This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Detection of Resource-Drained Attacks on SIP-Based Wireless VoIP Networks

Jin Tang, Yong Hao, Yu Cheng and Chi Zhou
Department of Electrical and Computer Engineering
Illinois Institute of Technology, Chicago, IL, USA 60616
Email: {jtang9, yhao4, cheng, zhou}@iit.edu

***Abstract*—The Session Initiation Protocol (SIP) has been widely used in VoIP for session control and management. As the basic SIP specifications do not require the proxy servers to track the states of established sessions, an extension header field "Session-Expires" has been proposed for SIP to allow the proxy server to hold resources for established sessions just within the specified periods. In this paper, we identify a novel denial of service (DoS) attack utilizing this SIP extension to drain resources of the proxy servers in wireless VoIP. In particular, by deliberately setting a large value of the "Session-Expires" header and then physically disconnecting from the wireless network, attackers can repeatedly hold resources of the proxy server as long as they want. Also, the low-volume nature of the attack allows it to avoid being detected by existing volume-based intrusion detection systems. As a counter-measure, we propose a robust detection scheme based on the statistical Anderson-Darling test. The key insight that leads to the scheme is the changed statistical property of the header values induced by the attack. We validate the performance through computer simulation. The scheme shows its ability to detect the attack and is even more effective when applied against the distributed denial of service (DDoS) attack.**

I. Introduction

Voice over IP (VoIP) has emerged as a prevailing Internet application recently. At the same time, the deployment of wireless networks such as the IEEE 802.11 WLANs is dramatically increasing over the years. The convergence of such two trends, VoIP over wireless networks, leads to a promising all-IP platform paradigm to provision economical high-quality voice services to mobile users anytime and anywhere, which has drawn more and more interest from both academia and industry. The Session Initiation Protocol (SIP) [1] has been widely used in VoIP as the signaling protocol to control and manage sessions. However, as SIP defines open-ended control message implementation, users are able to modify the values of some SIP headers as they like. This brings security concerns of the VoIP networks, especially in a more vulnerable wireless context. In this work, we identify a resource-drained denial of service (DoS) attack that takes advantage of the vulnerabilities of SIP and wireless networks, and propose a robust detection scheme based on the statistical Anderson-Darling test.

The basic SIP specifications do not require the proxy servers to track states for established sessions, thus a basic proxy server is not able to determine whether a session is alive or dead after it is established. As a result, the server will even hold resources reserved for failed sessions. To address this problem, an extension header field "Session-Expires", namely the session timer [2] has been proposed for SIP to serve as a keep-alive mechanism. It allows the proxy server to keep resources for established sessions just as long as the specified session timers if the sessions are not explicitly terminated by BYE messages. In normal situation, the "Session-Expires" header is used by SIP user agents to inform the proxy server the session durations. The proxy server will then assign resource for the session according to the specified amount of time. However, by utilizing this fact, an attacker can set an arbitrarily large value for the header and keep holding resource in the proxy server until the session timer expires. Also, because it is in wireless networks, the attacker can easily disconnect from the network and still hold resources on the proxy. By simply repeating the actions above, an attacker is able to gradually drain the resources on a proxy server and cause denial of service (DoS) to other normal users. The attack requests are sent to the proxy server following regular traffic rates, thus they can hardly be detected by existing volume-based intrusion detection systems. More severely, the attacks can cause even greater harm if they are initiated from distributed sources on a wireless VoIP network, i.e. the DDoS attack. In this case, resources of the SIP proxy servers will be drained at a much faster pace.

As a counter-measure, we propose a detection scheme for the resource-drained attack based on the statistical Anderson-Darling test [3], [4] through investigating the characteristics of both the normal and attack behaviors. The "Session-Expires" header conveys the duration of the session and there is no default value defined for the header [2]. Thus the header value can be modeled as a random variable which has the same distribution of the session holding times. According to existing research, the holding times of VoIP sessions closely follow a log-normal distribution to reflect the long tail characteristic [5]. Therefore the distribution of the "Session-Expires" header values should also have a log-normal distribution in normal situation. Attackers set arbitrarily long values for the session timers to maximize the attack effect. Although unpredictable, their behavior is still very likely to introduce deviation from the log-normal distribution of the session timers in normal situation. From this insight, we build our detection scheme based on one of the most powerful tools in normality test, the Anderson-Darling test. We monitor the session timer values from the whole wireless VoIP network as the input of the scheme. Specified parameter values of the session timer dis-

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

tribution are not required due to the strength of the Anderson-Darling test. The scheme is robust against any attacks deviating from the normal behavior. And the DDoS attacks are even easier to be detected as they will induce more significant deviation from the normal session timer distribution.

