

一种兼具主、被动防御的 WSNs 安全通信策略

孙家文 杨 波 贾新春

(山西大学数学科学学院, 太原 030006)

摘要 无线传感器网络(WSNs)由于其通信信道的开放性、节点资源受限性和部署随机性等特点, 其安全性面临很多挑战。针对某些部署在危险环境中的 WSNs 应用对安全性要求较高的问题, 提出了一种兼具主、被动防御的 WSNs 安全通信策略。通过对消息的加、解密, 签名认证, 完整性鉴别等主动防御措施和变换基站的被动防御措施相结合的策略, 为网络创造一个相对安全的工作环境。性能分析表明:该策略能降低网络受到攻击的可能性, 减小攻击影响, 提高网络的抗毁能力, 有效地延长网络的生命周期。

关键词 无线传感器网络 安全 主动防御 被动防御

中图法分类号 TP393. 08; **文献标志码** A

无线传感器网络^[1,2] WSNs (wireless sensor networks)是由大量具有感知、计算和通信能力的微型传感器节点通过无线通信方式形成的一个多跳、自组织的网络系统。它能够自主实现数据采集、融合和传输,使得逻辑上的信息世界和真实的物理世界紧密结合,真正实现“无处不在的计算”模式^[3]。在军事侦查、环境监测、交通管理、智能家居、工农业控制等方面都具有广阔的应用前景^[4]。由于无线传感器网络具有规模大、无人值守、资源严格受限等特点,其在数据采集、数据传输、服务提供等环节面临巨大的信息安全挑战。特别是一些部署在危险环境中的 WSNs 应用,由于易受监听和各种恶意攻击,通讯安全问题变得极为重要,为其创造一个相对安全的工作环境是关系到其能否真正走向实用的关键方面。

网络部署区域的开放特性以及无线电网络的广播特性^[5]是无线传感器网络安全隐患的根源。在某些安全需求较高的场合部署无线传感器网络时加入主动防御^[6]措施,如对发送的消息进行加密认证处理,对接收到的消息进行解密、签名认证、完整性鉴别等一系列检查,可以在一定程度上提高无线传感器网络的安全性。SPINS^[7] (security protocols for sensor network) 安全框架协议适用于各种无线传感器网络,是目前所提出的安全机制中比较经典、实用的网络安全协议。但此协议中基站需存储与网络中所有节点对应的主密钥,对存储空间是个极大的考

验^[8—10]。此外,它也没有考虑拒绝服务(DoS)攻击的可能性。又由于基站在整个网络通讯中起着承上启下的作用,在网络中其地位十分重要。一旦基站受到恶意节点攻击,没有备选措施网络将无法正常工作甚至面临瘫痪。

考虑上述不足,本文提出的兼具主、被动防御的无线传感器网络安全通讯策略,首先采用改进的 SPINS 安全框架协议为网络搭建主动防御,在网络构建之时采用分组的方法使基站只需存储组内节点对应的密钥,以减轻基站的存储负担;其次,初始阶段即建立起所有传感器节点和基站间有密钥认证的安全通讯,实行逐跳认证从根本上解决 DoS 攻击;最后,本文假设网络中某基站遭到恶意节点的攻击,采用基站变换的被动防御机制,减小攻击影响,保证网络的正常运行。

1 SPINS 安全协议简介

SPINS 是 Perrig 等人^[7] 提出的一种适用于 WSNs 的安全架构协议。它包括安全网络加密协议 SNEP(secure network encryption protocol) 和基于时间的高效的容忍丢包的流认证协议 uTESLA (micro timed efficient streaming loss-tolerant authentication protocol) 两个部分,在 SNEP 中使用计数器(counter, CTR) 模式的加密机制和消息验证码(message authentication code, MAC) 协议实现通信的机密性、完整性、新鲜性和点对点认证;在 uTESLA 中利用单向散列函数的单向特性,将密钥延迟发布,实现了无线传感器网络中点到多点的广播认证。

2 网络的构建

随机部署在监测区域的大量传感器节点通过自

组织的方式链接成网络,这种方式实现起来简单,但可能导致外界非法节点也加入网络(伪造),并且解决不了 DoS 攻击。受文献[11]的启发并考虑到目前分布式传感器网络多为分簇形式,本文建立一个树状网络模型。网络由一个远程控制设备 Homehost 和若干个传感器节点构成。传感器节点包括普通传感器节点和带有特殊功能的节点——基站节点 Base-station node(它电池电量高,内存大,计算能力强,通讯带宽高,覆盖范围广)。由远程控制设备 Homehost 管理网络,通过不同级别的基站将网络划分成不同的级别组,每一个分组由一个基站节点和若干数量的普通节点组成。建立的树状网络模型如图 1 所示。

