一种多种攻击并发下的WSN生存性评估模型

刘志锋 陈 凯 李 雷 周从华
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 无线传感器网络的生存性已成为部署传感器网络的一个重要考量因素。可生存的无线传感器网络要求在多种攻击并发的情况下能够继续提供关键服务,基于此提出一种多种攻击方式下的、基于簇的无线传感器网络生存性评估模型。因传感器网络的簇中存在多个遭受攻击的节点,为了更准确地判定簇的状态,设计了一种阈值机制来触发因多种攻击而产生的状态之间的转移,准确刻画了网络在遭遇攻击后采取的反制措施。利用连续时间马尔可夫链建立生存性评估模型并求解出可用性与生存性指标,分析了影响传感器网络生存性与可用性的若干因素。仿真结果表明,提高网络修复率和攻击响应率能有效提高生存性与可用性,并且提出的模型能正确地区分网络遭受的攻击形式。

关键词 无线传感器网络,生存性,有效性,攻击,连续时间马尔可夫链
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.08.023

Survivability Evaluation Model for Wireless Sensor Network under Multiple Attacks

LIU Zhi-feng CHEN Kai LI Lei ZHOU Cong-hua
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract Survivability of wireless sensor networks has emerged as a fundamental concern for sensor network deployment. One survivable wireless network demands continuous supplies of critical services under concurrent attacks. Due to such requirement, a survivability evaluation model of WSN under mixed means of attacks, where the network topology is described as a cluster-based one was presented. Because of several nodes being attacked in one single cluster, a threshold mechanism to trigger the transition between the states of WSN under mixed ways of attacks was designed to make countermeasures more accurately. Adopting the continuous time Markov chain, one survivability evaluation model of WSN is constructed, thus attributes as availability and survivability can be obtained. Parameters which influence the availability and survivability have been analyzed. Simulation results show that enhancing the repair rate and response rate of attack can improve the availability and survivability effectively and the introduced model can reflect means of attacks correctly.

Keywords Wireless sensor networks, Survivability, Availability, Attack, Continuoustime Markov chain

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)[1]是由大量微小的、自治的终端构成的,这些终端设备被称为传感节点。传感节点由电池供电,能提供完备的感知、数据传输、短距通信功能。然而,无线传感器网络也面临如节点能量有限、易受攻击等安全性问题,其生存能力受到严重影响。对无线传感器网络而言,生存性指在遭到攻击、故障的情况下仍可提供关键服务的能力,如何有效地对WSN的生存性进行量化评估已成为研究的热点。无线传感器网的生存性评估模型就是为方便分析WSN的生存能力而建立的一种数学模型,是分析和评价WSN的生存性的主要途径,亦为增强WSN的生存性提供重要依据[2]。在典型的应用场景中,随机部署传感节点以获得相关数据,传感器网络会遭遇节点失效或遭受敌方攻击,这些攻击通常是多样的、多种攻击方式的混合,因此设计一种能够准确判定传感器状态并区分多种攻击方式的生存性评估模型就显得格外重要。在敌意环境中,传感节点会面临攻击或被妥协,本文将拒绝服务攻击(DoS attack)[3]和女巫攻击(Sybil attack)[4]这两种无线传感器网络常见的攻击方式作为研究对象。针对实际应用中一个簇中会包含若干遭到不同攻击的普通节点的情况,设计了一种阈值机制来探测整个网络的状态,以确定每一个簇中遭到攻击的节点的数量,从而更准确地判定一个簇的状态。可生存的无线传感器网络不仅需要准确地探测网络中的非正常行为,而且要保证在攻击和故障下的服务可用性。为此,本文针对无线传感器网络易遭受多种不同方式攻击的特点,提出了一种基于连续时间马尔可夫链的分簇WSN生存性评估模型。在该模型中,传统的仅有单个受攻击状态的模型被改进为具体的DoS攻击

到稿日期:2016-10-26 返修日期:2017-02-15 本文受国家自然科学基金(61300228),江苏省六大人才高峰项目(2014-wlw-012),无锡市科技型中小企业创新基金(WX0301-B010508-160104-PB)资助。
刘志锋(1981—),男,博士,副教授,主要研究方向为访问控制、模式识别、可信计算与物联网;陈 凯(1993—),男,硕士生,主要研究方向为可信计算与物联网。

状态和 Sybil 攻击状态，模型能够有效地区分传感器网络中单个簇所处的状态，帮助研究人员有效地判定网络遭受的具体攻击方式。仿真表明，该模型能够有效、定量地评估影响 WSN 生存性的因素。本文第 2 节给出了背景及相关工作；第 3 节介绍了建模的准备工作；第 4 节具体描述了提出的生存性模型及其评估工作；最后对全文做出总结并明确进一步的研究方向。