In summary, the paper has contributions in three aspects. 1) We identify a novel DoS attack which utilizes vulnerabilities of SIP and wireless networks. The low-volume attack can gradually drain resources on the proxy servers and avoid detection from existing volume-based intrusion detection systems. 2) We propose a robust detection scheme based on the Anderson-Darling test through investigating the statistical properties of both normal and attack traffic. The scheme can effectively detect the resource-drained attack, especially the DDoS attack. 3) Computer simulation is conducted to validate the performance of the proposed scheme in terms of the number of samples needed to reach the detection decision.

The remainder of the paper is organized as follows. Section II reviews related work. Section III describes the novel resource-drained attack. Section IV presents the proposed attack detection scheme. In Section V, computer simulation results are presented to validate the performance of the scheme. The conclusion remark is given in Section VI.

II. Related Work

The "Session-Expires" extension header is proposed in RFC 4028 [2] as a keep-alive mechanism for SIP. In the "security considerations" section of the RFC, only attacks through setting very small session timers are addressed, where an attacker may force compliant user agents to frequently send session refreshes at a rapid rate. The RFC proposed a 422 (Session Interval Too Small) response to reject the attacker's request if the timer is smaller than the value specified in the "Min-SE" header. However, there is no enforcement of how large the session timer can be and we identify a novel resource-drained attack by utilizing this fact. Also, the victim of our identified attack is the SIP proxy server rather than the user agents as considered in the RFC.

Surveys of the DoS attacks in VoIP can be found in [6]–[8]. The SIP flooding attack is one of the major threats because it is easy to launch and capable of quickly overloading both the network and nodes. However, existing work such as [9], [10] can efficiently detect the attack.

The attack utilizing the open-ended implementation of SIP is another major problem on VoIP networks [8]. Attackers modify SIP header values and excessively consume processing capability of SIP nodes. The attack identified in this paper belongs to this category. We propose a detection scheme based on the statistical Anderson-Darling test to deal with the attack.

III. Resource-Drained Attacks on Wireless VoIP Networks

A. SIP Basic and the "Session-Expires" Extension

VoIP utilizes SIP as a signaling protocol to set up, manage and tear down communication sessions. Three basic components are identified in a SIP environment, which are User Agent Client (UAC), User Agent Server (UAS) and SIP proxy server. Messages are exchanged between these components to perform ordinary SIP operations. As shown in Figure 1, the SIP messages used to set up and tear down sessions are basically INVITE, 200 OK, ACK and BYE. UAC initiates a SIP session by sending out the INVITE. Intermediate proxies look over the destination SIP address encoded in the message and forward it to UAS who will respond with a 200 OK. An ACK message then finishes the three-way handshake to establish the session and media will go directly between UAC and UAS. When the session is finished, it will be terminated by a BYE message from either of the calling parties.

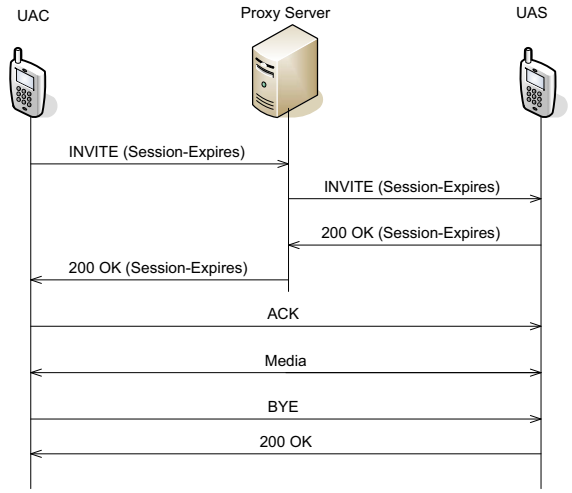

Fig. 1. Illustration of SIP signaling.

