基于风险熵和 Neyman-Pearson 准则的安防网络风险评估研究

胡瑞敏 [1, 2] 吕海涛 [1] 陈 军 [1]

摘 要 为应对严峻复杂的安全形势, 我国通过构建安全防范系统实现对公共安全的防护. 安全防范系统是由人和安防设备组成的复杂系统, 安全防范系统风险评估是判断其防护效能好坏的重要度量标准. 本文将部署在一个区域的安全防范系统抽象看成由多个安防节点组成的网络, 根据熵理论和 Neyman-Pearson 准则, 提出一种利用防护最薄弱路径定量度量安全防范系统风险的模型, 并给出安全防范网络防护最弱路径的表达式, 以及基于 Dijkstra 最短路径算法求解防护最薄弱路径的方法. 最后本文研究模型参数和安全防范系统部署的数量与安全防范网络的风险之间的关系, 给出相应的仿真结果, 并进行实际应用场景的风险评估实验. 实验结果表明, 本文提出的模型可以定量评估多节点的安全防范系统的风险, 提高评估结果的科学性.

关键词 安全防范系统, 风险熵, Neyman-Pearson 准则, 风险评估, 防护最薄弱路径

引用格式 胡瑞敏, 吕海涛, 陈军. 基于风险熵和 Neyman-Pearson 准则的安防网络风险评估研究. 自动化学报, 2014, **40**(12): 2737−2746

DOI 10.3724/SP.J.1004.2014.02737

Risk Evaluation Model of Security and Protection Network Based on Risk Entropy and Neyman-Pearson Criterion

HU Rui-Min[1, 2] LV Hai-Tao[1] CHEN Jun[1]

Abstract There is a growing interest in the construction of security systems to protect social public safety. For a security system, risk assessment is an important metric to judge its protection effectiveness. In this paper, a security system deployed in an area is regarded abstractly as a diagram of security network. Firstly, a method for risk assessment based on entropy theory and Neyman-Pearson criterion is proposed. Secondly, the most vulnerable path formulation of the security network is described and a solution by utilizing the Dijkstra′s shortest path algorithm is provided. The protection probability on the most vulnerable path is considered as the risk measure of the security network. Furthermore, the effects of some parameters on the risk and the breach protection probability are simulated, and a risk evaluation experiment is carried out with a real scenario. The results show that the model proposed in this paper can not only quantitatively evaluate the risk of the security network but also get a more scientific and reasonable evaluation result.

Key words Security system, risk entropy, Neyman-Pearson criterion, risk assessment, most vulnerable path

Citation Hu Rui-Min, Lv Hai-Tao, Chen Jun. Risk evaluation model of security and protection network based on risk entropy and Neyman-Pearson criterion. *Acta Automatica Sinica*, 2014, **40**(12): 2737−2746

2001 年发生在美国的 911 事件使世界各国开始重视当前人类面临的严重的公共安全问题, 对公共安全的安全防范研究也再次得到重视. 当前以信息技术为主, 结合人和建筑物构建安全防范系统是公共安全防范的主要手段. 以我国为例, 近几年积极开展的平安城市建设就是构建和整合大型安全防范系统, 增强对社会公共安全的保护力度[1]. 我国公安部在国标 GB50348-2004 中对安全防范系统做出明确定义: 以维护社会公共安全为目的, 运用安全防范产品及其他相关产品所构成的入侵报警系统、视频安防监控系统、出入口控制系统、防爆安全检查系统等, 或由这些系统为子系统组合、集成的电子系统或网络[2]. 定义中有两个关键词, 即 “系统” 和 “网络”, 本文将一个防护区域内部署的多个安全防范系统抽象地看成一个安全防范网络, 从网络的角度对区域安全防范系统的部署及风险评估进行研究. 安全防范网络结构如图 1 所示.

收稿日期 2013-07-01 录用日期 2014-02-20
Manuscript received July 1, 2013; accepted February 20, 2014
国家自然科学基金面上项目 (61170023), 国家自然科学基金重点项目 (61231015), 国家重大科技专项基金 (2010ZX03004-003-03) 资助
Supported by General Program of National Natural Science Foundation of China (61170023), Key Program of National Natural Science Foundation of China (61231015), and the Major National Science and Technology Special Projects (2010ZX03004-003-03)
本文责任编委 王红卫
Recommended by Associate Editor WANG Hong-Wei
1. 武汉大学国家多媒体软件工程技术研究中心 武汉 430072 2. 武汉大学计算机学院 武汉 430072
1. National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan 430072 2. School of Computer, Wuhan University, Wuhan 430072

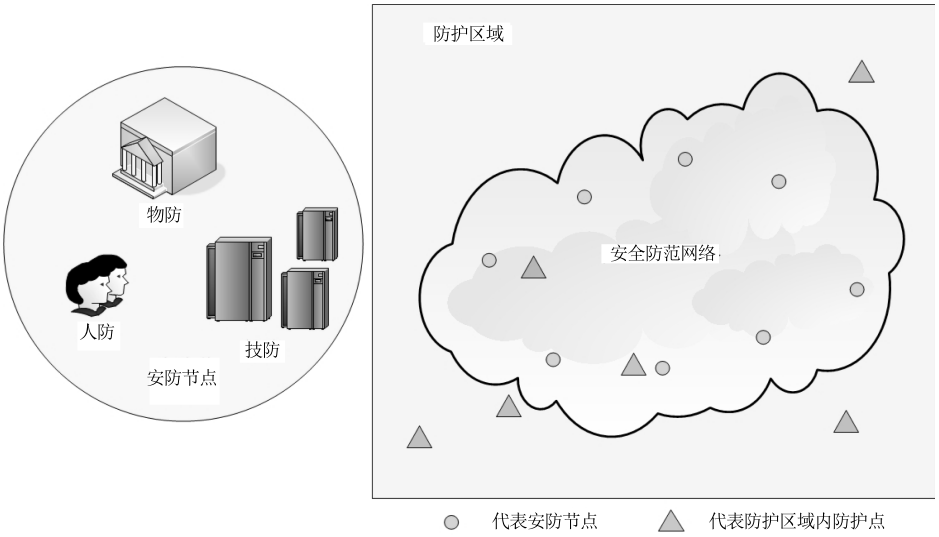


图 1 安全防范网络抽象结构图

Fig. 1 The abstract diagram of a security network

本文根据熵理论和 Neyman-Pearson 准则提出风险熵和安全防范系统防护模型, 通过系统对防护对象的防护概率来度量单个安防系统的风险, 然后以此为基础, 通过建立区域网格化模型, 将防护区域内的多个安防节点和道路抽象成图, 找出多节点所形成的安全防范网络的防护最薄弱路径, 用防护最薄弱路径度量安全防范网络的风险. 最后研究模型中不同参数及安全防范系统部署数量对安全防范网络整体风险的影响, 并给出相应的仿真结果. 本文的研究对安全防范网络的设计和评估有一定的指导意义.