2 相关工作

目前无线传感器网络安全相关的研究热点主要集中在入侵检测、入侵容忍、网络抗毁性等方面。文献[5]针对入侵检测系统本身会受到攻击者影响这一问题，引入博弈论理论检测系统与入侵者之间的重复博弈，实现了对入侵者的有效识别。文献[6]针对入侵容忍模型约束条件过多、评估不准确的问题，利用层次化算法组建安全态势模型，获取系统受到攻击影响的效果以修正无线网络安全态势模型，对容忍入侵能力进行优化评估。文献[7]考虑网络的动态性过程，在分簇结构中引入中继负载与感知负载等概念建立级联失效模型，基于网络演化分别提出分簇 WSN 的无标度网络和随机拓扑演化模型，并验证了级联失效模型中各关键参数对网络抗毁性的影响。上述研究分别针对无线传感器网络应对攻击的某一种局部的、具体的能力，缺少宏观的、整体上的安全性评估，因此还需要研究 WSN 生存性评估模型，从网络整体层面上对无线传感器网络在遭受攻击下继续提供服务的能力进行评估，并分析影响因素，以为发起安全操作提供决策依据。

最近国内外研究者已提出了一些与 WSN 相关的可生存性评估方法。文献[8]提出一种基于半马尔可夫过程的分簇 WSN 生存性评估模型，该模型在考虑应急通信中簇头的生存状态的基础上建立了基于 SMP 的簇头生存状态转移图，并对采用 SRPC 协议和 RLEACH 协议的 WSN 的生存能力进行了量化评估和比较分析。文献[9]针对无线 Ad Hoc 网络遭受黑洞攻击(Black Hole attack)的情况，运用 SMP 模型分析了网络的生存能力，并在此基础上分析了二项分布和负二项分布两种随机模型中节点连通度的问题。文献[10]利用内嵌 DTMC 解决无线传感器网络中的拓扑可用性、稳定性和服务率指标，提出了贝叶斯网络指标推理方法，该方法提高了系统容侵能力评估的准确性。文献[11]针对受恶意程序传染的分簇 WSN 使用能预测恶意程序传染行为的博弈模型，将恶意程序传染的故意性与马尔可夫链的随机性关联，实现利用马尔可夫链中的状态转换描述恶意程序传染行为的目的。与 WSN 生存性评估密切相关的还有 WSN 可靠性评估。文献[12]针对没有全面评估 WSN 可靠性的统一标准，从无线传感器网络的拓扑结构、协议栈结构和可靠性机制的角度对可靠性进行了剖析，提取了影响可靠性的性能指标，提出了一种基于模糊神经网络的可靠性评估模型。文献[13]针对难以准确、全面、系统地评估工业无线传感器网络可靠性的问题，提出了随时间演进的状态转移蒙特卡罗评估方法和网络功能值表示方法，并将其用于评估无线传感器网络的可靠性。

此外，针对无线传感器网络常见的几种攻击类型，国内外有不少研究者提出了相应的生存性评估模型。文献[14]提出了针对水母攻击、黑洞攻击的生存性评估模型，此模型较好地反映了单个节点的行为变化过程，但其假设节点分布满足泊松分布模型，与实际应用时的拓扑不太相符。文献[15]考虑了簇在遭受 DoS 攻击时仍能继续提供服务的能力，并同时考虑了节点隔离度的问题且假定簇头节点的行为等同于簇内传感节点的行为，减少了生存性指标的计算量，简化了模型。文献[16]考虑了单个节点遭受攻击时的生存状态，针对攻击修复时的节点自愈问题，设计了一种态势感知策略来驱动每一轮的攻击修复机制，该方案能帮助传感器节点在不同的攻击情况和入侵修复需求下选择合适的攻击修复行为，提高了节点的生存能力。在实际应用中，网络结构变化且攻击形式多样，仅通过评估簇头节点或普通传感节点的生存性来衡量 WSN 的生存能力缺乏合理性，同时管理人员需要全面了解网络遭受攻击的程度与具体的攻击类型，因此这些模型考虑的生存性因素不够全面，生存状态不够完善，不适用于多种攻击模式下节点的无线传感器网络生存性建模。

鉴于上述工作的不足，本文针对分簇 WSN 在遭到不同方式攻击下的行为变化特征，依据网络的生存性需求建立了一个多种攻击并发下的分簇 WSN 生存性评估模型，它通过一种阈值机制来衡量整个簇的生存能力，从而对 WSN 的生存能力进行量化评估，并通过模拟分析了影响 WSN 生存性的主要因素。

3 生存性评估模型

3.1 网络拓扑设定

基于簇的 WSN 拓扑具有节省能量和资源开销的优点，因此本文采用分簇 WSN 拓扑模型。图 1 是一个典型的基于簇的 WSN 网络拓扑的例子。按照文献[17]中的方式选择一个节点作为簇头节点并且形成若干个簇。传感节点交换必要的密钥来建立一个应用在 WSN 中的安全机制[18]。传感节点发送数据给簇头节点，簇头节点则将数据发送给基站(BS)，BS 则可以接入传统网络如因特网及卫星通讯系统中。

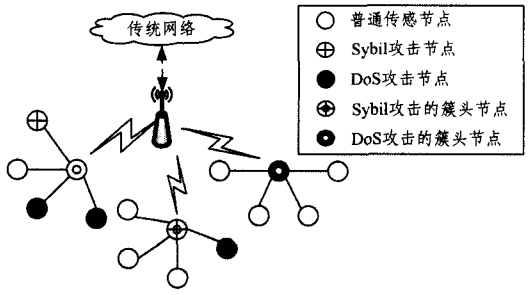

图 1 基于簇的传感器网络图

整个网络的详细设定如下：

1)基站对于攻击是鲁棒的，一些关于基站的安全机制[19-21]被用于保证基站的安全性；

2)传感节点易遭受攻击；

3)传感节点不能避免被敌方篡改；

4)传感节点在部署后处于固定位置；

5)使用一种连续的或者是间断的簇状态监控机制来反映每一个簇的状态；

6)使用一种妥协节点检测策略[22]来确定簇中妥协节点的数量。

3.2 威胁设定

如前文所述，传感节点易受多种方式的攻击。本文选择 Hello Flood 及 Sybil 两种常用攻击混合的攻击模式作为威胁模型。Hello Flood[23] 是拒绝服务攻击(Denial-of-service attack)的一种。针对 DoS 攻击的反制措施是最小化连接的数量或者使用 CPP(Client Puzzle Protocol)协议。文献[24]考虑了一种无线传感器网络中的安全路由机制，该机制建议采用一种经过认证的广播和洪泛来防止 Hello Flood 攻击。而在 Sybil 攻击中，一个单一的节点可以伪造多种身份，从而降低故障容忍机制如分布式存储、多径路由和拓扑维持[25] 的效率。针对 Sybil 攻击，文献[26]提出了一种基于 AOA 信任评估模型的 Sybil 攻击检测方案，以信号到达角的相位差为基础对传感器节点信任度作出评估，系统将低于某一信任阈值的节点身份列入 Sybil 黑名单并在未来的通信过程中予以排除。本文采用一种基于软件更新和重配置相结合的反制行为集，使得整个传感器网络在遭到 Hello Flood 和 Sybil 攻击时能够最大化节点的生存时间。

3.3 阈值功能

在实际应用中由于攻击方式多样，WSN 中混合了正常、失效、遭受不同攻击而妥协等不同状态的节点。将簇的状态归纳为一个简单的受攻击状态不能准确反映网络中主要的攻击类型，因此本文根据簇中各个状态的节点数量及其与节点总量的比值，在簇的层面上设计一种阈值机制来对簇进行状态切换以正确反映网络的攻击类型。阈值机制的具体设定如下：

1)一个 WSN 的拓扑是基于簇的 m 层结构，其中 $m=1,2,\cdots,n$ 且 n 为整数。

2)网络中总共有 N 个传感节点，其中 $N=1,2,\cdots,n$。如图 1 所示的无线传感器网络即为一个 2 层结构。

3)网络的最顶层总共有 K 个簇，其中 $K\leqslant N, K=1,2,\cdots,n$。

4)一个簇中有 n_d 个 DoS 节点和 n_s 个 Sybil 节点。

5)定义两个阈值参数 $t_1=N/\alpha K, t_2=N/\beta K$ 来判断每一个簇的状态。

6)定义阈值参数 α,β 来描述一个簇中遭到 DoS 和 Sybil 攻击而妥协的节点数的程度。

7)定义反制行为集 $A=\{a_1,a_2,\cdots,a_l\}$，其中 a_l 表示针对一种特定攻击所采取的行动。

8)所有 K 个簇中的第 i 个簇的状态可以表示为状态 S_i。

3.4 系统模型

本节提出了一种生存性模型，在介绍模型之前，先要解释为何采用随机模型来描述多个状态。考虑以下几个方面：

1)首先，考虑对两种状态即正常状态和妥协状态进行周期性的监控。

2)然后，考虑一种状态转移模型来模拟整个网络从一种状态向另一种状态的转移。需要明确规定网络中簇的状态以及相应的各状态之间的转移模型。

3)最后，考虑使用概率模型来对网络的状态进行检测。假设簇的状态按照一定的概率转移，而外部活动如攻击和反制会触发簇从一个状态向下一个状态转移。若周期性或分批次地对簇的状态进行检测，则能根据簇的状态信息采取相应的反制措施。因此，提出了一种基于随机模型的生存性模型，通过该模型可以很容易地得出簇各状态的稳态概率。图 2 为传感网中单个簇的生存模型的状态转移图。

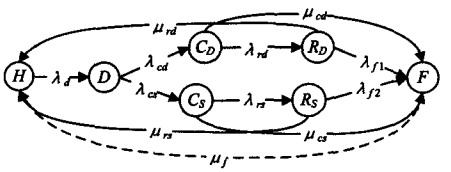

图 2　WSN 中单个簇的 CTMC 生存状态转换模型

将前述的阈值机制引入状态的判定中，状态转移图中的 s_i 表示簇目前所处的状态，而簇的状态由多种外界或自身的因素决定。为了简化所提模型，定义簇的状态由 t_1, t_2 和 A 决定，t_1 表示网络中 DoS 节点数占整个节点数的百分比的阈值参数，t_2 表示网络中 Sybil 节点数占整个节点数的百分比的阈值参数，而 A 则为一个有多种反制行为的行为集。设簇的生存状态集为 $S=\{H,D,C_d,C_s,R_d,R_s,F\}$，它的具体含义如下。