The basic SIP as described above does not require the proxy servers to track states for already established sessions. The result is that the proxy servers are not able to determine whether a session is alive or dead. If a session fails without sending a BYE message, the proxy server will retain its reserved resource and have no way to release it. To resolve this issue, a SIP extension header field "Session-Expires" [2], or also called session timer is proposed as a keep-alive mechanism. When initiating a session, a UAC specifies its desired session duration through this timer included in the first INVITE message. Both the proxy server and UAS will agree with this timer if it is not too small through the handshake as in Figure 1. The proxy server reserves resource for this session according to the timer. The resource will be released after the session timer expires or can be refreshed with a SIP UPDATE message. The UPDATE is not discussed in this paper as attackers disconnect from the network almost right after the session has been established and are unlikely to use the refreshing mechanism.

B. Resource-Drained Attacks on Wireless VoIP

SIP provides open-ended control message implementation to allow including additional capabilities to enhance itself over time, e.g., the "Session-Expires" extension as described above. However, one negative impact of such an open design is that

it provides opportunities for attackers to understand the new implementation and take advantage of its vulnerabilities to initiate attacks.

In normal situation, the session timer is utilized by SIP user agents to convey the durations of the sessions to the proxy server. But according to the standard of this SIP extension [2], only the minimum value for the timer is defined by the header "Min-SE". As a result, since no maximum value is enforced, an attacker can manipulate the session timer and specify its duration as long as he wants in the SIP INVITE messages to initiate the attack. The attacker also acts as both UAC and UAS himself, thus no third party would suspect these INVITEs. The proxy server will then reserve resource for the attacker according to the session timer. As the proxy server is not able to directly determine whether an established session is still alive or dead before the session timer expires, it allows the attacker to simply disconnect from the wireless network but still hold resource reserved for the session on the proxy server. After the disconnection, the attacker will be silent for a while and then initiate another session with an arbitrarily long timer to further reserve resources on the proxy server.

Such an attack causes damages to the proxy server and gives the attacker advantages in two folds. First, to maximize the effect of the attack, the attacker will set the session timer to a large value and reserve resources as long as possible on the proxy server. Wireless networks allow the attacker to easily disconnect from the network and the disconnection does not release the resources until the session timer expires. Thus the attacker can repeatedly reserve new resource besides the resources already held by him each time he initiates a session. As the attacker continues initiating sessions and disconnecting from the wireless network, he is able to hold multiple resources simultaneously on the proxy server and prevent normal users from getting access to the VoIP service. Second, the attacker keeps silent for a while after each disconnection and initiates the attack following the normal traffic rate. Thus it can hardly be detected by existing volume-based intrusion detection systems. The attack virtually costs no extra resource of the attacker other than simply setting a value of the "Session-Expires" header each time before initiating a session. More severely, if several distributed attackers collaborate to initiate the attack, resources on the proxy server will be drained at a much faster pace. Overall speaking, the identified attack can easily consume a considerable amount of processing capacity of the SIP proxy servers, and significantly downgrade the servers' performance to process normal messages and manage sessions. To the best of our knowledge, this resource-drained DoS attack has not been addressed in the literature and we are the first to identify it.

IV. Detection Scheme Design

A. Hypothesis Test and Observation Distributions

Our goal is to develop a scheme to efficiently detect the resource-drained attack. The main and most important characteristic of the attack behavior is unpredictable, which makes the detection problem very difficult. However, at a high level, the problem can be considered as making a decision on whether the attack exists or not in the wireless VoIP network. Thus by observing the values of the session timers from the whole network, we design the detection scheme following the statistical hypothesis test approach.