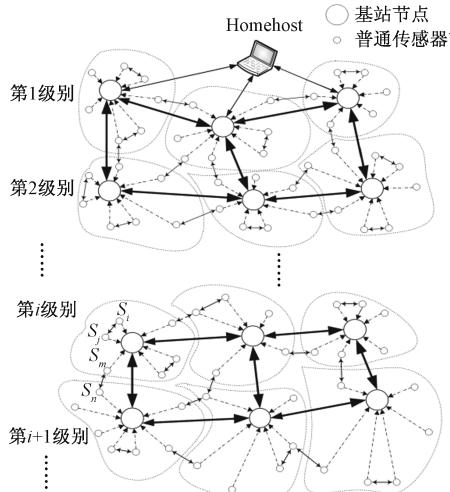


图 1 树状网络模型

Fig. 1 The tree-structured network model

2.1 网络主动防御机制的建立

网络配置前做如下准备工作:

①首先建立一个大容量的密钥池,给每一个传感器节点随机地预分配一个不同的密钥。

②由于可预先获得分组信息(即:将节点布置在哪块区域,需要多少节点),在组网之前以分组信息为依据确定每个组内的节点集合,组内的基站节点预先存储集合内所有节点的 ID 号和密钥,这样组内的每个节点都与基站存在一个共享密钥。

③对于基站,根据级别的不同,给不同级别的各个基站节点预分配一个不同的站间会话密钥;同级别的各个基站预分配一个相同的站间会话密钥。并在基站节点和远程控制设备 Homehost 的内存中予以存储。

基于上述网络模型及配置,以下详细描述网络主动防御机制的建立过程。表 1 中给出所涉及到的相关符号及其表示的含义。

表 1 网络主动防御机制建立过程中使用的符号定义

Table 1 The symbol definition of the process that the establishment of network active defense

符号	含义描述
H	远程控制设备
B	基站节点集合
S	普通传感器节点集合
B_i	第 i 级别的基站集合
S_i	普通传感器节点 i
ID_i	节点 i 的身份号
$Request$	请求消息
$Affirm$	确认消息
$Broadcast::(hello)$	广播 hello 消息
$Info$	基站、传感器节点通讯覆盖范围及资源使用情况信息
K_{B_i}	B_i 基站使用的站间会话密钥
KS_i	S_i 节点与基站之间的共享密钥
N_A	节点或基站 A 产生的一个随机数 Nonce
T	时间阈值:基站、节点最长的响应时间
$\{M\}K_{enc}$	表示用密钥 K_{enc} 加密的消息密文
$MAC(K_{mac}, C E)$	消息认证码协议,实现消息的完整性和点对点认证
λ_i	基站在网络中的级别为 i 级

主动防御建立的具体步骤如下:

(1) 远程控制设备 H 向网络中所有基站节点广播 hello 消息,在 $t \leq T$ 的时间范围内,最先响应的基站(网络中第 1 级别基站)向远程控制设备 H 发送自身的 ID 和 Info 信息,并利用预先存储的站间会话密钥 K_{B_1} 与之建立安全通信。此过程涉及到的加密与认证过程的公式化描述如下:

$$H \rightarrow B: Broadcast::(hello)$$

$$B_1 \rightarrow H: \{ID_{B_1} | Info\} K_{B_1}, MAC(K_{B_1}, N_{B_1} | ID_{B_1} | Info)$$

$$H \rightarrow B_1: Affirm, MAC(K_{B_1}, N_{B_1} | Affirm)$$

(2) 第 1 级别的基站 B_1 向远程控制设备 H 申请其周围第 2 级别的基站 B_2 的站间会话密钥 K_{B_2} 。两基站都拥有站间会话密钥 K_{B_2} 的条件下可以建立起安全通信。

$$B_1 \rightarrow H: ID_{B_1}, Request, MAC(K_{B_1}, N_{B_1} | ID_{B_1} | Request)$$

$$H \rightarrow B_1: Affirm, K_{B_2}, MAC(K_{B_1}, N_{B_1} | Affirm | K_{B_2})$$

$$B_1 \rightarrow B_2: Broadcast::(hello)$$

$$B_2 \rightarrow B_1: ID_{B_2}, \lambda_2, MAC(K_{B_2}, N_{B_1} | ID_{B_2} | \lambda_2)$$

(3) 这个过程持续下去直到网络中各个级别的基站节点建立起安全通信。即网络中第 i ($i \geq 2$) 级别的基站 B_i 向远程控制设备 H 申请周围距离其最近的第 $i+1$ 级别的基站 B_{i+1} 的站间会话密钥 $K_{B_{i+1}}$, 在两基站都拥有站间会话密钥 $K_{B_{i+1}}$ 的条件下可以建立起安全通信,公式化描述如下:

$$B_i \rightarrow H: ID_{B_i}, Request, MAC(K_{B_i}, N_{B_i} | ID_{B_i} | Request)$$

$$H \rightarrow B_i: Affirm, K_{B_{i+1}}, MAC(K_{B_i}, N_{B_i} | Affirm | K_{B_{i+1}})$$

$B_i \rightarrow B_{i+1} : Broadcast :: (hello)$

$B_{i+1} \rightarrow B_i : ID_{B_{i+1}}, \lambda_{i+1}, MAC(K_{B_{i+1}}, N_{B_i} | ID_{B_{i+1}} | \lambda_{i+1})$

(4) 对于同级别的两基站,由于两基站间拥有共同会话密钥,只需一方基站向另一方申请通讯即能建立起安全通讯。经过(1)(2)(3)(4)四步,建立基站间的安全通信。

(5) 每个基站节点向其周围普通传感器节点广播自己存储的节点 ID 列表 $\{ID_S\}$,在 $t \leq T$ 的时间范围内,广播范围内具有节点 ID 列表中 ID 号的节点响应消息并请求加入该基站所在的分组,这样每一个基站与其组内的节点建立起了安全通信。

$B_r \rightarrow S_r : Broadcast :: (ID_S)$

$S_r \rightarrow B_r : ID_{S_r}, Request, MAC(KS_r, N_{S_r} | ID_{S_r} | Request)$

$B_r \rightarrow S_r : Affirm, MAC(KS_r, N_{S_r} | Affirm)$

(6) 对于每一个组内,处于一跳直接通讯范围内的两普通传感器节点 S_i 和 S_j ,由任一方(这里假设为 S_j)向其从属的基站 B_i 申请临时的通信密钥 $SK_{S_i-S_j}$ (注:由于基站与其组内每个节点间存在着共享密钥,SNEP 协议^[5]保证了 S_i 和 S_j 可以通过基站为接下来的通信建立临时通信密钥 $SK_{S_i-S_j}$)在拥有通信密钥 $SK_{S_i-S_j}$ 的条件下两节点建立安全通信,公式化描述如下:

$S_i \rightarrow S_j : N_{S_i}, ID_{S_i}$

$S_j \rightarrow B_i : N_{S_i}, N_{S_j}, ID_{S_i}, ID_{S_j}, Request,$

$MAC(KS_j, N_{S_i} | N_{S_j} | ID_{S_i} | ID_{S_j} | Request)$

$B_i \rightarrow S_i : Affirm, \{SK_{S_i-S_j}\} KS_i,$

$MAC(KS_i, N_{S_i} | ID_{S_j} | Affirm | \{SK_{S_i-S_j}\} KS_i)$

$B_i \rightarrow S_j : Affirm, \{SK_{S_i-S_j}\} KS_j,$

$MAC(KS_j, N_{S_j} | ID_{S_i} | Affirm | \{SK_{S_i-S_j}\} KS_j)$

(7) 对于不同组间处于一跳的直接通讯范围内的两普通传感器节点 S_m 和 S_n 分别通过其各自所属基站找到共同控制他们的基站,然后向此基站申请临时的通信密钥(此过程类似于(5))。

经步骤(1)~(4),建立起基站间的安全通信;经步骤(5)每一个基站与其组内的节点建立起安全通信;步骤(6)建立了组内的节点间的通信;步骤(7)建立起不同组间的节点之间的通信。至此,采用改进的 SPINS 安全框架协议为网络搭建主动防御机制就完成了。图 2 是网络主动防御建立的详细流程图。