1)健康状态(H)。若 DoS 节点数和 Sybil 节点数小于设定的阈值数则认为该簇处于健康状态，此时网络能持续提供服务，在此状态下，不采取反制行为。形式化的表达为：

$$0<n_d\leqslant\frac{N}{\alpha K}\text{ and }0<n_s\leqslant\frac{N}{\beta K}, A=\{\varnothing\}$$

2)探测状态(D)。健康状态的簇会按照一定的速率对整个簇进行检测，以确定簇中的节点是否为 DoS 节点或者 Sybil 节点，对整个簇进行探测属于行为集 A。形式化的表达为：

$$0<n_d\leqslant\frac{N}{\alpha K}\text{ and }0<n_s\leqslant\frac{N}{\beta K}, A=\{a_i\}$$

3)DoS 状态(C_d)。根据状态探测机制得到的结果，DoS 节点的总数大于阈值，而 Sybil 节点数未超过，在此状态下无反制措施。形式化的表达为：

$$n_d\geqslant\frac{N}{\alpha K}\text{ and }0<n_s\leqslant\frac{N}{\beta K}, A=\{\varnothing\}$$

4)Sybil 状态(C_s)。与 DoS 状态相反，Sybil 节点的总数大于阈值，而 DoS 节点数未超过，在此状态下无反制措施。形式化的表达为：

$$0<n_d\leqslant\frac{N}{\alpha K}\text{ and }n_s\geqslant\frac{N}{\beta K}, A=\{\varnothing\}$$

5)DoS 响应状态(R_d)。处于该状态的簇会对 DoS 攻击进行反制，例如重配置或软件自愈，成功后转化为健康状态，否则进入失效状态，这些反制行为属于行为集 A。形式化的表达为：

$$n_d\geqslant\frac{N}{\alpha K}\text{ and }0<n_s\leqslant\frac{N}{\beta K}, A=\{a_i\}$$

6)Sybil 响应状态(R_s)。处于该状态的簇会对 Sybil 攻击进行反制，例如 Sybil 节点定位或者密钥重分配，成功后转化为健康状态，否则进入失效状态。形式化的表达为：

$$0<n_d\leqslant\frac{N}{\alpha K}\text{ and }n_s\geqslant\frac{N}{\beta K}, A=\{a_i\}$$

7)失效状态(F)。响应失效，网络不能持续提供基本的服务，只能由系统管理员经过手动修复和重配置以便恢复到健康状态。形式化的表达为：

$$n_d+n_s=\frac{N}{K}, A=\{\varnothing\}$$

CTMC 生存状态转移模型中各状态的稳态概率及其描述如表 1 所列。

表 1 各状态的稳态概率

稳态概率	描述
π_h	簇处于健康状态的概率
π_d	簇处于探测状态的概率
π_{cd}	簇处于 DoS 攻击状态的概率
π_{cs}	簇处于 Sybil 攻击状态的概率
π_{rd}	簇对 DoS 攻击做出相应反制措施的概率
π_{rs}	簇对 Sybil 攻击做出相应反制措施的概率
π_f	簇处于失效状态的概率

CTMC 生存状态转移模型中各项参数的定义如表 2 所列。

表 2 CTMC 生存状态转换模型中各项参数的定义

参数	描述
λ_d	进入探测状态的速率
λ_{cd}	进入 DoS 攻击状态的速率
λ_{cs}	进入 Sybil 攻击状态的速率
λ_{rd}	响应 DoS 攻击的速率
λ_{rs}	响应 Sybil 攻击的速率
λ_{f1}	响应 DoS 攻击失效的速率
λ_{f2}	响应 Sybil 攻击失效的速率
μ_{cd}	从 DoS 攻击进入失效状态的速率
μ_{cs}	从 Sybil 攻击进入失效状态的速率
μ_{rd}	从 DoS 响应状态后恢复的速率
μ_{rs}	从 Sybil 响应状态后恢复的速率
μ_f	从失效状态恢复的速率

3.5 WSN 可生存性评估

根据 CTMC 生存性模型对 WSN 网络的生存性进行分析，由状态转移模型和各项参数可以得到图 2 中生存状态模型的状态转移矩阵 $R(s,s')$，其中状态空间 $S=\{H,D,C_d,C_s,R_d,R_s,F\}$。

$$R=\begin{bmatrix} & \lambda_d & & & & & \\ & & \lambda_{cd} & \lambda_{cs} & & & \\ & & & & \lambda_{rd} & & \mu_{cd} \\ & & & & & \lambda_{rs} & \mu_{cs} \\ \mu_{rd} & & & & & & \lambda_{f1} \\ \mu_{rs} & & & & & & \lambda_{f2} \\ \mu_f & & & & & & \end{bmatrix}$$

