of this paper can be summarized as follows.

A. A modeling framework is specified for the risk evaluation of Denial-of-Service vulnerabilities in Security. To the best of our knowledge, this is the first model towards the risk evaluation of Security.

B. The risk metric "Risk-Factor" (RF) is defined to evaluate DoS resilience in Security, which represents how much computation resource is "at risk" with a given confidence. An algorithm for the computation of RF in Security is presented as well.

The rest of this paper is organized as follows. In Section II we elaborate on the motivation of this paper. Related work is defined in Section III. The system model of DoS risk evaluation is specified in Section IV. We conclude this paper in Section V.

II. Motivation

We will elaborate on the motivation of our work in this Section before going on to introduce the proposed economical model. We will explain why existing studies on both DoS assessment and security analysis do not fit with on-going requirement of understanding Security. As we have analyzed above, work on DoS assessment would give us a security evaluation for one particular attack model, but cannot give us an overall evaluation of Security under various attacks.

Risk evaluation, as a synthetic metric, can reflect the overall performance of the protocol under various attack models. Formal analysis of protocols, on the other side, although achieving great success during the last two decades, has been carried out from experts' perspective, and it fails to contribute much to the understanding of common protocol customers who have little knowledge of cryptography and information security. For instance, after a formal analysis tool is applied to the protocol, the experts can tell to some extend whether or not the protocol is vulnerable to certain kind of attacks, but for customers who have no idea of protocol analysis, it is really hard for them to understand whether it is proper to use this protocol. That is to say, common customers do not benefit from the protocol analysis directly. It is an implication that we should bridge the gap between the analysis result and common customers' understanding.

Risk evaluation is the very methodology to bridge this gap. The concept of risk evaluation has undergone a long history. Bernstein[7] asserted that the revolutionary idea that defined the boundary between modern times and the past is the mastery of risk. Risk evaluation helps us to put into practicewhat is known as sustainable development, which means we can make a good living when what we have prepared for potential hazards is sufficient for the expected losses. For DoS attacks, risk evaluation of Security can tell us how much is exposed to DoS attacks with a given level of confidence, and this evaluation result will help common customers a lot.

As for Security, let us settle down to reflect what is required from common customers' perspective. Common customers always want everything set up as simple as possible with the help of protocol analysis. For instance, they do not want to know what kind of attacks can be potentially dangerous, but they care about how many computation resources are exposed to these attacks; they are reluctant to understand why this protocol is better than others, but they are curious about how much one protocol will behave more securely and robustly than the others. Risk evaluation of Security meets this requirement quite well: common customers can figure out the expected losses if they chose to use the protocol, and they can easily compare different protocols with the risk evaluation results.

The same story goes for the companies. The boss, who has been reading about derivatives which potentially suffer from losses, wants to know just how much market risk the company is taking in the company's foreign exchange. Many years passed before we can start the best answer that "The Risk-Factor is . . .". In a nutshell, Risk-Factor (RF) aggregates all of the risks in the portfolio into a *single number* suitable for use in the boardroom, report to regulators, or disclosure in an annual report. For instance, RF can answer the very question that "What is the most the entity can, say with a 95% or 99% level of confidence, expect to lose in dollars over the next month". As an effective risk evaluation method, RF has been standardized by the Basel Committee on Banking Supervision [6].

The success of Risk-Factor in financial community has inspired many researches in applying it to the risk management of computer and networking systems [8-9]. But the community has not yet laid out the evaluation of the DoS vulnerability in Security. This paper is dedicated to proposing an economical model based on Risk-Factor to evaluate the risk of Denial-of-Service in Security. The evaluation result will benefit both common users and protocol designers. With the proposed model, common users can be aware of the risk of their protocols: what is expected to lose in their computing resources or anything else with a certain level of confidence. Taking advantage of this evaluation model, protocol designers and analysts can evaluate the resilience of their protocols to Denial -of-Service attacks, and get clues as how to make their designs better.

