基于卡尔曼滤波的 LDDoS 攻击检测方法

吴志军, 岳 猛
(中国民航大学电子信息工程学院, 天津 300300)

摘 要: 低速率分布式拒绝服务 LDDoS(Low-rate Distributed Denial of Service)攻击是一种新型的 DDoS 攻击. 它利用 TCP 协议超时重传 RTO(Retransmission Time Out)机制, 向受害者发送周期性的脉冲(Pulse)攻击. LDDoS 平均攻击速率较低, 因此它能躲避传统的检测方法. 本文针对 LDDoS 攻击提出了一种基于卡尔曼(Kalman)滤波的检测方法, 采用一步预测与最优估算的误差值作为检测依据. 通过模拟仿真和在实际网络环境中测试, 得到 89.6% 的检测率. 实验结果表明本文方法能有效地检测出 LDDoS 攻击.

关键词: 低速率分布式拒绝服务攻击; 超时重传; TCP; 流量; 卡尔曼滤波
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2008) 08-1590-05

Detection of LDDoS Attack Based on Kalman Filtering

WU Zhi-jun, YUE Meng
(*College of Electronics and Information Engineering, Civil Aviation University of China, Tianjin 300300, China*)

Abstract: LDDoS (Low-rate Distributed Denial of Service) attack is a new class of DDoS, which exploits TCP's RTO (Retransmission Time Out) mechanism. An LDDoS attack can elude the monitor of traditional detection approach by sending low-rate packets in the way of periodic pulse to a victim. This paper proposes an approach of detecting LDDoS attack based on kalman filter. The error between one step prediction and the optimal estimation is used as the detection criterion. Experiments in simulation environment and practical network are conducted to test the detect performance and about 89.6% detect probability is achieved. Results show that this approach has an expected effect in detecting LDDoS attack.

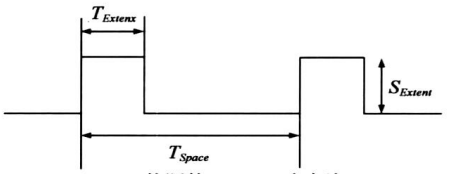
Key words: low-rate distributed denial of service (LDDoS); retransmission time out (RTO); TCP; traffic; kalman filtering

1 引言

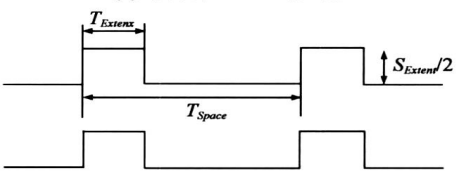
TCP 协议提供了一种可靠的面向连接的字节流运输层服务. 当对端用户可靠的时候, TCP 超时重传机制可以使网络的吞吐量达到最大; 而恶意用户也可以利用超时重传机制的弱点产生拒绝服务攻击, 严重的降低受害机器的吞吐量.

低速率分布式拒绝服务 LDDoS 攻击不同于以往的淹没型攻击, 它通过估计合法 TCP 流的 RTO 作为攻击的周期 T, 发送周期性的短脉冲, 如果攻击流量在 RTT (Round Trip Time) 内足够导致数据包丢失, 那么合法 TCP 流将进入超时状态. LDDoS 攻击最显著的特点是攻击者使用更少的攻击包就可以使受害主机的吞吐量大幅度的降低, 因此它更加隐蔽; 同时可以灵活的调整参数, 使受害者的受害程度有所不同[1].

一个单源 LDDoS 攻击脉冲序列可以用一个四元组表示为 $A(T_{Extent}, S_{Extent}, T_{Spaces}, N)$, 其中 T_{Extent} 是脉冲攻击长度, 代表攻击者持续发包的时间段; S_{Sxtent} 是脉冲幅度, 代表流量的最高速率; T_{Space} 表示两个脉冲之间的时间间隔; N 是一次攻击发出的脉冲总数. 而多元的



(*a*) 单源的 LDDoS 攻击流



(*b*) 两个半速率的 LDDoS 攻击流

图 1 LDDoS 攻击模型

收稿日期: 2007-11-27; 修回日期: 2008-03-18
基金项目: 国家自然科学基金委员会与中国民用航空总局联合资助项目(No. 60776808); 中国民航大学科技启动资金项目(No. 2006)

LDDoS 攻击需要产生周期、幅度等特征一致的方波, 这些方波到达受害端正好汇聚成一个足够大的脉冲. 模型如图 1 所示.