设簇头稳定状态的概率矢量为：

$\Pi=[\pi_h,\pi_d,\pi_{cd},\pi_{cs},\pi_{rd},\pi_{rs},\pi_f]$

根据连续马尔可夫性质，可以得到如下 3 个方程：

$$Q(s,s')=\begin{cases}R(s,s'), & \text{if } s\neq s'\\ -\sum R(s,s''), & s\neq s''\end{cases}$$

$$\Pi\cdot Q=0$$

$$\sum_{i\in S}\pi_i=1$$

根据以上方程组可得：

$$\pi_d=\frac{\lambda_d}{\lambda_{cd}+\lambda_{cs}}\pi_h$$

$$\pi_{cd}=\frac{\lambda_d\cdot\lambda_{cd}}{(\lambda_{cd}+\lambda_{cs})(\lambda_{rd}+\mu_{cd})}\pi_h$$

$$\pi_{cs}=\frac{\lambda_d\cdot\lambda_{cs}}{(\lambda_{cd}+\lambda_{cs})(\lambda_{rs}+\mu_{cs})}\pi_h$$

$$\pi_{rd}=\frac{\lambda_d\cdot\lambda_{cd}\cdot\lambda_{rd}}{(\lambda_{cd}+\lambda_{cs})(\lambda_{f1}+\mu_{rd})(\lambda_{rd}+\mu_{cd})}\pi_h$$

$$\pi_{rs}=\frac{\lambda_d\cdot\lambda_{cs}\cdot\lambda_{rs}}{(\lambda_{cd}+\lambda_{cs})(\lambda_{f2}+\mu_{rs})(\lambda_{rs}+\mu_{cs})}\pi_h$$

$$\pi_f=((\lambda_d(\lambda_{cd}+\lambda_{cs})(\lambda_{f1}\cdot\lambda_{f2}\cdot\lambda_{rd}\cdot\lambda_{rs}+\mu_{cd}\cdot\mu_{cs}\cdot\mu_{rd}\cdot\mu_{rs}))/((\lambda_{cd}+\lambda_{cs})(\lambda_{f2}+\mu_{rs})(\lambda_{rs}+\mu_{cs})))\pi_h$$

$$\pi_h=1-\pi_{cd}-\pi_{cs}-\pi_{rd}-\pi_{rs}-\pi_f$$

整个 WSN 的可用性和生存性可以由根据马尔可夫链解得的各状态的稳态概率值来表示：

$$Availability(A)=1-\pi_f$$

$$Survivability(S)=Availability-(\pi_{rd}+\pi_{rs})$$

4 实验分析

对生存性模型的验证要求在一定的实验条件下确定模型能否提供无线传感器网络的准确信息，如生存性指标对网络生存性的影响。本文采用 Matlab 仿真的方式对提出的模型进行分析验证。

首先，将前文所述的阈值机制实例化。以图 1 为例，该图描述的传感器网络拓扑的具体参数设定如下：$m=2,N=15,K=3,\alpha=3,\beta=2,l=4,A=\{a_1,a_2,a_3,a_4\}=\{$rebooting, key revocation, RS-SI detecting, reconfigure$\}$。本文考虑簇的生存性与可用性这两种度量指标，CTMC 模型中各状态间的转移速率如表 3 所列。

表 3 系统参数表

系统操作参数	值
λ_d	0,1,2,3,4,5 times/h
λ_{cd}	5 times/h
λ_{cs}	5 times/h
λ_{rd}	0,1/15,1/10,1/5,1/3(per min)
λ_{rs}	0,1/15,1/10,1/5,1/3(per min)
λ_{f1}	0,1,2,3,4,5 times/h
λ_{f2}	0,1,2,3,4,5 times/h
μ_{cd}	1 time/h
μ_{cs}	1 time/h
μ_{rd}	0.2,0.4,0.6,0.8,1 (per s)
μ_{rs}	0.2,0.4,0.6,0.8,1 (per s)
μ_f	0,1,2,3,4,5 times/h

考查进入入侵探测状态的速率对生存性和可用性的影响。取 λ_d 分别为 0,1,2,3,4,5 times/h，$(\lambda_{cd},\lambda_{cs},\lambda_{rd},\lambda_{rs},\lambda_{f1},\lambda_{f2},\mu_{cd},\mu_{cs},\mu_{rd},\mu_{rs},\mu_f)=(5,5,1/10,1/10,2,2,1,1,0.4,0.4,2)$。实验结果如图 3、图 4 所示，可用性 A 从 1 迅速下降至约 0.75(2 times/h 处)，之后缓慢降至 0.72，生存性 S 则从 1 逐渐下降到约 0.69，说明簇的生存性与可用性随入侵探测率的提高而降低。因为无线传感器网络能量有限，经常性地执行入侵检测会大量消耗节点的资源，造成生存性和可用性的下降，因此实验结果与实际是相符合的。