III. Related Work

Hamdi and Boudriga[10] gave a survey on the theory, challenges and countermeasures of computer and network security management. They reviewed the well-known risk management approaches and some shortcomings of the existing methodologies. They also set out common requirements that must be respected by any risk management frameworks, among which cost estimation and attack modeling requirements are covered. For DoS defense in networking system, both protocol level such as Client Puzzle[11] and architecture level approaches[12] are used. Yang *et al.*[12] proposed a capability-based DoS limiting architecture to allow the destination to control the packets they receive which touches the heart of DoS problem. As for DoS risk management, a lot of researches fall into the category of measuring and quantifying DoS Role[3,13-14], which are dedicated to measuring the Role of DoS attacks. In addition, a personalized trust model with risk evaluation [15] is proposed for P2P system, in which risk evaluation is used to reflect the short-term behaviour of peers.

On the DoS evaluation of Security, a cost-based framework for analyzing vulnerabilities to network DoS attacks in protocols was proposed by Meadows first in [4] and then refined in [5]. Taking advantage of this evaluation framework, the protocol designer specifies a tolerance relationship and tells whether the protocol's resilience to DoS is within its tolerance. The tolerance relation matrix describes how much effort he or she believes it should be necessary to expend against an attacker of given strength. Smith[16] applied Meadows' framework to analyze an Internet key agreement protocol. It was the first direct application of the cost framework, but it lacked any awareness of risk analysis.

The above analyzed researches have shed light on the evaluation of DoS vulnerabilities in protocols from a specific perspective. They can answer the question of how much to lose under a certain DoS attack, however, they are not able to evaluate the protocol's DoS vulnerability overall with the existence of all kinds of attacks. Comparatively, the notion of "risk" captures the overall performance of a protocol under DoS attacks. In this work we study how to evaluate the risk of DoS in Security. By characterizing the attackers with a probability model, this paper specifies how to evaluate the risk of DoS vulnerabilities in Security, which is indicated by the Risk Factor (RF), a widely accepted approach in financial risk management. Although proposed in financial community, RF is not a new comer for computer scientists and engineers.

Kleban and Clearwater did the first job employing the idea of RF to evaluate the risk of computer systems[8 -9], however, little effort has been made to apply RF to the risk evaluation of Security since then. Risk-Factor has a solid mathematical foundation and has achieved a great success in financial risk evaluation. As a result, we adopt the idea of *Risk Factor* to evaluate the risk of DoS attacks in Security in this paper.

IV. System Model

In this Section, we will introduce the risk evaluation model for Security. The specification used in our analysis is introduced first, after which the risk evaluation model based on Risk-Factor is specified.\

A. Protocol Specification

The specifications used in our model is the same as what is specified in [5]. The popular Alice-and-Bob specification of Security will be used throughout the whole paper.

Definition 1 (Alice-and-Bob Specification). *An Alice -and - Bob specification is a sequence of statements of the form A B : M where A and B are processes and M is a message.*

Annotated Alice-and-Bob specification style, which is the basis of some high level protocol description languages, includes message processing steps at both the protocol initiator and responder, as defined below.

Definition 2 (Annotated Alice-and-Bob Specification). *An annotated Alice -and- Bob specification is a sequence of statements of the form A B : $T_1, . . . , T_k \parallel M \parallel O_1, . . . , O_n$.*

The sequence $T_1, . . . , T_k$ represents the sequence of operations performed by A in producing message M, while the sequence $O_1, . . . , O_n$ represents the sequence of operations performed by B in processing and verifying M. More closely, study of each line leads to the definition of event.

Definition 3 (Protocol Event). *Let $L = A \quad B : T_1, . . . , T_k \parallel M \parallel O_1, . . . , O_n$ be a line in an annotated Alice- and-Bob specification. We say that X is an event occurring in L if*

1) *X is one of the T_i or O_i, or*
2) *X is "A sends M to B" or "B receives M from A".*

There are two kinds of events: *normal events* and *verification events*. Normal events (e.g., signature generation) occur at either sender or receiver, and have only one outcome: success, while verification events occur (e.g., signature verification) only at the receiver, and can come out with success or failure. To describe the responder *B*'s intention to proceed with the protocol after successfully verifying a message, an *accept event* is attached to the end of each line.

B. Intruder Capability and Its Probability Distribution

This subsection models protocol intruders by the definitions of intruder capability and its probability distribution function.