Let $\{T_n, n = 0, ..., k\}$ be a sequence of the session timer values observed from the network. The observation point can be the proxy server as it is the target of the attack and also monitors every going-by SIP message. We consider two hypotheses, H_0 and H_1. The null hypothesis H_0 corresponds to no attack in the network whereas the alternate hypothesis H_1 corresponds to attacks existing in the network. Then the problem can be formulated as

$$Decide\ Between \begin{cases} H_0: \ T_1, ..., T_k \ \sim \ f_0 \\ H_1: \ T_1, ..., T_k \ \sim \ f_1 \end{cases} \tag{1}$$

where f_0 is the distribution of the session timer values when there is no attack whereas f_1 is the distribution when attacks exist in the network. We will choose between the two hypotheses based on the actual observed distribution of the session timer values.

The session timer conveys the durations of the sessions and there is no default value defined for the timer [2]. An efficient normal session timer setting should reflect the characteristic of the session holding time and thus avoid frequent refreshments to increase the signaling burden. Therefore f_0 can be modeled to have the same distribution of the session holding times, which is log-normal to reflect the long tail characteristic according to existing research [5]. However, since the attacker behavior is unpredictable, the distribution f_1 of session timer values under attack can hardly be characterized. Thus it is necessary to use a non-parametric approach where no assumption on f_1 is required to perform the detection, which will be discussed in the following.

B. The Anderson-Darling Test Based Detection Scheme

The Anderson-Darling test [3], [4] is a powerful statistical test tool which can examine whether the actual observed distribution differs from the null hypothesis distribution f_0. For the resource-drained attack detection, we observe the session timer sequence $\{T_n\}$ of size k and prepare it for the Anderson-Darling test.

We first sort the logarithms of $\{T_n\}$ from low to high and obtain another sequence $\{X_n\}$ of the same size. Next we will use the A-D test to check the normality of $\{X_n\}$. Let μ and σ be the mean and standard deviation of $\{X_n\}$ respectively. We then standardize $\{X_n\}$ to get $\{Y_n\}$

$$Y_n = \frac{X_n - \mu}{\sigma}. \tag{2}$$

This standardization allows us to perform the normality test without knowing the specific parameters for the normal distribution. Then with the cumulative distribution function (CDF) of the standard normal distribution Φ, the Anderson-Darling test statistic is

$$A^2 = -k - S \tag{3}$$

where

$$S = \sum_{n=1}^{k} \frac{(2n-1)}{k} [\ln \Phi(Y_n) + \ln(1 - \Phi(Y_{k+1-n}))]. \quad (4)$$

Then an approximate adjustment of A^2 for the sample size k is calculated to avoid skewness [4]

$$A^{*2} = A^2(1 + \frac{4}{k} - \frac{25}{k^2}). \quad (5)$$

Finally, we have the detection stopping rule

$$Choose \begin{cases} H_0 : \ A^{*2} \leq \beta \\ H_1 : \ A^{*2} > \beta \end{cases} \quad (6)$$

where β is the critical value of the Anderson-Darling normality test and the choice of β's actual value is based on the significance level we want to achieve [4]. From (6), we see that the attack is detected when A^{*2} exceeds β. Algorithm 1 describes the detection scheme on a session timer sequence of size k.

Algorithm 1 A-D test based detection scheme with critical value β

1. Record k observations $\{T_n\}$ of the "Session-Expires" header values from the users in a wireless VoIP network.
2. Calculate the logarithm of every element in $\{T_n\}$, sort them from low to high, and obtain the sequence $\{X_n\}$.
3. Standardize $\{X_n\}$ to obtain $\{Y_n\}$ using (2).
4. Calculate the Anderson-Darling test statistic A^2 from $\{Y_n\}$ using (3).
5. Adjust A^2 for the sample size k to obtain the adjusted test statistic A^{*2} using (5).
6.

if $A^{*2} > \beta$ **then**
  reject H_0. The attack is detected.
else
  do not reject H_0. No attack is detected.
end if

Another powerful widely-used statistical test is the Kolmogorov-Smirnov test [11]. However, we choose the A-D test over the K-S test based on two of its merits. First, the A-D test is more sensitive at the tail of the distribution. Second, the A-D test is especially powerful at test for normality when the parameters of the reference normal distribution are not known. Both of the merits tally with the characteristic of f_0, which justifies our choice of the A-D test.