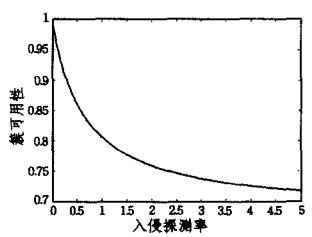

图 3 入侵探测率对可用性的影响

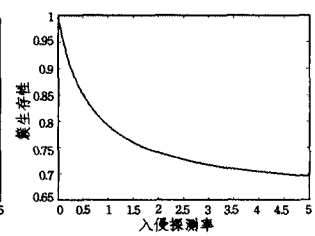

图 4 入侵探测率对生存性的影响

下面分析从失效状态修复为健康状态的速率对生存性和可用性的影响。取 μ_f 的值分别为 0,1,2,3,4,5 times/h，$(\lambda_d,\lambda_{cd},\lambda_{cs},\lambda_{rd},\lambda_{rs},\lambda_{f1},\lambda_{f2},\mu_{cd},\mu_{cs},\mu_{rd},\mu_{rs})=(2,5,5,1/10,$

1/10,2,2,1,1,0.4,0.4)。实验结果如图 5、图 6 所示，当修复率为 2times/h 时，可用性 A 从 0 迅速提高至 0.75，之后缓慢上升至接近 0.9；生存性 S 则从 0 迅速上升至 0.7，之后缓慢提高至0.85。实验表明，修复速率是提高生存性与可用性的决定因素，随着恢复速率的提高，可用性和生存性都得到了明显的提高，在到达一定值后趋于稳定。在实际中，通过人为更换失效节点的方式可以显著提高整个传感器网络的生存性和可用性，但次数过多则容易造成资源的浪费，且对生存性和可用性的继续提高作用不大。

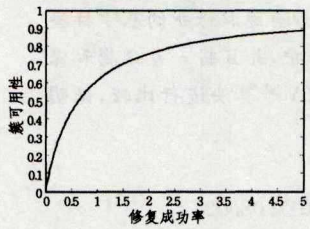

图 5　修复成功率对可用性的影响

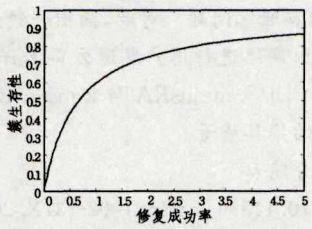

图 6　修复成功率对生存性的影响

以下考查响应失败率和响应成功率对网络可用性和生存性的影响。一些安全措施如软件重配置、密钥撤销、信任表等方式可以响应 DoS 攻击和 Sybil 攻击，分别将这些因遭受攻击而妥协的节点从 WSN 网络中剔除，或在这些节点恢复至健康状态后将其重新纳入路由，从而保证整个网络的安全性。在实际中由于持续攻击的存在，执行上述操作也可能失败，从而进入失效状态。实验中，取两种攻击方式的响应失败率 λ_{f1} 和 λ_{f2} 为 0,1,2,3,4,5 times/h，响应成功率 μ_{rd} 和 μ_{rs} 为0.2,0.4,0.6,0.8,1per s。$(\lambda_d,\lambda_{cd},\lambda_{cs},\lambda_{rd},\lambda_{rs},\mu_{cd},\mu_{cs})=(2,5,5,1/10,1/10,1,1,2)$。响应失败率对可用性和生存性的影响结果如图 7、图 8 所示，当 DoS 响应失败率和 Sybil 响应失败率最小时，可用性最高为 0.78，而生存性最弱达到约 0.68；反之，当两种攻击的响应失败率最高时，可用性最低至 0.75，而生存性达到最强 0.75。以上说明，攻击响应失败率的提高能降低可用性而提高生存性。响应成功率对可用性与生存性的影响结果如图 9、图 10 所示，当 DoS 响应成功率和 Sybil 响应成功率最小时，可用性和生存性均最弱，分别为 0.756 和 0.735；而当攻击的响应成功率最高时，可用性和生存性最强，接近 0.761 和 0.745。由此可知，成功响应攻击能有效提高网络的可用性和生存性。同时值得注意的是，当 DoS 响应不变时，可用性及生存性随 Sybil 响应明显改变，反之亦然，说明本文提出的模型可以很方便地判断出网络中主要遭受的是哪种形式的攻击，以为有针对性地对攻击进行反制提供参考。