Definition 4 (Intruder Action and Capability). We define an intruder action as an event engaged by an intruder that affects messages received by legitimate participants in a protocol. We define an intruder capability as a set of actions available to an intruder, partially ordered by set inclusion.

Examples of intruder capability would include such cases as an intruder who could send messages but not read messages that were not addressed to it, an intruder who can impersonalize as the other entities, an intruder who can generate valid time stamp for establishing communications, and an intruder who can generate valid signatures of legitimate participants.

Intruder capability characterizes the intruders' ability to persuade one participant of the protocol to consume resources participating in the protocol. Because different kinds of intruders distribute with different probabilities, we are going to introduce the definition of *Intruder Capability Probability Distribution Function* which characterizes the probability of intruders with different capabilities.

Definition 5 (Intruder Capability Probability Distribution).

Let be an Intruder Capability Probability Distribution

Function from the set of intruder capability to an probability value within [0, 1].

This function describes the probability distribution of intruders' capability. We assume that the more powerful the capability is, the less possible that intruders will own the capability. For example, the "packet sending" capability is perhaps the least powerful capability for an attacker, so each adversary can launch attacks by sending packets to a victim, i.e., (Packet Sending) = 1. On the contrary, the capability of cheating into the system by "forging authentication tokens" is much more difficult to get, so the possibility for the attacker to get this capability is relatively less. Related work[17] also made similar assumptions on attacker skill level distribution that fewer attackers own higher level attacking skills. Thus this is a reasonable assumption in this model.

We can also get the combined probability of an attacker with multiple capabilities. For example, if we can divide the intruder capabilities into n different sets, and the probability of intruders who have capability IC_i is p_i, i.e., $(IC_i) = p_i$,

$P(intruder\ ICS_i) = p_i$, for $i = 1, \ldots, n$. Assuming that n events of owning capability $IC_1, \ldots, IC_n$ are all independent, the probability of intruders who have only capabilities of $IC_1, \ldots, IC_k$ is $p_1 p_2 \ldots p_k(1\ p_{k+1}) \ldots (1\ p_n)$ (where ICS_i denotes the set including all the intruders that own capability IC_i).

Practically owning capability of different capabilities sometimes is not all independent. We can release this assumption using conditional probability deduction. The probability of owning capability $C_1, \ldots, C_k$ can be obtained as: $P(C_1C_2 \ldots C_k) = P(C_1)P(C_2|C_1)P(C_3|C_1C_2) \ldots P(C_k|C_1C_2 \ldots C_{k\ 1})$. Setting up the probability model of intruder capability is a crucial process for our risk evaluation model. As attackers with different capabilities can persuade the victim to stop at different steps of the protocol and thus consuming different amount of computation resource under DoS attacks, we can obtain the definition of the probability distribution of DoS loss after the cost set and the protocol engagement cost are defined.

C. Cost Set and Protocol Engagement Cost

In this subsection, we will study into the cost of participating in the security protocol which includes the cost of event execution, the cost of message acceptance and the cost of protocol engagement.

Definition 6 (Cost Set). *A cost set C is a partially ordered set with partial order < together with a function + from C ×C to C such that + is associative and commutative, and* $x + y\ \max(x, y)$, *along with a zero element* 0 *such that* $x = 0 + x = x + 0$, *for all x in C.*

An example of cost set would be the set including all the positive integers with 0 as the zero element, and the common addition function as the + function, and partially ordered by "less than" (<).

Definition 7 (Event Cost Function). *A function from the set of events defined by an annotated Alice -and-Bob specification to a cost set C which is* 0 *on the accept events is called an event cost function.*

Note that the cost of a verification event is expected to express the expense of performing the verification, and the cost of sending a message is expected to express the expense of preparing that message.

Definition 8 (Message Acceptance Cost Function) . *Let P be an annotated Alice-and-Bob protocol, C a cost set, and an event cost function defined on P and C.*

We define the message acceptance cost function associated with to be the function ' on events following the receipt of a message as follows.

If the line A B : $O_1, \ldots, O_k \,||M||\, V_1, \ldots, V_n$
appears in P, then for each event V_j *:*
$'(V_j) = (V_1) + \cdots + (V_j)$.