V. Performance Evaluation

In this section, we validate the performance of the proposed detection scheme on the novel resource-drained attack through computer simulation. The performance is measured in terms of the number of samples to reach the detection decision under different attack conditions. Besides showing its ability to detect the basic one attacker attack, the scheme works even more effectively when dealing with the DDoS attack.

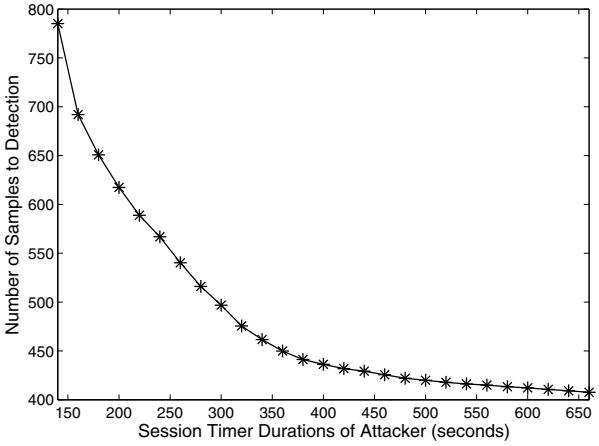

Fig. 2. Detection of basic one attacker attack.

A. Simulation Setup

We consider a wireless VoIP network with 60 users, who can be either attackers or normal users. The normal traffic is simulated based on the data set from [5]. Each user sets a value for the "Session-Expires" header field before sending out the INVITE message to initiate a SIP session. In the normal traffic, the session timer values follow a log-normal distribution, where the mean is 116.75s and the standard deviation is 262.28s. The critical value β is set to 0.751 to achieve a significance level of 5% [4]. The detection is performed according to Algorithm 1 each time a new sample is picked in. The normal data set passes the test even when the sample sizes are small thanks to the approximate adjustment of the test statistic and the significance level of 5%.

B. Detection of Basic One Attacker Attack

In this attack case, there is one attacker who can manipulate his own session timer values as long as he wants among the total 60 users. As the mean of the normal session timers is about 120s, the minimum timer of the attack is set to 140s for the attacker to gain some advantage over normal users. The severity of the attack goes up with the values of the attacker session timers. The traffic arrival of the attack is in conformance with the normal traffic, thus obviously it can not be detected by volume-based intrusion detection systems. We monitor the values of the session timers from all the users. Even though some INVITE messages sent by the users do not result in established sessions, we still include their session timer values into the test since they indicate the attempts of initiating sessions. Figure 2 shows the average detection delay in terms of the number of samples to reach the detection decision. The clear trend from the figure is that the longer the attacker wants to hold the resources on the proxy server each time, the faster it will take to detect the attack. Take the attack of 400s session timer for example, about 436 samples from the whole network are needed to detect the attack. However, considering the attacker sends his attempts at the frequency

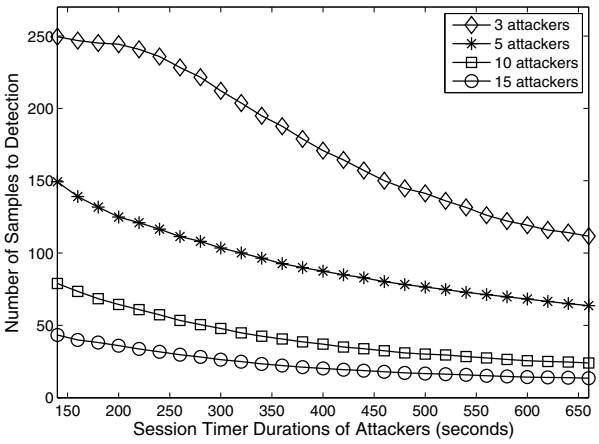

Fig. 3. Detection of DDoS attack.

of about every 60 INVITE messages of the whole network, the attack is detected around the 7th attempt of the attacker, where no severe damage has been done to the proxy server yet considering the processing capability of even open source SIP proxies [12].