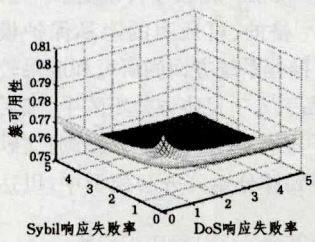

图 7　Sybil 和 DoS 响应失败率对可用性的影响

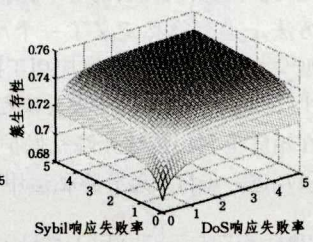

图 8　Sybil 和 DoS 响应失败率对生存性的影响

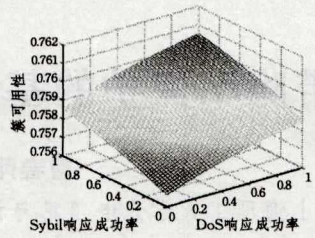

图 9　Sybil 和 DoS 响应成功率对可用性的影响

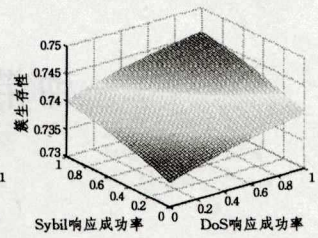

图 10　Sybil 和 DoS 响应成功率对生存性的影响

结束语　WSN 生存性评估模型是 WSN 生存性分析的重要内容，本文提出的生存性评估模型利用连续时间马尔可夫链描述基于簇的无线传感器网络中的单个簇在遭受多种方式攻击下的状态演进过程。本文设计了一种阈值机制来帮助判定簇的状态，更加符合实际应用的情况。分析验证结果表明，成功修复网络或对攻击进行响应是提高生存性与可用性的重要途径，且提出的阈值机制能有效区分攻击类型。

参 考 文 献

[1] MAHMOOD M A, SEAH W K G, WELCH I. Reliability in wireless sensor networks: A survey and challenges ahead[J]. Computer Networks, 2015, 79: 166-187.

[2] DENG X, ZHANG L J. Overview of WSNs survivability enhancing technology[J]. Transducer and Microsystem Technologies, 2014, 33(1): 1-4. (in Chinese)
邓鑫，张乐君. 无线传感器网络可生存性增强技术研究概述[J]. 传感器与微系统，2014，33(1)：1-4.

[3] ZHANG H, CHENG P, SHI L, et al. Optimal DoS Attack Scheduling in Wireless Networked Control System[J]. IEEE Transactions on Control Systems Technology, 2015, 24(3): 843-852.

[4] BHISE A M, KAMBLE S D. Review on Detection and Mitigation of Sybil Attack in the Network[J]. Procedia Computer Science, 2016, 78: 395-401.

[5] GUI M Q, LIU Y B, ZHOU L Y. Intrusion detection based on game theory in wireless sensor network [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2016, 28(3): 414-420. (in Chinese)
桂明倩，刘宴兵，周睒永. WSN 中基于博弈理论的入侵检测研究[J]. 重庆邮电大学学报(自然科学版)，2016，28(3)：414-420.

[6] JI G Y. Tolerate Invasion Ability Evaluation Modeling Wireless Network Simulation Analysis[J]. Computer Simulation, 2016, 33(7): 273-276. (in Chinese)
姬广永. 无线网络中容忍入侵能力评估模型仿真分析[J]. 计算机仿真，2016，33(7)：273-276.

[7] FU X W, LI W F, DUAN Y. Invulner-Ability of Clustering Wireless Sensor Networks Towards Cascading Failures[J]. Journal of Computer Research and Development, 2016, 53(12): 2882-2892. (in Chinese)
符修文，李文锋，段莹. 分簇无线传感器网络级联失效抗毁性研究[J]. 计算机研究与发展，2016，53(12)：2882-2892.

[8] ZHU S C, WANG H T, WU L C, et al. Survivability Estimation Model for Clustered Wireless Sensor Network Based on SMP [J]. Chinese Journal of Sensors & Actuators, 2014, 27(3): 383-387. (in Chinese)

(下转第 161 页)

2014,37(1):246-258.

[11] HUANG L S,TIAN M M,HUANG H. Preserving Privacy in Big Data:A Survey from the Cryptographic Perspective[J]. Journal of Software,2015,26(4):945-959. (in Chinese)
黄刘生，田苗苗，黄河. 大数据隐私保护密码技术研究综述[J]. 软件学报，2015,26(4):945-959.

[12] ZHANG P,DONG Y H,TANG S H,et al. An Effective Method for Privacy Preserving Association Rule Mining[J]. Journal of Software,2006,17(8):1764-1774. (in Chinese)
张鹏，童云海，唐世渭，等. 一种有效的隐私保护关联规则挖掘方法[J]. 软件学报，2006,17(8):1764-1774.

[13] FU S,ZHOU H J. The Research and Improvement of Apriori-Algoruthm for Mining Association Rules[J]. Microelectronics & Computer,2013(9):110-114. (in Chinese)
付沙，周航军. 关联规则挖掘 Apriori 算法的研究与改进[J]. 微电子学与计算机，2013(9):110-114.

[14] HSSEIN M,EL-SISI A,ISMAIL N. Fast Cryptographic Privacy Preserving Association Rules Mining on Distributed Homogenous Data Base [C] // Proceedings of the 12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems,Part II. Springer-Verlag,2008:607-616.

[15] ZHANG Y,WANG H G,SHAO Z Z,et al. Frequentitemsets mining based on Apriori-bit[J]. Application Research of Computers,2013,30(9):2610-2612. (in Chinese)
张岳，王洪国，邵增珍，等. 基于先验位运算的频繁项集挖掘[J]. 计算机应用研究，2013,30(9):2610-2612.

[16] WAHAB A,OMAR,HACHAMI,et al. DARM:a privacy-preserving approach for distributed association rules mining on horizontally-partitioned data[C] // International Database Engineering & Applications Symposium. ACM,2014.

[17] YI X,RAO F Y,BERTINO E,et al. Privacy-Preserving Association Rule Mining in Cloud Computing[C] // Proceedings of the 10th ACM Symposium on Information,Computer and Communications Security. ACM,2015:439-450.

(上接第 133 页)

朱世才，王海涛，吴连才，等. 基于 SMP 的分簇 WSN 生存性评估模型[J]. 传感技术学报，2014,27(3):383-387.

[9] YI Z,DOHI T,OKAMURA H. Survivability modeling and analysis for a power-aware wireless ad hoc network[C] // International Congress on Ultra Modern Telecommunications and Control Systems and Workshops. IEEE,2012:813-819.

[10] XIONG S M,WANG L M,ZHAN Y Z. Quantitative evaluation of topology intrusion tolerance in wireless sensor networks based on semi-Markov process[J]. Journal on Communications,2010,31(7):24-32. (in Chinese)
熊书明，王良民，詹永照. 基于 SMP 的无线传感器网络拓扑容侵定量评估[J]. 通信学报，2010,31(7):24-32.

[11] SHEN S G,HUANG L J,FAN E. Survivability evaluation for WSNs under malware infection[J]. Chinese Journal of Sensors and Actuators,2016,29(7):1083-1089. (in Chinese)
沈士根，黄龙军，范恩. 受恶意程序传染的 WSNs 可生存性评估[J]. 传感技术学报，2016,29(7):1083-1089.

[12] LI J P,WANG X K. WSN reliability evaluation based on fuzzy neural network[J]. Journal of Computer Applications,2016,36(A02):69-72. (in Chinese)
李建平，王晓凯. 基于模糊神经网络的无线传感器网络可靠性评估[J]. 计算机应用，2016,36(A02):69-72.

[13] YUE Y,LI J,FAN H,et al. An efficient reliability evaluation method for industrial wireless sensor networks[J]. Journal of Southeast University,2016,32(2):195-200.

[14] YI Z,DOHI T. Survivability Analysis for a Wireless Ad Hoc Network Based on Semi-Markov Model[J]. IEICE Transactions on Information&Systems,2012,E95. D (12):2844-2851.

[15] CHANG C J,ZHU C H,WANG H G,et al. Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attacks[C] // Wireless Communications,Networking and Mobile Computing. 2009.

[16] STAVROU E,PITSLLIDES A. Situation aware intrusion recovery policy in WSNs[C] // International Conference on Cyber Situational Awareness,Data Analytics and Assessment. 2016:1-8.

[17] VIRMANI D,KAUR S,JAIN S. Secure and Fault Tolerant Dynamic Cluster Head Selection Method for Wireless Sensor Networks [J]. Procedia Computer Science,2015,46(2):989-996.

[18] NEWELL A,YAO H,RYKER A,et al. Node-Capture Resilient Key Establishment in Sensor Networks:Design Space and New Protocols [J]. Acm Computing Surveys,2015,47(2):1-34.

[19] HAMMOUDEH M,NEWMAN R. Adaptive routing in wireless sensor networks:QoS optimisation for enhanced application performance [J]. Information Fusion,2015,22(71):3-15.

[20] WARD J R,YOUNIS M. Base Station anonymity distributed Self-assessment in Wireless Sensor Networks[C] // IEEE International Conference on Intelligence and Security Informatics. IEEE,2015.

[21] KIM T Y,LEED R. Communication method,base station,communication system,and mobile terminal [J]. Journal of Organizational Behavior,2015,30(7):1001-1018.

[22] ZHANG Q,YU T,NING P. A Framework for Identifying Compromised Nodes in Wireless Sensor Networks [J]. ACM Transactions on Information & System Security,2008,11(3):1-10.

[23] SINGH V P,JAIN S,SINGHAI J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks [J]. International Journal of Computer Science Issues,2010,7(3):23-24.

[24] KARLOF C,WAGNER D. Secure routing in wireless sensor networks:attacks and countermeasures [C] // IEEE International Workshop on Sensor Network Protocols and Applications,2003. IEEE,2003:293-315.

[25] GOYAL S,BHATIA T,VERMA A K. Wormhole and Sybil attack in WSN:A review[C] // International Conference on Computing for Sustainable Global Development. IEEE,2015.

[26] ZHANG Y,FAN K F,ZHANG S B. AOA based trust evaluation scheme for Sybil attack detection in WSN[J]. Application Research of Computers,2010,27(5):1847-1844. (in Chinese)
张艳，范科峰，张素兵. 一种基于 AOA 信任评估的无线传感器网络 Sybil 攻击检测新方法[J]. 计算机应用研究，2010,27(5):1847-1849.