The message acceptance cost function specifies the cost of processing messages up to reaching a failed verification event. Meadows[4-5] went on to introduce protocol engagement cost based on event cost function and message acceptance cost function. But Meadows' protocol engagement cost function is only defined on accept events. We extend the definition of protocol engagement cost to include all the valid events occurring at the defender of the protocol.

Definition 9 (Protocol Engagement Cost Function). *We define the protocol engagement cost function associated with to be the function defined on all the events as follows.*

For each event Vm in line A B : $O_1, \ldots O_k \,||M||\, V_1, \ldots, V_n$:

1) *If V_m is not an accept event, then (V_m) is the sum of the costs of all operations occurring at B desirably-preceding V_m plus the cost of V_m (i.e., (V_m)).*
2) *If V_m is an accept event and there are no lines B X : $O'_1, \ldots, O'_k, \| M' \| V_1', \ldots, V_n'$, then ($V_m$) is the sum of all the costs of all operations occurring at B desirably-preceding V_m.*
3) *If V_m is an accept event and there is a line B X : O'_1, . . . , $O'_k, \| M' \| V_1', \ldots, V_n'$, then ($V_m$) is the sum of the costs of all operations occurring at B desirably-preceding V_m plus the sum of the costs of the O_i' ((O_1') + · · · + (O_k')).*

Note as well the notion of *desirably-precede* is the same as what is defined in [4]. This protocol engagement cost reflects one of the most common ways in which Denial-of-Service attacks can proceed: to persuade a principal to waste resources participating in a bogus instance of the protocol. The more capable the intruder is, the more steps the victim will be persuaded to take in the protocol. As a result, the protocol engagement cost represents the victim's loss under Denial-of-Service attacks.

D. DoS Loss Probability Distribution

Before defining the DoS Loss Probability Distribution, we give the definition of *fail point*, which characterizes the failure model of Security. The participant stops participating in the protocol until it reaches a fail point, where the verification event comes out unsuccessfully.

Definition 10 (Fail Point). *A fail point P is a pair (L,E) denoting the place where the protocol will fail in verification at event E in line L.*

If the responder of the protocol fails in the verification of the first event in the first message, we say it fails at point *P*(*L*1,*E*1);
if the responder proceeds to participate in the protocol until the last event in the last message, we say it fails at the last accept event because the cost of accept event is zero ((*accept event*) = 0). We will use *P.E* to denote the event in fail point *P*.

Definition 11 (Intruder Fail Point Function). *A function defined from the set of intruder's capabilities to the set of fail points is called Intruder Fail Point Function.*

Definition 12 (DoS Loss). *The loss under Denialof-Service attacks L_{DoS} is defined as the sum of the costs of all operations occurring at the principal participating in the protocol until it fails at a point P(L,E).*

If an intruder with capability *IC i* persuades the responder to participate in the protocol until the responder fails at point $P_i(L,E)$, the *intruder fail point function* maps IC_i to a fail point *Pi*, i.e., (IC_i) = *Pi*, and the DoS Loss of the defender is ((IC_i).*E*), i.e., L_{DoS} = ((IC_i).*E*).

Since we have all the definitions above, we arrive at the very point to figure out the DoS Loss Probability Distribution as follows.

Definition 13 (DoS Loss Probability Distribution Function). *The DoS Loss Probability Distribution Function is defined from the set of DoS Loss (L_{DoS}) to a probability value within* [0, 1].

Assume there are *n* different intruder capabilities IC_i, IC_2, . . . , IC_n with the probability of (IC_1), (IC_2), . . . , (IC_n), respectively. Intruders with those *n* capabilities can persuade the legitimate entity to participate in the protocol until failing at points (IC_1), (IC_2), . . . , (IC_n), respectively. The DoS Loss Probability Distribution is computed as follows.

$Pr(L_{\text{DoS}} = loss) = {}_{i=1,\ldots,n} \{ (IC_i) | ((IC_i) .E) = loss\}$ (1) Since we have arrived at the probability distribution of DoS losses, we can take Risk -Factor as the method to evaluate the risk of Denial-of-Service in Security.

E. Risk Evaluation with RF

Before giving the RF definition of DoS risk in Security, we should recall the definition of RF in financial language.