由于 T_{Extent}/T_{Space}的值很小, 发送攻击的平均速率很低, 因此得名低速攻击[2].

2　相关研究

传统的 DDoS 攻击大量消耗网络带宽和系统资源, 导致该网络或系统瘫痪或停止提供正常的网络服务. 对于传统 DDoS 攻击的一般检测方法主要有两种[3,4]: (1) 基于网络的入侵检测系统(NIDS), 它主要是通过单位时间的链路流量是否超过预先设定的极限值来判断网络中是否发生 DDoS 攻击; (2) 基于主机的入侵检测系统(HDIS), 它主要是通过单位时间内到达主机的数据包的数量是否超过预先设定的极限值来判断该主机是否遭到 DDoS 攻击. 但是 LDDoS 攻击甚至比淹没型 DDoS 攻击对网络的危害更大, 由于它具有低速率周期性, 因此传统的 IDS 无法有效的对其进行检测[5].

随着对 LDDoS 特性的逐步研究, YU CHEN, KAI HWANG 等提出了基于数字信号处理的检测方法, 主要思想是提取流量的频域特性来进行检测[6~8]. 因为 LDDoS 攻击是周期性的脉冲, 所以包含攻击的流量其功率普密度集中在低频段. 在低频段选取某一个频点, 对正常流与异常流的累计归一化功率普密度 NCPSD(Normalized Cumulative PSD) 进行比较就可以检测出 LDDoS 攻击. 但是这种检测方法漏警律比较高, 为 12.0%, 并且频率点取不同值造成的检测结果不够稳定.

根据网络流量矩阵估算理论以及网络在遭受 LDDoS 攻击时流量突然减小的事实, 本文提出了基于卡尔曼滤波的一种检测方法. 卡尔曼滤波算法本身在数学上是一种统计估算方法, 通过处理一系列带有误差的实际量测数据而得到的物理参数的最佳估算, 它是最优的, 效率最高的一种算法[9]. 卡尔曼滤波算法能够对流量矩阵进行有效的预测和估算[10~12], 然后通过比较预测与估算的误差就可以有效的检测 LDDoS 攻击.

3　卡尔曼滤波检测法

卡尔曼滤波器是一种高效率的递归滤波器(自回归滤波器). 对于一个离散控制过程的系统可以用一个线性随机微分方程来描述:

$$X(k|k)=AX(k-1)+BU(k)+W(k)\quad QR \tag{1}$$

再加上系统的测量值:

$$Z(k)=HX(k)+V(k) \tag{2}$$

上两式子中, $X(k)$ 是 k 时刻的系统状态, $U(k)$ 是 k 时刻对系统的控制量, A 和 B 是系统参数. $Z(k)$ 是 k 时刻的测量值, H 是测量系统的参数. $W(k)$ 和 $V(k)$ 分别表示过程和测量的噪声. 它们被假设成高斯白噪声, 它们的协方差分别是 Q, R(不随系统状态变化而变化). 卡尔曼滤波器可以结合预测值和测量值, 得到现在状态 k 的最优化估算值 $X(k|k)$. 它是最优的信息处理器.

假设现在的系统状态是 k, 根据系统的模型, 可以基于系统的上一状态而预测出现在状态:

$$X(k|k-1)=AX(k-1|k-1)+BU(k) \tag{3}$$

式(3)中, $X(k|k-1)$是利用上一状态预测的结果, $X(k-1|k-1)$是上一状态最优估算的结果, $U(k)$ 为现在状态的控制量, 如果没有控制量, 它可以为 0. 然后更新对应于 $X(k|k-1)$的协方差 P:

$$P(k|k-1)=AP(k-1|k-1)A'+Q \tag{4}$$

式(4)中, $P(k|k-1)$是 $X(k|k-1)$对应的协方差, $P(k-1|k-1)$是 $X(k-1|k-1)$对应的协方差, A' 表示 A 的转置矩阵, Q 是系统过程的协方差. 式(3), (4)就是对系统的预测.

有了预测结果, 再结合测量值, 就可以得到现在状态 k 的最优化估算值 $X(k|k)$:

$$X(k|k)=X(k|k-1)+Kg(k)(Z(k)-HX(k|k-1)) \tag{5}$$

其中, Kg 为卡尔曼增益(Kalman Gain).

$$Kg(k)=P(k|k-1)H'/(HP(k|k-1)H'+R) \tag{6}$$

通过式(5), (6)就得到了 k 状态下最优的估算值 $X(k|k)$. 但是要令卡尔曼滤波器不断的运行下去直到系统过程结束, 还要更新 k 状态下 $X(k|k)$的协方差:

$$P(k|k)=(I-Kg(k)H)P(k|k-1) \tag{7}$$

其中, I 为单位矩阵, 对于单模型单测量, $I=1$. 当系统进入 $k+1$ 状态时, $P(k|k)$就是式(4)中的 $P(k-1|k-1)$. 这样, 算法就可以自回归的运算下去. 有了卡尔曼滤波的基本原理, 就可以进行下面的步骤.

3.1　波形趋势提取

要对 LDDoS 攻击进行检测, 首先要研究攻击发生时网络流量的特性. 在受害端的上一跳路由器上进行流量监测, 对进入路由器的流量(Byte) 每隔 0.25s 进行一次统计, 统计时间 900s. 为便于比较, 文中所有图的横轴范围统一为 0~ 900s. 由图 2 可以看出攻击发生期间(181s~ 720s)受害端流量下降, 并且流量的波动性更强.

为了便于分析比较, 需要对取样信号进行平滑, 提取波形的变化趋势. 先用离散小波变换对流量进行处理. 对于一个信号 $f(t)\in L^2(R)$, 可以用尺度函数 $\phi_{j,k}(t)$和小波函数 $\varphi_{j,k}(t)$将其表示为:

$$f(t)=\sum_k c_{j_0}(k)\phi_{j_0,k}(t)+\sum_k\sum_{j=j_0}d_j(k)\varphi_{j,k}(t) \tag{8}$$

其中, $c_j(k)$和 $d_j(k)$分别是原信号的平滑信号和细节信号, 它们可以通过 Mallat 算法求出[13]:

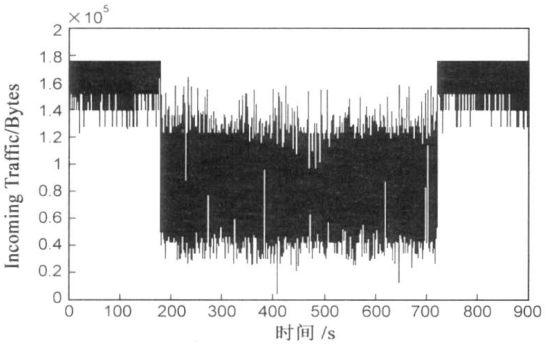


图 2 进入受害端的流量取样

$$c_j(k)=\sum_m h_0(m-2k)\,c_{j-1}(m) \tag{9}$$

$$d_j(k)=\sum_m h_1(m-2k)\,c_{j-1}(m) \tag{10}$$

式中, h_0 和 h_1 分别是低通滤波器系数和高通滤波器系数. 因为平滑信号具有低通特性, 所以它能滤除原始信号的高频分量. 如图 3 所示, 这里对原始数据使用 db(1) 小波做 5 级分解. 经过这一变换, 原始波形变得相对平滑了, 只有在攻击发生和结束的时刻有突变, 同时待处理的数据量也减少了, 从而有利于卡尔曼滤波器的运算.

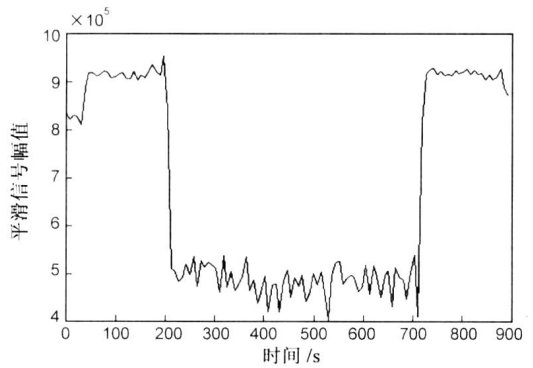


图 3 流量的波形趋势

3.2 Kalman 算法

在上面小波分析的基础上建立一个流量矩阵模型并用卡尔曼滤波算法进行预测和估算. 把平滑信号作为观测值 Y_t, 它与实际的系统状态值 X_t 的关系可以用线性方程表示为:

$$Y_t=A_tX_t+V_t \tag{11}$$

其中, A_t 表示路由器矩阵, V_t 表示一个非相关, 零均值的高斯白噪声. 对下一时刻状态的一步预测表示为:

$$X_{t+1}=C_tX_t+W_t \tag{12}$$

其中 C_t 反映了流量的时空相关性, W_t 是非相关, 零均值的高斯白噪声, 由流的随机波动造成[14].

根据卡尔曼滤波的原理, 基于上一状态可预测出现在的状态, 同时更新 X_t 的自协方差 P_t. 用公式表示为:

$$\begin{cases}\hat{X}_{t+1|t}=C_t\hat{X}_{t|t}\\ P_{t+1|t}=C_tP_{t|t}C_t^T+Q_t\end{cases} \tag{13}$$

其中, $\hat{X}_{t+1|t}$ 表示一步预测, $P_{t+1|t}$ 表示预测方差, Q_t 表示 W_t 的协方差.

$$E[W_kW_l^T]=\begin{cases}Q_k, & \text{if } k=l\\ 0, & \text{otherwise}\end{cases} \tag{14}$$

有了现在状态的预测结果, 然后再收集现在状态的测量值. 结合预测值和测量值, 可以得到状态 $t+1$ 的最优化估算值 $\hat{X}_{t+1|t+1}$, 同时更新 $t+1$ 状态下 $X_{t+1|t+1}$ 的自协方差 $P_{t+1|t+1}$.

$$\begin{cases}\hat{X}_{t+1|t+1}=\hat{X}_{t+1|t}+K_{t+1}[Y_{t+1}-A_{t+1}\hat{X}_{t+1|t}]\\ P_{t+1|t+1}=(I-K_{t+1}A_{t+1})P_{t+1|t}(I-K_{t+1}A_{t+1})^T\\ \qquad\qquad +K_{t+1}R_{t+1}K_{t+1}^T\end{cases} \tag{15}$$

其中, $K_{t+1}=P_{t+1|t}A_{t+1}^T[A_tP_{t+1|t}A_{t+1}^T+R_{t+1}]^{-1}$, R_t 表示 V_t 的协方差.

$$E[V_kV_l^T]=\begin{cases}R_k, & \text{if } k=l\\ 0, & \text{otherwise}\end{cases} \tag{16}$$

为了进行实时的检测, 设定一个检测周期为 20s, 同时将前一周期观测数据的均值作为下一周期预测的初值, 随着卡尔曼的工作, X 会逐渐的收敛[15]. 这样卡尔曼预测的结果如图 4 中实线所示, 虚线是最优估算的结果.

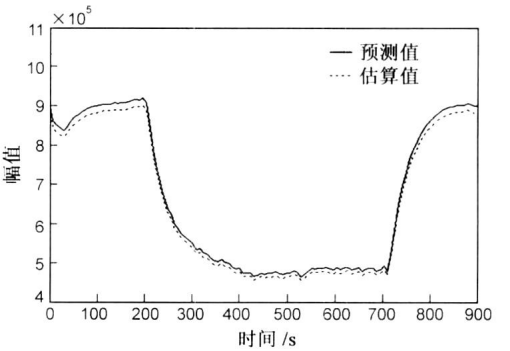


图 4 预测值与估算值的比较

下面对 $t+1$ 时刻的一步预测值与最优估算值进行比较, 误差表达式为:

$$\varepsilon_{t+1}=|\hat{X}_{t+1|t}-\hat{X}_{t+1|t+1}| \tag{17}$$

由于 $\hat{X}_{t+1|t}$ 只是靠 t 状态及以前的信息得出的, 而对 $\hat{X}_{t+1|t+1}$ 的估算还用到了 $t+1$ 状态的信息, 因此当突然出现异常时估算值与预测值会产生很大的误差. 图 5 是归一化的误差, 在异常突变时误差确实会变得很大, 如果它超过一定的门限值则认为发生攻击.

4 假设检验

由图 5 还可以看出攻击开始和结束时误差都很大, 因为从受攻击状态恢复正常流量也是发生了突变. 为了只对攻击发生时的突变进行报警, 下面用一个假设检验

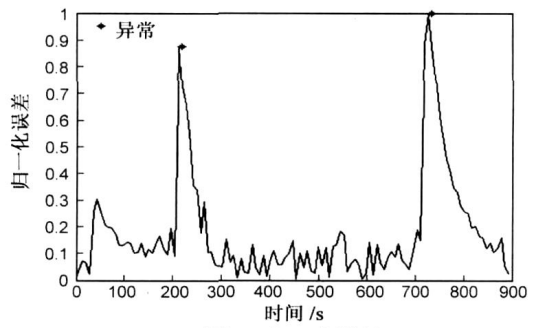


图 5　归一化误差

的方法判定攻击的开始与结束, 用 t 检验法, 这样就可以减小误报. 一旦检测出 ε_i 的值超过门限的情况, 就开始对下一时刻的原始流量进行检测. 把一个检测周期分为 n 个相同的时间间隔小段, 用 t 检验法来判定攻击是开始还是结束. 需要检验:

$$H_0: \mu \geq \mu_0 = M_k / n$$

$$H_1: \mu < M_k / n$$

其中 M_k 是在正常情况下通过学习得到的一个流量的数学期望. 则拒绝域为:

$$t = \frac{F_{avg} - \mu_0}{s/\sqrt{n}} < t_{1-\alpha}(n-1)$$

式中, F_{avg} 为这一段时间流量的平均值. 如果 H_1 可以接受, 则认为攻击刚刚开始; 如果 H_1 被拒绝, 则认为攻击已经结束. 这样就只留下一个突变点认为是攻击, 另一个突变点不做报警.

5　模拟实验及结果分析

本文的实验系统使用五台 PC 机、两台 Cisco 路由器和一台 Cisco 交换机, 在 linux 平台下模拟 LDDoS 攻击并实现最终的检测. 该网络结构可以代表真实网络的一般特性.

5.1　实验环境和步骤

实验的环境如图 6 所示. 图中的路由器为 Cisco2621, 路由器间的带宽 10Mbps. 其它各设备配置如表 1 所示.

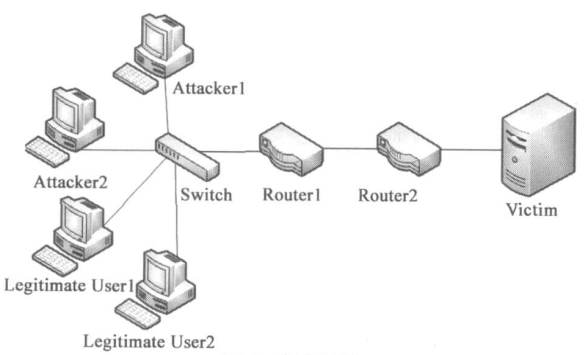


图 6　实验环境

攻击时, 设定的攻击模型参数为 A (200ms, 5Mbps, 1s, 540).

实验开始, 先让LegitimateUser正常下载服务器的

表 1　实验设备配置

机器编号	IP 地址	操作系统
Attacker1	192. 168. 20. 23	RedHat 9. 0
Attacker2	192. 168. 20. 24	RedHat 9. 0
Legitimate User1	192. 168. 20. 25	Windows 2000
Legitimate User2	192. 168. 20. 26	Windows 2000
Victim	192. 168. 40. 8	RedHat 9. 0

FTP 资源, 180s 后 Attacker 发起 UDP 攻击, 每次攻击持续时间为 540s, 然后再让 Legitimate User 正常下载 180s, 以此类推. 在受害端每 0. 25s 对流量进行一次统计, 以字节作单位, 这样就获得了要处理的原始数据.

5.2　实验结果及分析

为了验证卡尔曼算法的检测效果, 共进行 1000 次攻击, 检测周期取 20s; 对采样取得的原始数据使用 db (1) 小波做 5 级分解. 实验数据如表 2 所示.

表 2　实验数据统计

攻击次数	判决门限	正确判决次数	漏警次数	虚警次数
1000	0. 850	853	147	105
1000	0. 650	896	104	126
1000	0. 550	902	98	177
1000	0. 350	918	82	212

因为要在检测概率、漏警概率和虚警概率之间进行折中, 所以必须选取一个合适的判决门限. 经过大量实验, 统计正常情况和异常情况下 ε_i 的分布规律, 选取门限值为 0. 650. 在这个门限下, 由表可得出正确判决的概率为 89. 6% (与 Yu Chen 的检测率比较提高了近 2 个百分点), 漏警率为 10. 4%, 虚警率为 12. 6%. 其中, 虚警率的大小主要依赖于网络质量和 t 检验的效率. 与其它门限值相比, 它使得正确判决率足够高, 误判率足够低, 符合要求. 因此, 这个门限值是最优的.

6　总结

本文针对 LDDoS 攻击提出了一种卡尔曼检测法. 先经过小波变换提取波形趋势, 简化待处理的数据; 然后基于卡尔曼滤波算法, 预测值与估算值在流量发生突变时会产生很大的误差, 通过误差值与门限值的比较来检测攻击. 通过实验证明此方法可以实时有效的检测出 LDDoS 攻击, 同时通过假设检验消除了负面影响, 从而降低了误报率. 最后达到 89. 6% 的检测率.

但是, 实际网络流量是多变的、复杂的, 加之 LDDoS 攻击的隐蔽性和伪装性, 很多时候单靠一种方法去检测和防范是不能完全奏效的, 更好的做法是针对这种攻击的各种特征结合多种手段去应对. 因此, 今后的工作是要发现更多更明显的攻击流特征, 进一步优化判决算法

以及尝试结合其它方法进行研究,以期取得令人更加满意的效果.

参考文献:

[1] Yu Chen, Yur Kwong Kwok, Kai Hwang. Collaborative Defense Against Periodic Shrew DDoS Attacks in Frequency Domain [J]. Journal of Parallel and Distributed Computing. 2006, 66(9): 1137- 1151.

[2] M Delio. New breed of attack zombies lurk [R/OL]. http://www.acm.org/technews/articles/2001-3/0514m.html, 2001-5-1.

[3] 张杰, 刘宗藩, 孙东卫. 网络入侵检测系统的实现[J]. 现代电子技术, 2003, 6(22): 27- 30.

[4] 李旺, 吴礼发, 胡谷雨. 分布式网络入侵检测系统[J]. 软件学报, 2002, 13(8): 1723- 1727.

[5] Kuzmanovic A, Knightly E. Low-rate TCP-targeted denial of service attacks [A]. Proc ACM SIGCOMM'03 [C]. USA: ACM Press 2003. 75- 86.

[6] Cheng C-M, Kung H, Tan K-S Tan. Use of spectral analysis in defense against DoS attacks [J]. Proc IEEE GLOBECOM. 2002, 3(75): 2143- 2148.

[7] Y-K Kwok, R Tripathi, Y Chen, K Hwang. HAWK: Halting Anomaly with Weighted ChoKing to Rescue Well-Behaved TCP Sessions from Shrew DoS Attacks [J]. LNCS Computer Networks and Mobile Computing. 2005, 3619(47): 423- 432.

[8] Chen Y, Hwang K, Kwok YW. Filtering of shrew DDoS attacks in frequency domain [A]. In: Proc of the IEEE Conf. on Local Computer Networks, 30th Anniversary [C]. New York: IEEE Inc, 2005. 786- 793.

[9] 宋文尧, 张牙. 卡尔曼滤波[M]. 北京: 科学出版社, 1991.

[10] Kailath T, Sayed A H, Hassibi B, Sayed A H, Hassibi B. Linear Estimation [M]. NJ: Prentice Hall, 2000.

[11] Soule A, Salamatian K, Taft N. Traffic matrix tracking using kalman filters [A]. ACM SIGMETRICS Performance Evaluation Review [C]. USA: ACM Press, 2005. 33(3): 24- 31.

[12] Soule A, Nucci A, Cruz R, Leonardi E, taft N. How to identify and estimate the largest traffic matrix elements in a dynamic environment [A]. In ACM Sigmetrics [C]. USA: ACM Press, 2004. 32(1): 73- 84.

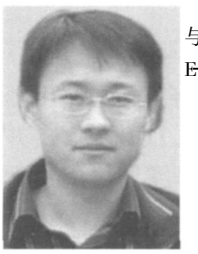
[13] C Burrus, R Gopinath, H Guo. Introduction to Wavelets and Wavelet Transforms: A Primer [M]. NJ: Prentice Hall, 1998. 162- 213.

[14] Grewal M, Andrews A. Kalman Filtering Theory and Practice Using MATLAB (Second Edition) [M]. John Wiley & Sons, Inc, 2001. 114- 165.

[15] F C Ham, R G Brown. Observability, Eigenvalues, and Kalman Filtering [J]. IEEE Transactions on Aerospace and Electronic Systems, 1983, 19(2): 269- 273.

作者简介:

吴志军 男, 1965 生, 教授, 博导, 研究方向: 网络与信息安全.
E-mail: caucwu@263.net



岳 猛 男, 1984 生, 硕士, 研究方向: 网络与信息安全
E-mail: myue_23@163.com