1 相关研究介绍

安全防范系统的前身是实体保护系统 (Physical protection system). 20 世纪 60 年代, 美国最先开始对应用在核设施及辐射化学品仓库的实体保护系统的效能和风险评估进行研究, 我国在 90 年代初期开始这方面的研究. 进入 21 世纪, 随着信息技术的发展及信息化设备在安全防范中的广泛使用, 实体保护系统从初期的以人员和实体建筑为主的防护方式转变成由人防、物防和技防综合运用的方式, 实体保护系统的概念也因此开始发生变化, 尤其是随着 911 事件的爆发, 公共安全成为世界各国关注的问题, 基于人防、物防和技防的具有综合防范能力的实体保护系统开始被应用到公共安全的领域, 负责对人身、重要的设施和物品进行保护, 实体保护系统开始被称为安全防范系统或安全系统 (Security system). 通过对相关文献进行研究, 当前安全防范系统风险评估的方法主要分为两类: 基于构建评估指标的方法和基于概率统计的方法[3]. 下面分别从这两个方面介绍安全防范系统风险评估的相关研究成果和面临的问题.

1.1 基于构建评估指标的方法

1996 年和 2006 年, 中国人民公安大学陈志华承担公安部部级项目《防入侵盗窃系统评估研究》和《安全防范系统评估 — 评价体系与评价方法研究》, 针对安全防范系统风险评估问题, 提出构建风险评估指标体系的评价防范, 以《安全防范工程技术规范》为制定指标的标准, 收集专家对安全防范系统风险的意见, 通过专家确定的指标权重计算安全防范系统的评估结果, 最终根据结果对系统的风险进行风险高或低的定性评估. 2010 年, Sendi 等[4] 在安全防范系统风险评估中引入模糊数学的理论, 建立一种基于指标的模糊专家模型, 利用模糊数学中的隶属度函数对指标进行定量评估, 具体的评估模型由三部分组成: 1) 利用隶属度函数给定各项指标在闭区间 $(0, 1)$ 内相应的数值, 称为单因素隶属度; 2) 利用单因素隶属函数对各项指标进行单项评估; 3) 对各单因素隶属度函数进行加权算术平均, 计算综合隶属度, 得出综合评估的指标值. 其结果越接近 0 表明越差, 越接近 1 表明越好, 从而实现对安全防范系统风险的定量评估[5]. 该方法在对风险评估指标评分过程中引入模糊理论, 一定程度上解决了构建指标评估方法对风险定量评估的问题, 但其隶属度函数权重是通过专家确定的, 确定过程中依然很难避免人为主观的因素. 吴穹等[6] 在模糊专家模型的基础上, 建立基于 “空间风险和时间风险” 为特性的安全防范系统评价指标体系, 并采用层次分析法确定各评估指标的权重和相关隶属度函数的权重,

层次分析法在一定程度上降低了人为确定指标权重的主观因素的影响, 但层次分析法本身属于主观评估方法, 因为各层指标间一致性检验矩阵是人为指定的, 且在风险评估指标层次划分上也存在很大不确定性, 由于安防系统的各组成部分差异较大, 如人防、物防和技防很难适用同一个层次划分方法[7]. 2012 年, Xu 等[8] 在北京地铁供电机组的安全防范系统的风险评估中, 综合采用模糊专家评分法和故障树的方法, 即根据模糊专家评分法获得评估结果后, 运用故障树模型对结果数据进行分析, 以故障发生的概率衡量系统的风险. 但建立故障树模型需要很多基本事件发生的概率, 其数据源于对历史数据的统计, 如果数据统计量不够大, 统计结果就会出现很多不确定性, 这些不确定性会影响评估结果的合理性.

1.2 基于概率统计的方法

基于概率统计的方法主要是通过模拟仿真攻击者对目标的攻击行为, 统计成功和失败的次数, 以安全防范系统成功对目标进行防护的概率度量安全防范系统的风险. 根据系统风险评估结果的不同, 基于概率统计的方法可以分为三类: 定性评价、定量评价和定性与定量相结合的评价. 如最早的美国桑迪亚国家实验室 (Sandia National Laboratories) 提出的敌手序列模型 (Adversary sequence diagram), 通过对假设的敌人为到达防护目标需要经过的各个障碍进行分析, 以敌人成功破坏目标的概率作为系统风险分析的依据. 依据敌手序列模型对风险的评估是一种定性评估, 即概率在某个范围内代表一个风险等级. 在敌手序列模型之后出现的单路径分析模型和多路径分析模型都是以敌手序列模型为基础, 如 Doyon[9] 针对包含有警卫、实体建筑和探测器的安全防范系统的风险评估, 引入多路径分析模型, 对入侵者在不同位置对防护目标进行攻击时被发现的概率作为系统风险度量的依据. Hug 和 Giampapa 对包含出入口控制的安全防范系统的风险进行评估, 在 Doyon[9] 的基础上考虑系统的误报警率和漏报警率, 综合对系统的风险进行评估[10]. 上述评估结果都是对风险的定性评估. 1998 年, Hicks 等[11] 提出基于成本 – 效能的风险评估方法, 通过可能的经济损失作为风险的评估结果, 具体模型如下:

$$Risk = P(A) \times [1 - P(E)] \times C$$

其中, $P(A)$ 为防护目标被攻击的概率, $P(E)$ 为系统阻止防护目标被攻击的概率, C 为防护目标的价值. 该方法在某种程度上实现对风险的定量评估. 但其防护目标被攻击的概率是通过综合领域专家的意见及历史数据的统计得到的, 因此存在不确定性. 2001 年和 2005 年, 美国桑迪亚实验室的学者 Garcia 出版了 *The Design and Evaluation of Physical Protection Systems*[12] 和 *Vulnerability Assessment of Physical Protection Systems*[13] 两本专著, 其中借鉴了 Fischer 等[14] 在 2004 年的专著 *Introduction to Security* 中使用概率矩阵、临界矩阵和脆弱性矩阵对工业危险原料仓库风险评估的理论, 提出了对安全防范系统的风险评估方法, 综合运用路径分析法、概率分析法和成本 – 效能分析法对安全防范系统进行风险评估, 在风险评估中考虑安全防范系统的脆弱性, 以攻击者到防护目标的防护薄弱路径作为系统风险评估的依据. 2010 年, Xu 等[15] 在安全防范系统风险评估过程中引入 Dempster-Shafer 证据推理理论, 降低基于概率统计的评估结果的不确定性, 对统计结果引入专家评判过程, 首先建立对风险评估结果的评价指标, 随后根据 D-S 理论通过建立推理规则推导评估结果的可信度. D-S 理论属于不确定推理方法, 在一定程度上降低了概率统计中的不确定性, 但 D-S 理论推导出的结果可信度是建立在评价指标的绝对独立和打分的绝对公正基础上的, 而这一点仅在理论上存在, 实际操作难度很大, 很容易出现一票否决的现象. 而且推理规则和指标是指数级增长关系, 可信度结果很容易陷入理论上可以计算出来的窘境[16]. 2012 年, Dai 等[17] 在 Hicks 等[11] 和 Garcia[12] 风险评估理论的基础上, 提出运用成本 – 收益分析法 (Benefit-cost analysis) 对安全防范系统的效能评估, 风险评估模型如下:

$$Risk = P(A) \times p(r) \times C$$

其中, $P(A)$ 为防护目标被攻击的概率, $p(r)$ 为攻击者成功攻击的概率, C 为防护目标的价值. 该方法理论上可实现对风险的定量评估, 但在确定防护目标被攻击的概率阶段依然不能避免人为确定, 实际上攻击者很可能不知道防护目标的价值, 因此其风险评估结果依然存在很大的主观性和不确定性.

综上所述, 当前针对安全防范系统风险评估的研究主要集中在基于构建指标体系的系统效能评估, 主要通过确定评估指标的重要程度, 依靠管理科学的一些评估方法实现对安全防范系统风险进行评估, 其优点是简便易算, 但也存在明显不足, 评估指标的建立和确定其权重的过程中都可能存在人为主观的因素, 因此评价只能是定性的, 不能给出定量的评估, 同时上述评估方法主要是针对单个的安全防范系统的风险评估, 难以对一个区域内的多个安全防范系统组成的安全防范网络的风险进行准确评估.

2 Neyman-Pearson 防护模型与风险熵

安全防范系统是一个复杂系统, 对防护目标的保护受很多因素影响, 致使安全防范系统对目标防护具有不确定性, 本文用安全防范系统对区域内防护目标的保护不确定性程度来度量系统的风险. 对多个安全防范系统组成的安全防范网络, 用攻击者到防护目标的防护最弱的路径度量安全防范网络的风险. 同时, 根据熵理论, 借鉴信息论中信息熵度量信息量的方法, 本文提出风险熵的概念, 利用风险熵度量安全防范系统的防护不确定性, 并通过风险熵建立起防护能力不确定性和系统风险之间的定量的度量关系.

2.1 Neyman-Pearson 防护模型

安全防范系统对目标进行保护主要有 3 个步骤: 探测、延迟和响应. 探测是指及时发现攻击者的攻击行为; 延迟是指通过组织响应的防护力量延迟或阻止攻击者的攻击行为; 响应是指当发现对保护目标的攻击行为后, 对防护目标采取的保护行动. 因此, 安全防范系统对目标的防护过程可抽象地看成是一个决策的过程. 假设用 α 代表安全防范系统的误报警率, 根据 Neyman-Pearson 规则, 安全防范系统对目标防护的最优化等价于在最大可允许的误报警率的前提下, 系统对保护对象提供的最大防护概率. 为定量计算一个安全防范系统对防护区域内各点的防护概率, 本文把安全防范系统发现威胁并处理威胁的过程抽象地看成信号处理的过程, 攻击者可被抽象地看成是安全防范系统被动接收的信号, 根据信号处理相关理论, 假设其为均值为 0、方差为 σ_n^2 的加性高斯白噪声 (Additive white Gaussian noise), 信号的强度随着距离的增加呈指数级减弱, 用 η 代表信号衰减指数, d_{vi} 代表区域内攻击者所在的位置 v 与安全防范系统 S_i 之间的欧氏距离, p_{vi} 代表安全防范系统 S_i 在位置 v 的防护概率. 定义基于 Neyman-Pearson 准则的安全防范系统防护模型如下:

$$p_{vi} = 1 - \Phi\left(\Phi^{-1}(1-\alpha) - \sqrt{\gamma L d_{vi}^{-\eta}}\right) \qquad (1)$$

其中, $\Phi(x)$ 为高斯累计分布函数, 表示随机变量在点 x 服从标准正态分布. L 代表安全防范系统做出决策需要的信号样本数量, 假设信号样本收集的速度足够快, 则在观测期间攻击者与安全防范系统间的距离是恒定的. γ 代表安全防范系统的信噪比, 衡量系统抗干扰的程度. 假设有 4 个安防系统, 相关参数如表 1 所示, 防护能力随着与攻击者或防护目标间的距离的变化关系如图 2 所示.

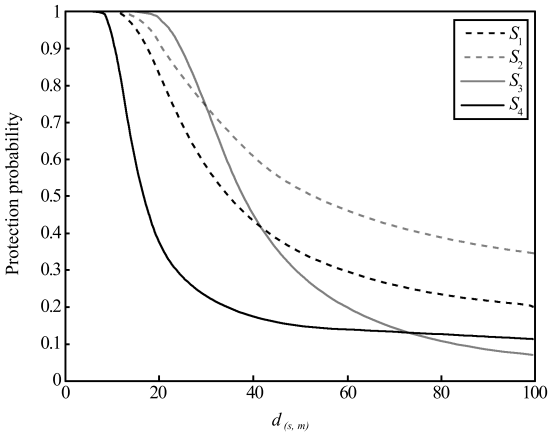


图 2 安防系统 S_1, S_2, S_3, S_4 防护能力的变化趋势

Fig. 2 Sample protection probability of the four security systems

安防系统的误报警率是衡量系统灵敏度的重要指标, 现实中可通过 "技防" 设备的相关设置参数获得, 取值范围一般不高于 0.2. 误报警率越高, 代表系统越灵敏, 反映到现实就是对陌生人或陌生事物很敏感, 等同于增加对陌生事物的盘查力度, 提高误报警率, 可能会浪费人力物力, 但可以显著提高一个地区的安全程度, 这一点通过比较安全防范系统 S_1 和 S_2 可以看出. 系统信噪比 γ 主要用来衡量系统的抗干扰程度, 系统的整体抗干扰越好, 越有利于发挥防护能力, 可以增大一个安全防范系统的绝对有效防护范围 (防护概率为 1). 样本数 L 与区域部署的监控感应设备的数量有关, 一般用于安防的摄像头每秒大概可传送 25 ∼ 50 帧的画面, 如果监控设备很多, 单位时间内安防人员可获得更多区域的安全信息, 便于及时发现和阻止危险发生. 样本数 L 和系统

表 1 4 个安防节点参数信息表

Table 1 Parameter values of four security systems

安防节点	误报警率 α	系统信噪比 γ (dB)	样本数 L	防护衰减参数 η
S_1	0.1	20	100	2
S_2	0.2	20	100	2
S_3	0.01	40	200	2
S_4	0.1	40	200	3

信噪比 γ 都可以影响安全防范系统的绝对有效防护范围的大小. 防护能力衰减参数用于衡量系统设备老化、失效、过期等因素对防护能力的影响, 现实中, 这种情况对安全防范系统的防护能力影响很明显, 这一点从图 2 安全防范系统 S_4 的防护能力变化的趋势可以看出. 同时从图 2 可以看出, 随着距离的增大, 安防节点的防护能力趋近一个恒定的值. 这一现象可通过对式 (1) 求极限得以证明, 分别以 $d \to \infty$, $L \to 0$, $\gamma \to 0$ 和 $\eta \to \infty$ 对式 (1) 求极限, 结果如下:

$$\begin{aligned}&\lim_{d_{vi}\to\infty} p_{vi} = \alpha\\ &\lim_{L\to 0} p_{vi} = \alpha\\ &\lim_{\gamma\to 0} p_{vi} = \alpha\\ &\lim_{\eta\to\infty} p_{vi} = \alpha\end{aligned}$$

一个安全防范系统对目标最小的防护概率等于其误报警率, 反映在现实中相当于安全防范系统仅剩威慑作用.

当区域内部署多个安全防范系统, 这些安全防范系统组成一个安全防范网络, 网络内的安全防范系统称为安全防范网络的安防节点. 此时位置 v 的防护概率 p_v 为

$$p_v = 1 - \prod_{i=1}^{n} (1 - p_{vi}) \tag{2}$$

其中, n 为区域内部署的安防节点的数量.

为便于计算防护区域内各个位置的防护概率, 对防护区域进行网格化抽象处理, 将防护区域划分成对角线互连的正方形. 经网格化处理后, 防护区域可抽象地看成一个离散的点和边构成的图. 定义两个特殊的点分别代表防护区域入口和防护对象所在的位置. 防护区域网格化模型定义如下:

假设区域的长为 N, 宽为 M, 建立二维坐标, 分别对 x 轴和 y 轴做 $N-1$ 等分和 $M-1$ 等分, 区域内任意点的坐标为 (x_v, y_v), 其中 $x_v = 0, 1, \cdots, N-1$, $y_v = 0, 1, \cdots, M-1$, 用 v 代表任意一点 (x_v, y_v) 的编号, $v = y_v N + x_v + 1$. 默认将区域入口点的编号计为 $v = 0$, 防护对象所在的位置点计为 $v = NM + 1$. 用矩阵 $c_{v,w} \in C_{(NM+2)\times(NM+2)}$ 代表区域内各点间的互连信息. $c_{v,m} = 1$ 代表点 v 和点 w 间有一条路径. $c_{v,m} = 0$ 代表两点间没有路径, 矩阵具体定义如下:

$$c_{v,w} = \begin{cases} 1, & \text{若 } 0 < v, w < NM+1 \text{ 且} \\ & \quad (x_v - x_w, y_v - y_w) \in D \\ 1, & \text{若 } v = 0 \text{ 且 } y_w = 0 \\ 1, & \text{若 } w = NM+1 \text{ 且 } y_v = M-1 \\ 0, & \text{否则} \end{cases} \tag{3}$$

其中, $D = \{\{-1, 0, 1\} \times \{-1, 0, 1\}\} - \{(0, 0)\}$. 举一简单示例, 假设一个长 8 米、宽 4 米的防护区域, 经网格化处理后的效果如图 3 所示.

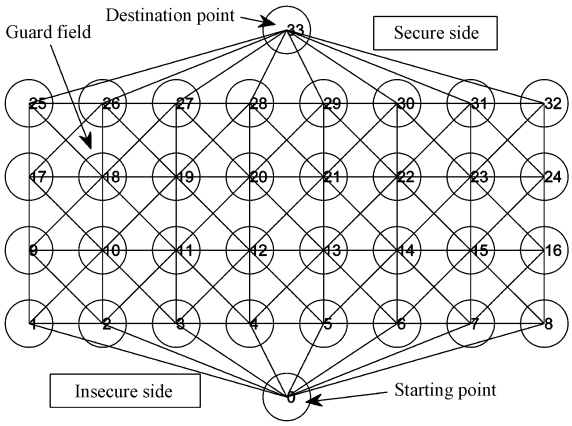


图 3　防护区域网格化示例

Fig. 3　A sample protection area that is gridded

防护区域经网格化处理后, 假设区域内任意一条路径对应的点集合 $V = \{v_1, v_2, \cdots, v_k\}$, 该路径的防护失效概率 p 定义如下:

$$p = \prod_{vi\in V} (1 - p_{vi}) \tag{4}$$

区域内防护最薄弱路径问题等价于找到一条路径, 其防护失效概率最大. 区域内防护最薄弱路径等价于求解如下方程的最优化解.

$$\begin{aligned}&\max \prod_{(i,j)\in C} (1 - p_i)\, x_{ij}\\ &\text{s.t.} \sum_{(s,j)\in C} x_{sj} = 1\\ &\qquad \sum_{(i,d)\in C} x_{id} = 1\\ &\qquad \sum_{(i,d)\in C} x_{ij} - \sum_{(k,i)\in C} x_{kj} = 0,\\ &\qquad\qquad \forall\, i = 1, 2, \cdots, N \times M\\ &\qquad x_{ij} = \begin{cases} 1, & c_{ij} = 1 \\ 0, & c_{ij} = 0 \end{cases}\end{aligned} \tag{5}$$

其中, C 代表区域网格化后的所有的顶点集合, s 代表攻击起始点, d 代表防护目标的位置或攻击目标位置, i 和 j 代表顶点集合 C 中的任意两点, 当 $x_{ij}=1$, 代表顶点 i 和 j 间存在一条路径, 否则顶点 i 和 j 间没有路径. 顶点集合 C 中各点链接关系满足式 (3) 的定义.