C. Detection of DDoS Attack

To increase the intensity of the attack and hold resources on the proxy server as fast as possible, one option for an attacker is to increase his attacking rate. Nevertheless, this approach also increases the traffic volume of the attacker and is very likely to be detected by volume-based intrusion detection systems. The main damage of the resource-drained attack identified in this paper does not depend on the sending rates of the attack attempts, but on the duration of the manipulated session timer in each attempt. Instead of increasing one attacker's attacking rate, multiple distributed attackers can collaborate to initiate the attacks together. The attackers all set long session timers themselves and collaboratively initiate attacks to drain the resources on the proxy server at a much faster pace. Note that in this case the traffic arrival of all the attackers still follows the normal traffic arrival but collectively they can significantly increase the intensity of the attack and still escape the volume-based detection. Figure 3 shows the average detection delay of the DDoS attacks. Attack cases of 3, 5, 10 and 15 attackers out of the total 60 users are considered in our simulation. Each attacker sends the same form of the resource-drained attack and collaboratively they can hold resources on the proxy server multiple times as fast as the one attacker case based on the number of attackers in the attack. From Figure 3, besides the trend that longer attacking session timer causes quicker detection, we see that the DDoS attacks are detected much more quickly than the one attacker attack of the same session timer durations. Also, the more the attackers there are, the quickly the attacks will be detected. Thus the detection scheme is more effective when dealing with the DDoS attack.

VI. Conclusion

In this paper we identify a novel resource-drained denial of service attack which targets SIP-based wireless VoIP networks. The attack works by exploiting vulnerabilities of one SIP protocol extension and wireless networks. The "Session-Expires" header, or the session timer, is originally proposed as a keep-alive mechanism for SIP. However, it provides attackers opportunities to reserve resources on the SIP proxy servers as long as they want. Also, wireless networks allow attackers to easily disconnect from the network and the disconnection does not release the resources on the proxy servers until the session timer expires. Attackers can hold multiple resources through repeating reservations and disconnections, and greater damages can be caused if collaborative attacks are initiated from distributed attackers. Moreover, the low-volume nature of the attack allows it to avoid being detected by existing volume-based intrusion detection systems. As a counter-measure, we propose a robust detection scheme for the resource-drained attack based on the statistical Anderson-Darling test through investigating the characteristics of both the normal and attack behaviors. The scheme utilizes the changed statistical property of the session timers induced by the attack as the key insight that leads to detection. Through computer simulation, we show that besides the capability to detect the basic one attacker resource-drained attack, the scheme is even more effective when dealing with the DDoS attack. As future work, we will investigate and quantify the damage level caused by the attack through measures such as call dropping rate and SIP proxy server overload. Also, better statistical measures will be identified to more accurately and realistically model the distribution of the session timer values.

References

[1] J. Rosenberg, H. Schulzrinne and G. Camarillo, "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.
[2] S. Donovan, and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)," IETF RFC 4028, April 2005.
[3] T. Anderson and D. Darling, "Asymptotic theory of certain "goodness-of-fit" criteria based on stochastic processes," *Annals of Mathematical Statistics*, 1952.
[4] M. Stephens, "EDF Statistics for Goodness of Fit and Some Comparisons," *Journal of the American Statistical Association*, vol. 69, pp. 730-737, 1974.
[5] F. Gustafson and M. Lindahl, "Evaluation of Statistical Distributions for VoIP Traffic Modelling," University Essay from University West, Department of Economics and IT, 2009.
[6] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms," *IEEE Network*, vol. 20, no. 5, pp. 26-31, 2006.
[7] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert and D. Sisalem and S. Ehlert, "Survey of Security Vulnerabiliteis in Session Initiation Protocol," *IEEE Communication Surveys & Tutorials*, vol. 8, no. 3, pp. 68-81, 2006.
[8] VoIPSA "VoIP Security and Privacy Threat Taxonomy," Public Release 1.0, 2005.
[9] J. Tang, Y. Cheng and C. Zhou, "Sketch-Based SIP Flooding Detection Using Hellinger Distance," in *Proc. IEEE Globecom*, 2009.
[10] H. Sengar, H. Wang, D. Wijesekera and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 6, pp. 794-805, June 2008.
[11] Chakravarti, Laha, and Roy, (1967). *Handbook of Methods of Applied Statistics, Volume I*, John Wiley and Sons, pp. 392-394, 1967.
[12] SIP Express Router, [Online:]http://www.iptel.org/ser/.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE