基于 D-S 证据理论的无线传感器网络 MAC 层安全研究 *

张聚伟[1,2]，孙雨耕[2]，杨 挺[2]
（1. 河南科技大学 电子信息工程学院，河南 洛阳 471003；2. 天津大学 电气与自动化工程学院，天津 300072）

摘 要：研究了无线传感器网络 MAC 层安全问题，分析了现有无线传感器网络 MAC 层协议安全体系的不足之处，针对无线传感器网络遭到非法入侵的情况，提出了一个基于 D-S 证据理论的 MAC 层入侵检测机制。该机制利用碰撞率、数据包平均等待时间、RTS 包到达率以及邻居节点的报警作为证据，对网络的状态进行实时的分析检测，根据网络的状态作出响应。该算法能够应用于现有的 MAC 协议如 S-MAC、IEEE 802.15.4 中，仿真结果表明，该算法能够较好地抵御针对 MAC 层的攻击，保证网络的安全运行。

关键词：介质访问控制层协议；安全；D-S 证据理论；无线传感器网络；入侵检测
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2009)01-0330-04

Research on MAC security based on D-S evidence theory in wireless sensor networks

ZHANG Ju-wei[1,2], SUN Yu-geng[2], YANG Ting[2]
(1. *School of Electronic Information Engineering, Henan University of Science & Technology, Luoyang Henan* 471003, *China*; 2. *School of Electrical Engineering & Automation, Tianjin University, Tianjin* 300072, *China*)

Abstract: This paper considered the security problem at MAC layer in wireless sensor networks, analyzed the security defects in current works on MAC protocols, and then presented a intrusion detection system(IDS) on MAC layer based on D-S evidence theory for the condition that current security system was broken down. In the IDS, selected the collision ratio, data packet's waiting time, RTS packets arrival ratio and the other nodes' alarms as evidences to detect the attacks such as collision attack, unfairness attack and exhaustion attack. This IDS can be used in S-MAC, IEEE 820.15.4 directly. To evaluate the performance of the system, analyzed the IDS with NS-2, the results show that the IDS can defense attacks on MAC layer, and guarantee the wireless sensor networks work well.

Key words: MAC layer; security; D-S evidence theory; wireless sensor networks; intrusion detection system

0 引言

无线传感器网络是近年来出现的一种 Ad hoc 类网络，由大量微型廉价的传感器节点组成，这些节点通过飞机抛撒或炮弹发射到观察者不能或不方便到达的区域，通过无线信号以一跳或多跳的方式形成一个自组网，协作地感知被监测区域的信息，并发布给观察者[1,2]。无线传感器网络具有十分广阔的应用前景，在军事国防、生物医学、环境监测等许多重要领域均有潜在的实用价值。

针对无线传感器网络的不同应用，目前国内外均提出了较多的介质访问控制(medium access control，MAC)协议[3~7]。这些协议从节省能量、可扩展性、网络效率(包括网络的公平性、吞吐量、实时性、带宽利用率等)方面对传感器网络 MAC 层进行了研究，而在网络的安全性方面考虑不多。本文针对这一问题，对现有的 MAC 协议进行了研究分析，提出了一个基于 D-S 证据理论的安全 MAC 入侵检测方案(以下称为DS-MAC)，同时利用 NS2 网络模拟器对该方案进行仿真分析。

1 无线传感器网络链路层安全分析

1.1 常见的无线传感器网络链路层安全体系

IEEE 802.11 的安全方案有线等效私密性(wired equivalent privacy，WEP)已经被证明在身份认证、密钥管理等方面存在着诸多的缺陷，2001 年底，在因特网上已经可以找到相应的工具在很短时间内就可以攻破 WEP。为了解决这些问题，IEEE 802.11i 为 IEEE 802.11 提出了一系列的解决方案，但是该标准不能解决 DoS 攻击的问题。

IEEE 802.15.4[8] 标准覆盖了低速率个域网的物理层和 MAC 层，其设计目标是在无线传感器网络、家庭自动化、家庭设备等领域中的应用，该标准综合了前两类协议的方式，具有低能耗、低成本的特点，尤其适合于无线传感器网络。IEEE 802.15.4 提供了三种安全模式[8]，即非安全模式、接入控制列表(ACL)安全模式和安全模式。在第一种模式下不提供安全

收稿日期：2008-03-06；**修回日期**：2008-05-27 **基金项目**：国家自然科学基金资助项目(60702037)；国家教育部博士点学科基金资助项目(20030056007)；中国博士后科学基金资助项目(2006040018)；河南科技大学博士科研启动基金资助

作者简介：张聚伟(1978-)，男，河南伊川人，讲师，博士，主要研究方向为无线传感器网络、信息安全等(juweizhang@hotmail.com)；孙雨耕(1940-)，男，教授，博导，主要研究方向为电路理论、图论与网络优化、无线传感器网络等.

服务;ACL 模式提供了一种方法让设备根据帧中的源地址对接收到的帧进行过滤,但是这种方法不能安全地确定由哪个设备发送该帧,不能抵御重放攻击;安全模式可以提供访问控制、数据加密、保证帧完整性、序列更新四种服务。这些安全服务在一定程度上保证了网络的安全性,但是还有较多的不足之处,不能解决针对 MAC 层的泛洪攻击、碰撞攻击、耗尽攻击、不公平竞争攻击等。

1.2　针对 MAC 层的攻击

无线传感器网络的 MAC 协议大致可分为三类:

a)基于带冲突避免的载波侦听多路访问(CSMA with collision avoidance, CSMA/CA)协议。IEEE 802.11 协议[9]中的 DCF 控制方式是这种基于 CSMA 类协议的代表。在此基础上,研究者提出了较多的基于 CSMA/CA 方式的 MAC 层协议。常见的有 S-MAC[3]、T-MAC[4]、Sift[5]协议等。

b)采用基于时间表的 TDMA(time division multiple access)类协议。这类协议常见的有 Leach[6]、TRAMA[7]等。

c)其他类型的协议,如采用 CDMA(code division multiple access)或 FDMA(frequency division multiple access)方式的协议等。

这三类协议中,较常见的是前两类,第三类在无线传感器网络中采用较少。本文主要针对第一类协议进行研究。

无线传感器网络 MAC 层遇到的攻击主要有以下几种[10,11]:

a)碰撞攻击。由于无线信道的开放性,如果两个设备同时进行发送,那么它们的输出信号会因相互叠加而不能够被分离出来。在数据帧中如果有一个字节在传输过程中发生了碰撞,那么整个包均要被丢弃。攻击者利用无线信道的这种特性,在检测到其他节点发送数据的同时发送干扰数据,这样导致数据的传送失败,这种攻击称为碰撞攻击。

b)耗尽攻击。就是利用协议漏洞,通过持续通信的方式使节点能量资源耗尽。在基于 RTS/CTS/ACK 机制的 MAC 协议中,攻击者发出 RTS 请求帧时,接收者必须发送 CTS 帧进行确认,但是接收者不能分辨出发送者是否恶意节点,在这种情况下,攻击者通过不断地发送 RTS 控制类帧,接收者被迫回复 CTS 控制帧,最终接收者的能量被耗尽。在 IEEE 802.15.4 中,主协调器收到请求数据发送命令时,返回一个确认帧。如果主协调器中存在有要传送给该从设备的数据,主协调器将采用 CSMA/CA 机制,向从设备发送数据帧;如果不存在,则主协调器将发送一个净荷长度为 0 的数据帧;恶意节点可以连续不断地发送数据请求帧,从而耗尽主协调器的能量。

c)非公平竞争攻击。在基于 CSMA/CA 机制的 MAC 层协议中,每一个节点均以相同的优先级访问信道。当某一个节点获得信道时,其他节点必须等待随机时间,再次尝试发送数据,每一个节点均执行相同的退避算法从而保证每一个节点均有相同机会访问信道。但是恶意节点或被俘节点在选择随机时间时,可以选择非常小的等待时间,获得更高的优先级来访问信道,从而导致其他节点在通信过程中处于劣势,降低整个网络的通信效率。

1.3　入侵检测与防御

传统的安全机制如加密、数字签名、认证协议等仍然在无线传感器网络安全中起着重要的作用,但是在无线传感器网络的某些应用(如军事等)中,节点往往被部署在敌方或战场上,一旦节点被俘获重新编程或密钥泄露,敌方就获得了合法进入网络的手段,很容易对 MAC 层发起前文所述的攻击。对这些攻击进行防御,入侵检测机制是重要的手段之一。在无线传感器网络受到攻击时,网络的一些运行数据就会发生很大的变化。在进行入侵检测时,网络异常特征的选取是非常重要的。一般均依赖于专家的经验,选取的标准在于:选取的特征对正常和异常的区分度较高,且获得该特征所需的计算量较小。本文选取如下几个网络运行指标[10]:

a)碰撞率(R_c)。该率是一段时间内某个节点平均每秒检测到的无线信号碰撞数。

b)平均等待时间(T_w)。T_w 是数据包在 MAC 层的数据缓冲区中的平均等待传输时间。

c)RTS 包到达率(R_{RTS})。R_{RTS} 是一段时间内某个节点每秒平均收到的 RTS 请求的个数。

2　基于 D-S 证据理论的安全 MAC 协议

2.1　D-S 证据理论[12]

D-S 证据理论讨论了一个辨识框架 Θ,Θ 是关于命题的相互独立的可能答案或假设的集合。对某个事件的肯定与否定不是简单的真与伪的判断,而是有测度的。D-S 证据理论的目的是根据一些对系统状态的观察 $E_1, E_2, \cdots, E_n$ 推测出系统目前所处的状态。

定义 1　设 Θ 为识别框架,如果集函数 $m: 2^{\Theta} \to [0\ 1]$(2^{Θ} 为 Θ 的幂集)满足 $m(\Phi)=0$, $\sum_{A\subset\Theta} m(A)=1$,则称 m 为识别框架 Θ 上的基本可信度分配,$m(A)$称为 A 的基本可信数。称由 $\mathrm{Bel}(A)=\sum_{B\subset A} m(B)$ $(\forall A\subset\Theta)$ 定义的函数 $\mathrm{Bel}: 2^{\Theta}\to[0\ 1]$ 为 Θ 上的信度函数。

信度函数反映了某个证据支持某个系统状态的概率函数。

为了利用多个证据,D-S 证据理论提出了多个证据的组合规则,即

定义 2　Dempster-Shafer 合成法则。设 m_1 和 m_2 为两个证据的信度分配函数,则由这两个证据的组合证据的信度分配函数为

$$m_1(A)\oplus m_2(A)=K^{-1}\sum_{A_i\cap B_j=A} m_1(A_i)m_2(B_j),\ A\neq\Phi$$

其中:$K=1-\sum_{A_i\cap B_j=\Phi} m_1(A_i)m_2(B_j)$。

2.2　基于 D-S 证据理论的入侵检测模型

根据 D-S 证据理论,设计出了一个入侵检测模型,如图 1 所示。取辨识框架 Θ 为 $\{N,A\}$,N 为正常、A 为异常,$N\cap A=\Phi$,信度分配函数为 $M(\{N\},\{A\},\{N,A\})$,$M(\{N\})+M(\{A\})+M(\{N,A\})=1$。这里,$M(\{N\})$表示当前特征支持正常行为的信度;$M(\{A\})$表示当前特征支持异常行为的信度;$M(\{N,A\})$表示根据该证据不能确定是正常还是异常行为。

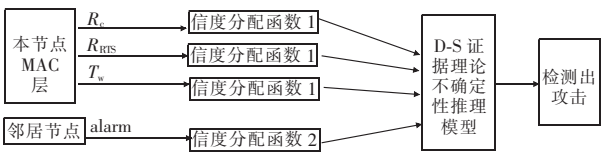

图 1　D-S 证据理论入侵检测模型

在进行入侵检测时,节点收集本节点上 MAC 层的运行特征数据作为置信度函数的输入,得到各个特征数据的信度;同时,将邻居节点是否有报警也作为一个证据输入;然后通过定义 2 的 D-S 证据理论合成法则进行不确定性推理,最终作出是

否有恶意节点攻击的结论。

2.3　信度分配函数的选择

2.3.1　信度分配函数 1 的选择

信度分配函数表示证据对某个模式的支持程度,带有一定的主观性,不同的想法构成不同的信度分配函数,为了更好地对辨识框架 Θ 进行辨识,信度分配函数的选择是十分重要的也是比较困难的。信度分配函数 1 需要将一个变化范围较大的数映射到[0 1]内,根据这种要求,笔者选择 S 型函数[10]:

$$y(x) = 1/(1 + e^{-A(x-C)}) \tag{1}$$

式(1)的图形如图 2 中所示,是一个 S 型曲线。由图 2 可以看出 y 的值存在于[0 1]内,同时斜率和位置可调,可以实现输入到[0 1]内的非线性映射,符合信度分配函数的要求。

参数 A 决定了图2 中曲线的斜率,参数 C 决定了曲线在坐标轴上的位置,A 和 C 的获得通过自适应算法训练得到。

为了获得合适的参数 A 和 C,采用下面训练方法[13]:

选取的代价函数为

$$E(x) = (y_d - y)^2 \tag{2}$$

其中:y_d 是期望值;y 是实际值。

问题在于如何调节 A 和 C 使得代价函数 $E(x)$ 最小,优化计算的方法很多,一般采用一阶梯度法,也叫最速下降法[10,13]。一阶梯度法寻优的关键是计算优化目标函数 E 对寻优参数的一阶导数:

$$\partial E/\partial C = 2(y_d - y)[-Ae^{-A(x-C)}]/[1 + e^{-A(x-C)}]^2 \tag{3}$$

$$\partial E/\partial A = 2(y_d - y)A/[1 + e^{-A(x-C)}]^2 \tag{4}$$

这样可得到 A 和 C 的计算方法:

$$A(k+1) = A(k) + \alpha(\partial E/\partial A) \quad 0 < \alpha < 1 \tag{5}$$

$$C(k+1) = C(k) + \alpha(\partial E/\partial C) \quad 0 < \alpha < 1 \tag{6}$$

其中:α 是学习的速率,取值为 0 ~ 1。

在实际应用中,可采用如下方式确定 A 和 C:在放置节点前,根据网络环境的复杂度,使用网络仿真器对网络环境进行仿真模拟,利用仿真结果首先在普通计算机上求出 A、C 的值,将结果预先写入节点中,节点再根据实际的网络环境对 A 和 C 进行微调节,这样可省去较多计算量,更易于找到最优参数。

2.3.2　信度分配函数 2 的选择

信度分配函数 2 是用于分配邻居节点报警信号的信度。当某节点通过入侵检测模块检测出网络受到攻击时,该节点向其他邻居节点发出报警信号,邻居节点在收到报警信号后,通过入侵检测模块通知上层协议栈或控制物理层进行进一步的处理。因此信度分配函数 2 比较简单:

$$y(n) = \begin{cases} 0.5 & n \leqslant \Delta \\ 0.9 & n > \Delta \end{cases} \tag{7}$$

式中:Δ 为常数;n 为报警的节点个数。当有低于 Δ 个节点报警时,有可能为误报或是攻击者释放的假信息,因此分配信度为 0.5;当有多于 Δ 个节点报警时,则几乎可以确定有网络攻击,因此分配信度为 0.9。

2.4　防御模块

在入侵检测模块检测出网络攻击后,必须采取防御措施使得网络攻击造成损失最小。防御模块如图 3 所示。入侵检测模块向协议栈各层均发出通知,网络中的各层根据不同的攻击采用相应的措施,这里简单介绍几种方法:

针对碰撞攻击,MAC 层可采用的方法有[11]:a)降低本节点工作的占空比。在敌方进行攻击时进入睡眠状态,定时检测攻击是否仍然存在。如果探测到攻击方停止攻击,则恢复正常工作。b)使用纠错码通过在通信数据包中增加冗余信息来纠正数据包中的数据。

针对耗尽攻击,则可以将恶意节点列入黑名单,拒绝与恶意节点通信。

在检测到有不公平竞争攻击时,可以采取一定的惩罚措施,将本节点与恶意节点的通信量降低。

当网络层接收到本节点受到攻击的信号时,可以重新启动路由算法,绕开恶意节点或受攻击节点,寻找新的路由,从而保证数据的传输。

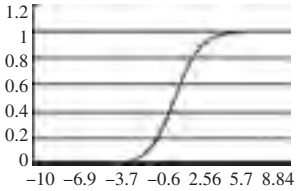

图 2　信度分配函数 1

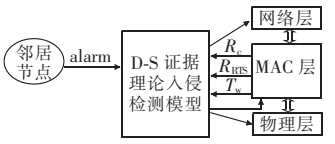

图 3　系统防御模块

3　算法分析与仿真验证

在本文中,难度主要来自于对参数 A 和 C 的确定,由于抛撒节点之前已经对网络进行了仿真,A、C 的值离理想值的位置已比较接近,为了更好地对入侵节点进行辨识,在网络运行时还需要对 A、C 进行微调节。在计算式(3)(4)时,需要花费较多的计算量,但是信度分配函数无须过高的精确度,精确至 0.05 左右,可采用查表法进行计算。本算法实现简单,可以很方便地嵌入到 IEEE 802.11 或 IEEE 802.15.4 协议中,而无须对这些协议进行修改。

为了对算法的性能进行测试,笔者利用 NS2 网络模拟器在 Cygwin 环境下进行了仿真实验。在 1 000 m × 1 000 m 的范围内放置 50 个节点,节点的初始能量为 2 J,MAC 层采用 IEEE 802.11。当节点数目相同时,针对不同的拓扑,算法的相关性能如能耗、安全性等可能相差很大;为了对算法进行对比,只对节点抛撒一次,利用一个拓扑内进行仿真。

仿真结果如图 4 所示。图 4 中 normal 为网络正常运行时的节点平均能量变化曲线,attack1 和 attack2 分别为网络中有一个和两个恶意节点的情况,detection 是在协议中加上本文提出的 IDS 的结果。由图 4 中可以看出,在网络受到恶意攻击时节点的平均能量快速下降,由曲线的斜率可看出,其下降速度远大于网络正常运行时的状况。当在协议中加入本文算法时(曲线 detection),节点一旦察觉到恶意节点就会通知其他邻居节点,如果检测到碰撞率 R_c 较高,就会进入睡眠状态,一段时间后自动唤醒,重新检测,这样就节省了较多的能量,因而曲线 detection 下降速度较慢;如果检测到某个节点发出了耗尽攻击,就会拒绝与此节点进行通信,同时通知上层协议重新组网。

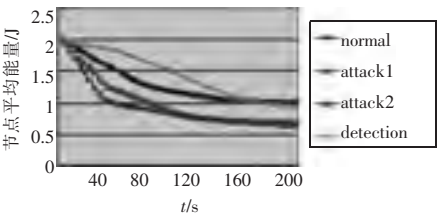

图 4　节点平均剩余能量变化曲线

在表 1 中,针对网络运行的三种情况,使距 sink 节点较远的一个节点以恒定的速率以 UDP 方式向 sink 节点发送数据,可以看出,在上层协议的配合下,DS-MAC 较好地保持了网络的性能,数据源节点发包成功率由 50.7% 提高到了 82.6%。

表 1　网络运行性能比较

比较项	网络受到攻击			网络正常运行	DS-MAC		
发送包个数	378	378	378	378	378	378	378
成功接收包个数	222	174	179	367	296	331	310
平均成功率/%	50.7			97	82.6		

4　结束语

D-S 证据理论作为新兴的一种不确定性推理理论,符合人类决策的推理过程,推理过程简单,已经被广泛地应用于故障诊断、多传感器数据融合、决策分析等领域。本文探讨了其在无线传感器网络 MAC 层入侵检测中的应用。由仿真结果可以看出,本文所提出的 DS-MAC 能够较好地抵御针对无线传感器网络 MAC 层的攻击,有效地节省节点的能量,并通过一定的网络层路由算法的配合,能够更好地保证数据的可靠传输。但是本文提出的方法还存在误警报问题,如何减少对入侵节点的误报率是下一步需要研究的问题。

参考文献:

[1] AKYILDIZ I F, SU Wei-lian, SUBR-MANIAM Y S, *et al*. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[2] 孙雨耕,张静,孙永进,等. 无线自组传感器网络[J]. 传感技术学报,2004,17(2):331-335,348.

[3] YE W, HEIDEMANN J, ESTRIN D. An energy-efficient MAC protocol for wireless sensor networks[C]//Proc of INFOCOM. New York, IEEE Press, 2002: 1567-1576.

[4] DAM T van, LANGENDOEN K. An adaptive energy-efficient MAC protocol for wireless sensor networks[C]//Proc of the 1st Int'l Conf on Embedded Networked Sensor Systems (SenSys). New York: ACM Press, 2003: 171-180.

[5] JAMIESON K, BALAKRISHNAN H, TAY Y C. Sift: an MAC protocol for event-driven wireless sensor networks, MIT-LCS-TR-894[R]. Massachusetts: MIT Lab for Computer Science, 2003.

[6] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Trans on Wireless Communications, 2002, 1(4): 660-670.

[7] RAJENDRAN V, OBRACZKA K, GARCIA -LUNA-ACEVES J J. Energy-efficient, collision-free medium access control for wireless sensor networks[C]//Proc of ACM SenSys. New York: ACM Press, 2003: 181-192.

[8] IEEE Computer Society LAN/MAN Standards Committee. IEEE 802.15.4, Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks[S]. 2006.

[9] IEEE Computer Society LAN/MAN Standards Committee. IEEE std 802.11—1999, Wireless LAN medium access control (MAC) and physical layer(PHY) specifications[S]. 1999.

[10] REN Qing-chun, LIANG Qi-lian. Secure media access control(MAC) in wireless sensor networks: intrusion detections and countermeasures[C]//Proc of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. 2004: 3025-3029.

[11] 孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[12] YU Dong, FRINCKE D. Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer theory[C]//Proc of the 43rd Annual Southeast Regional Conference. New York: ACM Press, 2005: 2-147.

[13] 袁亚湘,孙文瑜. 最优化理论与方法[M]. 北京:科学出版社,1999.

(上接第 329 页)

5　结束语

本文提出了一种分布式报警聚合模型,由本地和网络组件构成,本地组件将 IDS 上报的原始报警转换为基于 IDMEF 模型的统一报警信息格式。在经过聚合模块采用基于分类和属性相似度的报警聚合处理后,网络组件对各 IDS 上报的 IDMEF 超报警进行再聚合。该模型不仅设计了超报警的信息格式,并设计了多种消息内容用于满足模型中本地组件和网络组件间通信需求,可以较好地搭建一个分布式入侵检测系统。未来工作包括:a)目前工作集中在基于网络的 IDS,基于主机的部分还没有考虑;b)报警聚合后还需要进一步地将有关报警进行关联,以发现攻击者的真实意图。

参考文献:

[1] ROESCH W. Snort user manual 2.0.0[EB/OL]. [2006-05-23]. http://www.snort.org/docs/snort_htmanuals/htmanual_261/.

[2] PORRAS P. The common intrusion detection framework architecture[EB/OL]. [1999-09-10]. http://gost.isi.edu/cidf/drafts/architecture.txt.

[3] 穆成坡,黄厚宽,田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展,2006,43(1):1-8.

[4] PORRAS P, NEUMANN P G. EMERALD: event monitoring enabling response to anomalous live disturbances[C]//Proc of the 20th National Information System Security Conference. 1997: 353-365.

[5] SPAFFORD E H, ZAMBONI D. Intrusion detection using autonomous agents[J]. Computer Networks, 2000, 34: 547-570.

[6] 马恒太,蒋建春,陈伟峰,等. 基于 agent 的分布式入侵检测系统模型[J]. 软件学报,2000,11(10):1312-1319.

[7] VALDES A, SKINNER K. Probabilistic alert correlation[C]//Proc of the 4th International Symposium on Recent Advance in Intrusion Detection. Berlin: Springer-Verlag, 2001: 54-68.

[8] DEBAR H, WESPI A. Aggregation and correlation of intrusion-detection alerts[C]//Proc of the 4th International Symposium on Recent Advance in Intrusion Detection. Berlin: Springer-Verlag, 2001: 85-103.

[9] AUREL F, CUPPENS F. Using an intrusion detection alert similarity operator to aggregate and fuse alerts[C]//Proc of the 4th Conference on Security and Network Architectures. 2005.

[10] 穆成坡,黄厚宽,田盛丰. 基于模糊综合评判的入侵检测报警信息处理[J]. 计算机研究与发展,2005,42(10):1679-1685.

[11] OLIVER D, ROBERT C. Fusing a heterogeneous alert stream into scenarios[C]//Proc of ACM Workshop on Data Mining for Security Applications. 2001: 1-13.

[12] MIT Lincoln Labs. 1999 DARPA intrusion detection evaluation[EB/OL]. (1999). http://www.ll.mit.edu/IST/ideval/index.html.