Definition 14 (Risk-Factor). Using a probability of percent and holding period of t days, an entity's Risk-Factor is the loss that is expected to be exceeded with a probability of only percent during the next t-day holding period.

Mathematically, RF is the -quantile of the Probality & Loss (P & L) distribution, i.e., it satisfies the relation:

Pr(( ) RF) = (2) where we assume that the P&L distribution is a continuous and strictly monotone function, and both ( ) (the financial loss function) and RF are the absolute value of loss.

There are two key factors in the definition of RF: the loss probability and the time interval t. The choice of probability is determined primarily by how the designer and/or user of the risk management system wants to interpret the Value-at-Risk: an "abnormal" loss that occurs with a probability of . This means the probability of loss greater than RF will be less than . Because the risk of financial markets highly correlates with the holding time, the time interval t cannot be neglected. But when we are evaluating the risk of DoS attacks in Security, the holding time is not inevitable, for the vulnerabilities in Security do not vary with respect to time.

Now that we have recalled the definition of RF in financial language, we are ready for the definition of RF for DoS vulnerabilities in the language of Security.

Because the loss under Denial -of-Service attacks in our model is discretely distributed, the definition of RF should be modified to accommodate the discretely distributed variables.

Definition 15 (Risk-Factor for DoS). Using a probability of , an entity's Risk-Factor is the maximum of the DoS loss value that is expected to be exceeded with a probability equal to or greater than .

Mathematically, RF is the value satisfying the relation:

RF = max Li s.t. Pr(LDoS Li) (3)

where L1, L2, . . . , Ln are the n discretely distributed loss values with probabilities (L1), (L2), . . . , (Ln).

Based on this definition of RF in Security, we give an algorithm for the computation of RF value as Algorithm 1. In Algorithm 1, we find a value i with the probability of DoS loss greater than Li is less than the predefined confidence . At the beginning, we sort L1, . . ., Ln so that Li Lj for every i < j. RF value is initialized to infinity and i is assigned n. Then Pr, the sum of the probability of DoS loss greater than Li is figured out. If Pr is greater than , the algorithm returns Li, and otherwise i is decreased by 1 and back to the loop.

```
Algorithm 1. RF
Computation Input: L1, . . .
,Ln, Output: RF value
sort(L1, L2, . . . , Ln) so that Li < Li+1; for
i = n to 1 do
          Pr     0;
for j = i to n do
Pr                Pr +  (Lj)
end
if Pr                   then
RF    =    Li;
return     RF
end
end
```

Definition 16. For the same probability , the less the RF value computed in our evaluation model is, the stronger the protocol is resistant to Denial-of-Service attacks.

Because RF is the absolute value for the risk of the protocol under Denial -of-Service attacks, the less the risk, the stronger the protocol is resistant to Denial of-Service attacks. As a result, Definition 16 is self-evident.

We summarize the procedure of risk evaluation for security protocol with the proposed model as follows.

1. Use the annotated Alice-and-Bob specifications to describe the security protocol we want to analyse.

2. Choose a Cost Set C and specify an event cost function for each event in the annotated Alice-and-Bob specifications.

3. Following the second step, go on to figure out the message acceptance function _ and protocol engagement cost function for each event occurring at the defender.

4. Analyse the intruders. Specify all the intruder capabilities that threat the protocol and give the intruder capability probability distribution function .

5. For each intruder capability, determine the fail point where the intruders with this capability will fail at participating the protocol, then we get the intruder fail point function .

6. Figure out the DoS Loss Probability Distribution Function from (1).

7. Choose a probability value , and take Algorithm 1 to figure out the RF.

8. Use the RF to evaluate the protocol: compare with other protocols or tell whether the system can survive under such a risk.

Since we have defined the economical model for the risk evaluation of Security based on Risk Factor, we are ready to apply the model to existing protocols to validate its applicability.

V. Conclusion

An economical model has been proposed to evaluate the DoS risk in Security. The risk metric "Risk-Factor (RF)" is defined and used for risk evaluation. "RF" represents how much computation resource is "at risk" with a certain level of confidence, which aggregates all the potential risk into a simple number to analyze and compare performance of different protocols. Using the proposed model, we have identified a DoS vulnerability in a key agreement protocol used in sensor networks and get clues to enhancing its resilience. The applicability and effectiveness of the proposed model is further validated by applying it to analyzing two public key based authentication protocols.

We have also implemented the protocols and simulated them in the network simulator. Simulation results are consistent with the analytic results using our model. Future work includes further investigation of the applicabilities of the proposed model and incorporating different attack models to extend the current risk evaluation model.

REFERENCES

[1] Perrig A, Szewczyk R, Wen V et al. SPINS: Security for sensor networks. In Proc. the Seventh Annual International Conference on Mobile Computing and Networks (MobiCOM 2001), Rome, Italy, July 16-21, 2001, pp.189-199.

[2] Meadows C. Formal methods for cryptographic protocol analysis: Emerging issues and trends. IEEE Journal on Selected Areas in Communications, 2003, 21(1): 44-54.

[3] Mirkovic J, Reiher P L, Fahmy S, Thomas R K, Hussain A, Schwab S, Ko C. Measuring denial of service. In Proc. the 2nd ACM Workshop on Quality of Protection, Alexandria, USA, October 30, 2006, pp.53-58.

[4] Meadows C. A formal framework and evaluation method for network denial of service. In Proc. the 12th IEEE Computer Security Foundations Workshop (CSFW 1999), Mordano, Italy, June 28-30, 1999, pp.4-13.

[5] Meadows C. A cost-based framework for analysis of denial of service networks. Journal of Computer Security, 2001, 9(1): 143-164.

[6] Holton G A. Value-at-Risk Theory and Practice. Elsevier, 2003.

[7] Bernstein P. Against the Gods: The Remarkable Story of Risk. John Wiley and Sons Inc, 1996.

[8] Kleban S, Clearwater S. Computation-at-risk: Assessing job portfolio management risk on clusters. In Proc. the 18th International Parallel and Distributed Processing Symposium (IPDPS 2004), Santa Fe, USA, April 26-30, 2004, pp.254-260.

[9] Kleban S, Clearwater S. Computation-at-risk: Employing the grid for computational risk management. In Proc. 2004 IEEE International Conference on Cluster Computing (CLUSTER 2004), San Diego, USA, September 20-23, 2004, pp.347-352.

[10] Hamdi M, Boudriga N. Computer and network security risk management: Theory, challenges, and countermeasures. International Journal of Communication Systems, 2005, 18(8): 763-793.

[11] Aura T, Nikander P, Leiwo J. Dos-resistant authentication with client puzzles. In Revised Papers, 8th International Workshop on Security, London, UK, 2001, pp.170-177.

[12] Yang X, Wetherall D, Anderson T E. A dos-limiting network architecture. In Proc. the ACM SIGCOMM 2005 Conference on Applications, Technologies, Architectures, and Protocol for Computer Communications, Philadelphia, USA, August 22-26, 2005, pp.241-252.

[13] Mirkovic J, Hussain A, Fahmy S, Reiher P L, Thomas R K. Accurately measuring denial of service in simulation and testbed experiments. IEEE Trans. Dependable Sec. Comput., 2009, 6(2): 81-95.

[14] Chen Y, Bargteil A, Bindel D, Katz R H, Kubiatowicz J. Quantifying network denial of service: A location service case study. In Proc. the 3rd Int. Conf. Information and Communications Security, Xian, China, Nov. 13-16, 2001, pp.340- 351.

[15] Liang Z, Shi W. Pet: A personalized trust model with reputation and risk evaluation for P2P resource sharing. In Proc. the 38th Hawaii International Conference on System Sciences(HICSS 2005), Big Island, USA, January 3-6, 2005, pp.1-10.

[16] Smith J, Nieto J M G, Boyd C. Modelling denial of service attacks on JFK with meadows's cost-based framework. In Proc. the Fourth Australasian Symposium on Grid Computing and e-Research (AusGrid 2006) and the Fourth Australasian Information Security Workshop (Network Security) (AISW 2006), Hobart, Tasmania, Australia, January 2006, pp.125-134.

[17] Paulauskas N, Garsva E. Attacker skill level distribution estimation in the system mean time-to-compromise. In Proc. the 1st IEEE International Conference on Information Technology (IT 2008), Gdansk, Poland, May 19-21, 2008, pp.1-4.