2.2 风险熵

熵是法国科学家 Clausius[18] 在 1865 年为完成热力学第二定律的量化问题引进的一个状态函数, 后经奥地利物理学家 Boltzmann 对熵的统计解释, 熵成为一个系统无序或不确定性的度量. 1948 年, 信息论奠基人美国科学家 Shannon[19] 用信息熵度量信息论. 信息熵代表信源的平均不定程度, 信息量是解除不确定程度所需的信息的度量, 信息论中对于一个发生概率为 $p(x_i)$ 的随机事件 x_i 的不确定性的度量模型如下:

$$I(x_i) = -\log p(x_i)$$

其中, $I(x_i)$ 代表随机事件 x_i 的不确定性, 称为自信息.

安全防范系统在区域内某一点的防护概率, 某种意义上代表该点受保护的不确定性, 这种不确定性相当于该点被攻击而发生风险的可能性, 因此借鉴信息论中关于自信息的定义, 本文用熵对某一点防护不确定性进行度量, 称为风险熵, 以此实现对区域内任意一点可能发生的风险进行定量度量. 具体定义如下:

$$I_v = -\log p_v \tag{6}$$

其中, p_v 代表安全防范网络 S 在点 v 的防护概率, 其定义参照式 (2), I_v 代表点 v 的风险熵.

防护区域经网格化处理后, 假设区域内任意一条路径对应的点集合 $V=\{v_1, v_2, \cdots, v_k\}$, 该路径的风险熵 $I(V)$ 定义为

$$I(V) = \sum_{v_i \in V} I_{vi} \tag{7}$$

假设通过式 (5) 找到区域内防护最薄弱路径, 其对应的点集合为 $V_{\max}$, 则安全防范网络的风险 $R(S)$ 定义为

$$R(S) = \frac{I(V_{\max})}{n} \tag{8}$$

其中, n 代表防护最薄弱路径上顶点的个数.

3 仿真实验与分析

3.1 安全防范网络防护最薄弱路径

假设在长 100 米、宽 60 米的区域内部署由 5 个安防节点组成的安全防范网络, 安防节点的位置信息与相关参数如表 2 所示, 攻击的起始点为 $(0, 0)$, 防护目标位置为 $(100, 60)$. 根据本文提出的风险评估模型, 安全防范网络的防护最薄弱路径相当于求解方程 (5) 的最优解, 通过使用对数函数可将方程式 (5) 转化成线性规划的问题, 具体转化如下:

$$\min \sum_{(i,j)\in C} -\log(1-p_i)x_{ij}$$

防护区域经网格化处理后, 可被抽象地看成一个图, 上述线性规划问题等同于寻找图的最短路径问题, 图中每个点的权重为 $-\log(1-p_i)$, 其中 p_i 是安全防范网络在点 i 的防护概率, 采用 Dijkstra 最短路径算法找到的最短路径即为防护最薄弱路径. 首先通过式 (1) 求出各安防节点在区域网格化后的各顶点的防护概率, 通过式 (2) 求出 5 个安防节点组成的安全防范网络在每个点的防护概率; 随后基于防护概率和网格化模型, 可给出安全防范网络在区域上的防护概率分布二值图像, 如图 4 (b) 所示, 图中圆圈代表安防节点的位置. 黑色星号形状的是以本文提出的以防护失效概率为权重的防护最薄弱路径.

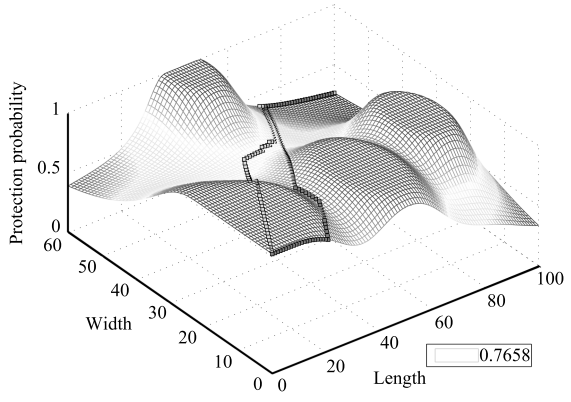
根据基于构建评估指标的方法, 如 Sendi 等[4] 提出的风险评估方法, 将 5 个安防节点组成的网络看成一个系统, 建立相应的评估指标, 通过专家打分得出系统的风险评估值, 根据评估值所在区间给出系统的风险级别, 此类方法仅针对单路径防护的情况, 即从入口到目标仅有一条路径, 所有安防节点均

表 2 5 个安防节点参数信息表

Table 2 Parameter values of five security systems

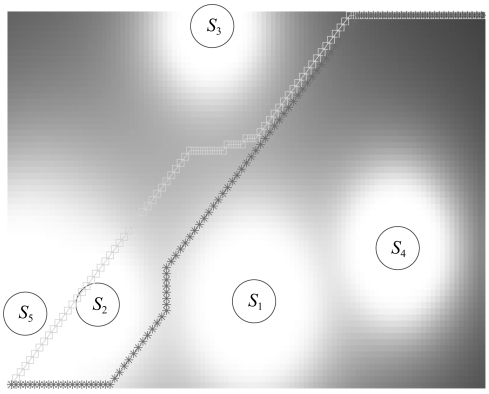
安防节点	误报警率 α	系统信噪比 γ (dB)	样本数 L	防护衰减参数 η	x 坐标	y 坐标
S_1	0.01	20	120	2	52	14
S_2	0.02	15	180	2.5	18	13
S_3	0.03	14	70	2	43	58
S_4	0.01	30	80	2.2	82	22
S_5	0.01	25	100	1.8	3	12

在该路径上. 对核反应材料和重大危险品的安防系统通常采用单路径的防护模型, 但对公共安全防护的安防系统通常采用多路径的防护模型, 因此传统指标的风险评估方法很难适合多路径防护的安防系统的风险分析. 美国桑迪亚国家实验室研究员 Garcia[12] 在敌手序列图的基础上提出多路径的分析方法, 即对区域进行网格化划分, 根据安防节点的防护能力随着距离的增大而逐渐衰减的特性, 通过各网格顶点到安防节点的距离计算安防节点在各顶点的防护概率, 利用图论相关知识找到防护最弱路径, 根据 Garcia[12] 的方法, 以防护概率为网格顶点的权重, 求得防护最薄弱路径如图 4 中的浅色空心矩形的路径.



(a) 防护最薄弱路径的三维展示

(a) The most vulnerable path shown in three-dimensional space



(b) 防护最薄弱路径的二维展示

(b) The most vulnerable path shown in two-dimensional space

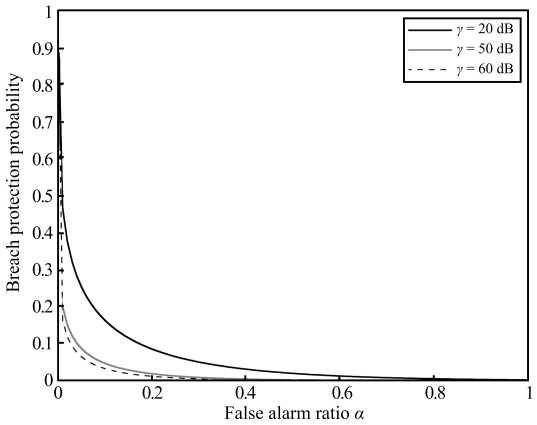
图 4　安全防范网络的防护最薄弱路径

Fig. 4　The most vulnerable path of a security network

图 4 (b) 是在以安全防范网络在区域内的防护概率分布的二值图像上, 对比展示以本文提出的基于防护失效概率的防护最薄弱路径和以防护概率为权重的最短路径, 不难看出, 基于本文提出方法的路径更为合理. 根据式 (8) 可求得安全防范网络的风险为 0.4619. 本例假设的是一个攻击点和一个防护目标, 根据图论的知识易于扩展到多个攻击点和多个防护对象.

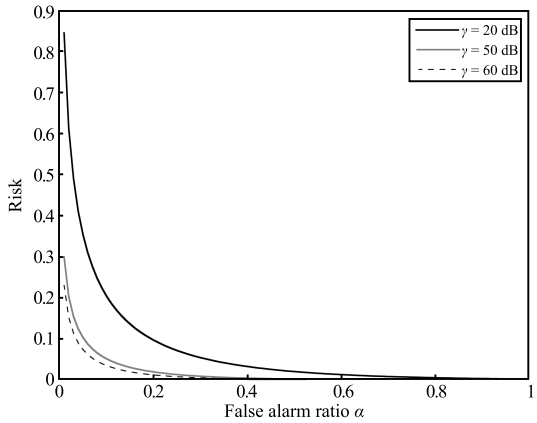
3.2　Neyman-Pearson 防护模型参数与防护概率和风险的关系

在第 3.1 节讨论了单个安防系统条件下, 模型各参数对防护概率的影响. 本节以图 4 所示的安全防范网络为基础, 讨论模型参数对多个安防节点组成的安全防范网络的影响. 在区间 $[0, 0.3]$ 平均取 100 个值分别作为 5 个安防节点的误报警率, 分别针对系统的信噪比 $\gamma = 20\,\mathrm{dB}$、$\gamma = 50\,\mathrm{dB}$ 和 $\gamma = 60\,\mathrm{dB}$ 三种情况对区域的防护最薄弱路径的防护失效率和风险进行统计, 如图 5 所示. 从仿真结果可以看出, 误报警率 α 对安全防范网络的防护失效率和风险的影响很大, 增加误报警率可迅速降低区域的风险.



(a) 对防护失效率的影响

(a) The effect of α on breach protection probability



(b) 对风险的影响

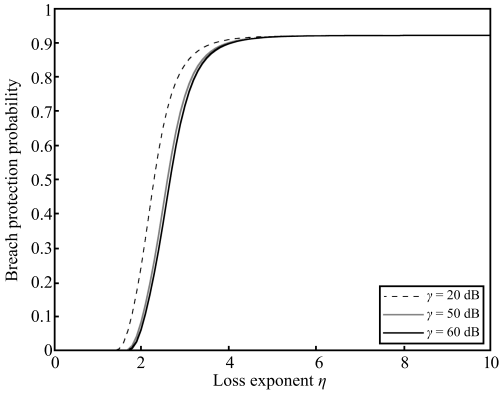
(b) The effect of α on risk

图 5　误报警率对安全防范网络风险的影响

Fig. 5　The effect of α on the risk and breach protection probability of a security network

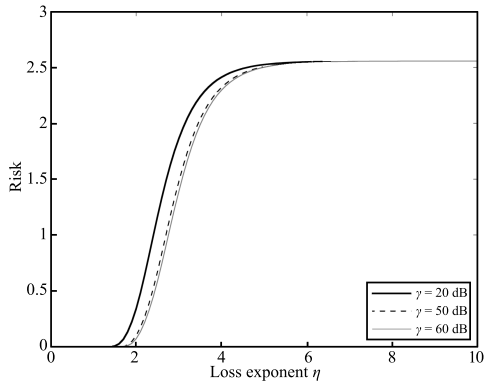
同样以图 4 中安全防范网络为对象, 研究防护

衰减参数对安全防范网络的影响, 在区间 $[0.1, 10]$ 平均取 100 个值分别作为 5 个安防节点的防护衰减参数, 分别针对系统的信噪比 $\gamma = 20\,\mathrm{dB}$、$\gamma = 50\,\mathrm{dB}$ 和 $\gamma = 60\,\mathrm{dB}$ 三种情况对区域的防护最薄弱路径的防护失效率和风险进行统计, 如图 6 所示. 随着 η 的增大, 安全防范网络的防护能力衰减的速度越快, 其防护失效概率和风险也越大. 从图 6 可以看出, 当衰减参数增大到一定数值时, 区域的风险和防护失效率都趋于一个恒定的值, 这是因为每个安防节点对攻击者或目标的最小的防护概率等于其误报警率, 关于此观点可参见第 3.1 节的相关论述. 现实中, 可能因为设备老化或人员变动等原因, 一个安全防范网络可能会失去防护能力, 但只要其存在, 就依然能对攻击者起到震慑作用, 即等效于对防护目标依然有保护作用.



(a) η 对防护失效率的影响

(a) The effect of η on breach protection probability



(b) η 对风险的影响

(b) The effect of η on risk

图 6 误报警率对安全防范网络风险的影响

Fig. 6 The effect of η on the risk and breach protection probability of a security network

现实中某个区域在进行安全防范系统部署的过程中, 经常遇到一个区域应该部署多少个安防节点的问题. 运用本文提出的模型和方法可近似解决该问题. 仍以图 4 中的区域为例, 假设目前有 5 种安防节点, 参数信息如表 2 所示. 运用模型建立区域内节点数量与区域防护失效概率间的关系, 如图 7 所示. 从图 7 可大致判断, 如需把 100×60 区域的防护失效率或风险控制在 0.1 以下, 大概需要 5 个 S_5, 或 13 个 S_3, 或 17 个 S_1, 或 35 个 S_4, 或 50 个 S_2. 虽然这是一个大概的估计, 但对安全防范系统部署施工有一定的指导意义.

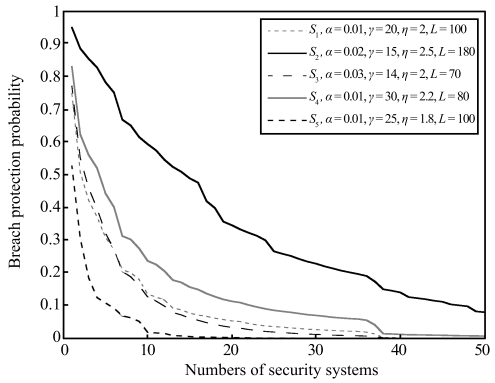


图 7 安防节点个数对安全防范网络防护失效概率的影响

Fig. 7 The effect of numbers of security and protection systems on the breach protection probability

3.3 应用实例

现实中某小区, 如图 8 所示, 楼间距约为 100 米, 有 9 个安防节点, 将安防节点、小区道路和建筑物抽象为一个图. 现实中很多路不是完全直线, 在评估过程中都近似看成直线, 小区的保安主要通过安防监控中心的画面判断是否有紧急情况, 一边的监控摄像头每秒可传输大约 25～50 帧画面, 小区的监控探头一般都是每条路对射, 一些生理学和心理学的研究成果表明, 人对画面的注意时间为 3～4 秒, 如果这段期间不能引起注意, 画面一般不会被大脑深度记忆, 由此大概可假设小区的安防监控点每秒获得的数据样本约在 100～200 个之间, 通过对小区内 9 个安防点相关设置的查看与评估, 相关参数如表 3 所示. 运用本文提出的模型和方法, 可分别求出入口到每栋楼的防护最薄弱路径, 如图 9 所示. 其中方框代表小区的楼栋, 具体与图 8 相对应, 方框下面的数字代表根据本文提出模型和方法计算出的风险值.

4 结论

针对当前难以对多安防节点所形成的安全防范网络的风险进行定量科学评估的问题, 本文提出了基于风险熵和 Neyman-Pearson 准则的安全防范网络风险评估模型, 通过该模型可以定量计算防护区域内某个安防节点在区域内各个位置的防护概率, 并以此为基础, 通过对防护区域进行网格化处理, 将防护区域内的安防节点以及区域内的道路抽象成一个图,利用图论的相关知识确定安全防范网络的防护

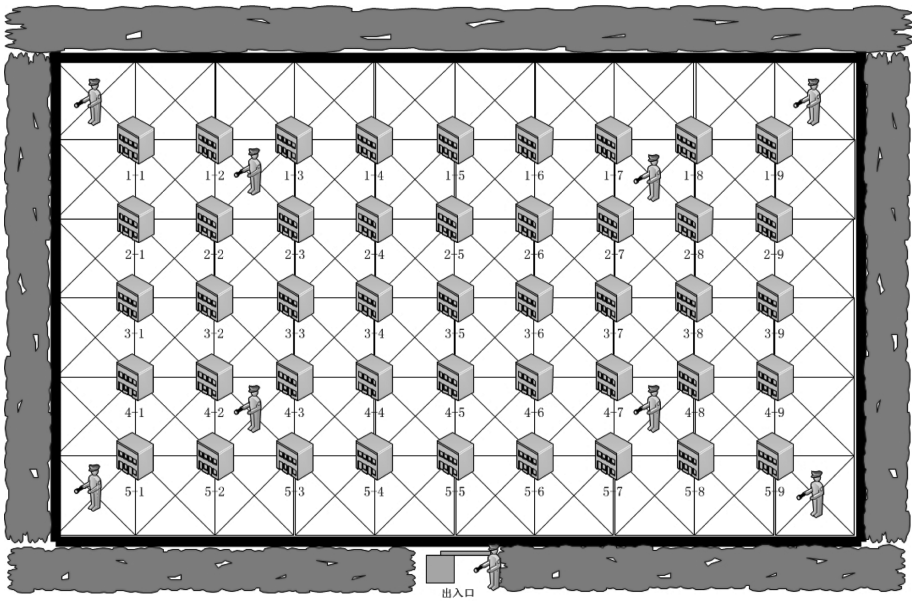


图 8　某小区安保结构图

Fig. 8　The distribution of security systems in a district

表 3　某小区 9 个安防节点参数信息表

Table 3　Parameter values of nine security systems in a district

安防节点	误报警率 α	系统信噪比 γ (dB)	样本数 L	防护衰减参数 η	x 坐标	y 坐标
S_1	0.05	20	100	2	50	50
S_2	0.01	40	100	2.5	500	0
S_3	0.05	20	100	2	950	50
S_4	0.1	40	150	2.2	250	150
S_5	0.1	40	150	1.8	750	150
S_6	0.1	40	150	2.2	250	450
S_7	0.1	40	150	1.8	750	450
S_8	0.05	20	100	2.2	50	550
S_9	0.05	20	100	1.8	950	550

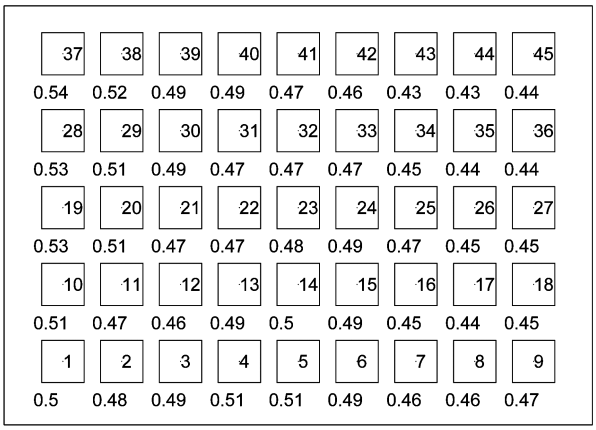


图 9　某小区风险分布图

Fig. 9　The risk distribution of a district

最薄弱路径, 从而实现对安全防范网络的风险的评估. 最后通过 Matlab 对本文提出的模型和方法进行仿真. 结果表明, 本文提出的模型和方法具有合理性, 对现实中安全防范系统的风险评估和部署有一定的指导意义.

现实中安全防范系统应该是有生命周期的, 一个安全防范系统的防护资源耗尽后, 该安全防范系统将会失效, 某个安全防范系统的失效肯定会对整个安全防范网络的风险产生影响. 本文没有考虑安全防范系统失效的情况, 在下一步的研究中将考虑安全防范网络中某些安防节点 (安全防范系统) 失效的情形, 以及防护区域的形状对区域内整个安全防护网络风险的影响.

References

1 Li Ben-Xian, Li Meng-Jun. The simulation of fear diffusion based on parallel system under the paroxysmal terrorism incident circumstance. *Computer Engineering and Application*, 2012, **38**(8): 1321−1328
(李本先, 李孟军. 基于平行系统的恐怖突发事件下恐惧传播的仿真

研究. 自动化学报, 2012, **38**(8): 1321−1328)

2 Zheng Zhou-Yi, Du Zhi-Guo, Wang Xin. Visual implementation for vulnerability assessment algorithm of security and protection systems. *Computer Engineering and Application*, 2014, **50**(5): 70−73
(郑舟毅, 杜志国, 王欣. 安防系统弱点评估算法的可视化实现. 计算机工程与应用, 2014, **50**(5): 70−73)

3 Guo Xi, Hu Rui-Min. The effectiveness evaluation for security system based on risk entropy model and Bayesian network theory. In: Proceedings of the 2010 IEEE International Carnahan Conference Security Technology ICCST. San Jose, CAL: IEEE, 2010. 57−65

4 Sendi A S, Jabbarifar M, Shajari M, Dagenais M. FEMRA: fuzzy expert model for risk assessment. In: Proceedings of the 5th Inter National Conference on Internet Monitoring and Protection. Barcelona: IEEE, 2010. 48−52

5 Zhu Zong-Lin, Guo Shi-Min. Research for automatic control equipment system Synthetical evaluation. *Acta Automatica Sinica*, 1999, **25**(2): 59−63
(朱宗林, 郭世民. 自动控制装置系统综合评估研究. 自动化学报, 1999, **25**(2): 59−63)

6 Wu Qiong, Yan Li-Li. The risk evaluation research of enterprise security and protection systems. *Security Science and Technology*, 2010, **9**(10): 10−14
(吴穹, 闫黎黎. 企业安全防范系统风险评价模式研究. 安防科技, 2010, **9**(10): 10−14)

7 Huang Min, Yang Hong-Mei, Wang Xing-Wei. Genetic algorithm and fuzzy synthetic evaluation based risk programming for virtual enterprise. *Acta Automatica Sinica*, 2004, **30**(3): 449−454
(黄敏, 杨红梅, 王兴伟. 基于遗传算法和模糊综合评价的虚拟企业风险规划. 自动化学报, 2004, **30**(3): 449−454)

8 Xu Tian-Kun, Liang Qing-Huai, Ren Xing-Chen. Risk assessment of metro DC750V power supply system operation based on fault tree model. *Journal of Beijing Jiaotong University*, 2012, (6): 57−62

9 Doyon L R. Stochastic modeling of facility security-systems for analytical solutions. *Computers and Industrial Engineering*, 1981, **5**(2): 127−138

10 Hug G, Giampapa J A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 2012, **3**(3): 1362−1370

11 Hicks M J, Snell M S, Sandoval J S, Potter C S. Physical protection systems cost and performance analysis: a case study. *Aerospace and Electronic Systems Magazine*, 1999, **14**(4): 9−13

12 Garcia M L. *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann, 2001. 135−149

13 Garcia M L. *Vulnerability Assessment of Physical Protection Systems*. Boston: Butterworth-Heinemann, 2005. 123−144

14 Fischer R J, Halibozek E P, Walters D C. *Introduction to Security*. Boston: Butterworth-Heinemann, 2012.

15 Xu P, Su X, Wu J, Sun X, Zhang Y, Deng Y. Risk analysis of physical protection system based on evidence theory. *Journal of Information and Computational Science*, 2010, **7**: 2871−2878

16 Xie Lei, Feng Hao, Zhang Jian-Ming. A new approach to performance assessment based on initial closed-system. *Acta Automatica Sinica*, 2013, **39**(5): 649−653
(谢磊, 冯皓, 张建明. 一种基于初始闭环系统的性能评估方法. 自动化学报, 2013, **39**(5): 649−653)

17 Dai J J, Hu R M, Chen J, Cai Q. Benefit-cost analysis of security systems for multiple protected assets based on information entropy. *Entropy*, 2012, **14**(3): 571−580

18 Clausius R. *The Mechanical Theory of Heat: with Its Applications to the Steam-Engine and to the Physical Properties of Bodies*. London: John van Voorst, 1867

19 Shannon C E. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2001, **5**(1): 3−55

胡瑞敏 武汉大学计算机学院教授. 分别于 1984 年、1990 年和 1994 年获得南京邮电学院学士、硕士和华中科技大学工学博士学位. 主要研究方向为安防应急通信信息系统, 音视频编解码和视频监控与多媒体数据处理.
E-mail: hurm1964@gmail.com
(**HU Rui-Min** Professor at the School of Computer, Wuhan University. He received his bachelor and master degrees from Nanjing University of Posts and Tele-communications in 1984 and in 1990, and Ph. D. degree in communication and electronic system from Huazhong University of Science and Technology in 1994. His research interest covers communication and information systems of security and protection systems, audio/video coding and decoding, video surveillance and multimedia data processing.)

吕海涛 武汉大学国家多媒体软件工程技术研究中心博士研究生. 分别于 2002 年和 2006 年获得解放军信息工程大学计算机系学士学位和华中科技大学计算机系硕士学位. 主要研究方向为安防应急通信信息系统. 本文通信作者.
E-mail: lvhaitao0301@gmail.com
(**LV Hai-Tao** Ph. D. candidate at the National Engineering Research Center for Multimedia Software, Wuhan University. He received his bachelor degree in computer science from PLA University of Information Science and Technology in 2002 and master degree in computer science from Huazhong University of Science and Technology in 2006. His research interest covers communication and information systems of security and protection systems, video surveillance and multimedia data processing. Corresponding author of this paper.)

陈 军 武汉大学教授. 1997 年在华中理工大学自动控制系自动化仪表专业获得硕士学位, 2007 年在武汉大学国家多媒体软件工程技术研究中心获得博士学位. 主要研究方向为多媒体网络通信, 安防应急信息处理和多媒体应用系统.
E-mail: chenj@whu.edu.cn
(**CHEN Jun** Professor at Wuhan University. He received his master degree in instrumentation from Huazhong University of Science and Technology in 1997, and his Ph. D. degree in photogrammetry and remote sensing from Wuhan University in 2007. His research interest covers multimedia communications and security emergency information processing.)