2.2 网络被动防御机制的建立——变换基站

传感器网络节点可以采用各种主动和被动的防御措施来抵制进攻者的攻击行为。被动防御^[5]是指网络遭受攻击后,节点为减小攻击影响而采取的

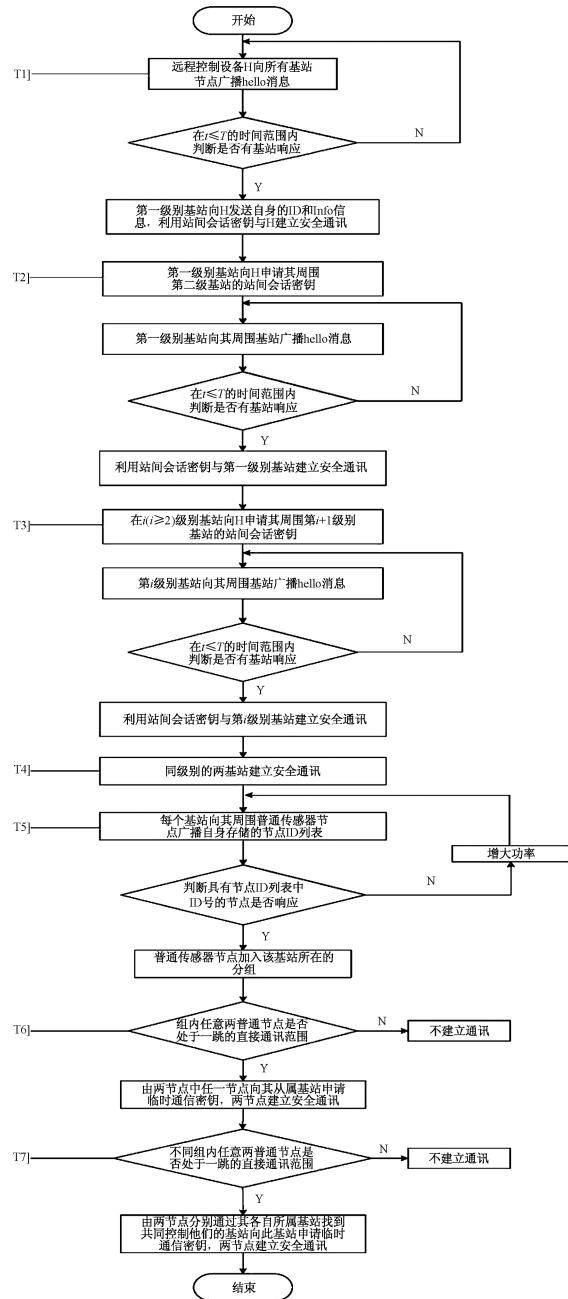


图 2 网络主动防御建立的流程图

Fig. 2 The process diagram of the establishment of active defense

措施。尽管上面建立的网络模型采用了密钥认证的主动防御机制,能抵御多数攻击,但并非万能。本文考虑到基站在整个网络通讯中的重要作用,提出了一种被动防御机制——变换基站,即基站不可信^[8]的情况下将当前基站在整个网络中饰演的角色交给附近同一级别的基站,进而保证整个网络的正常运行。下面就基站变换过程作详细的描述,为了叙述的方便不妨假设 B_{22} 基站遭受攻击,为了网络的正常运行需要将其饰演的角色交付与距离其最近的同一级别的基站 B_{23} 。采用表 1 的描述方法,此过程给出涉及到的相关符号及其表示的含义如表 2 所示。

表 2 基站变换过程中使用的符号定义

Table 2 The symbol definition of the process
that exchange of base-station

符号	含义描述
H	远程控制设备
B_{22}	假设遭受攻击的基站
B_{23}	基站变换过程替换 B_{22} 的基站
S	普通传感器节点的集合
S_i	普通传感器节点 i
$\{ID_s\}$	B_{22} 基站存储的组内节点 ID 列表
$Request$	请求消息
$Affirm$	确认消息
$Agree$	允许变换消息
$K_{B_{22}}$	B_{22} 基站使用的站间会话密钥

(1) 基站 B_{22} 遭受攻击报警, 启动基站变换过程, 由 B_{22} 向远程控制设备 H 提交变换申请并提交自己的 ID 号, 基站等级 λ_2 和替换它的基站 B_{23} 的 ID 号, 远程控制设备 H 核对基站所提供的信息并发送允许变换消息。公式化描述如下:

$$\begin{aligned} & B_{22} \rightarrow H : ID_{B_{22}}, ID_{B_{23}}, Request, \\ & MAC(K_{B_{22}}, N_{B_{22}} | ID_{B_{22}} | ID_{B_{23}} | \lambda_2 | Request) \\ & H \rightarrow B_{22} : Agree, MAC(K_{B_{22}}, N_{B_{22}} | Agree) \end{aligned}$$

(2) 基站 B_{22} 向替换它的基站 B_{23} 发送其存储的组内所有节点的 ID 列表和密钥(假设为: $\{KS_1, KS_2, KS_3 \dots, KS_n\}$), B_{23} 收到后发送确认消息。

$$\begin{aligned} & B_{22} \rightarrow B_{23} : \{ID_s\}, \{KS_1 | KS_2 | KS_3 | \dots | KS_n\}, \\ & MAC(K_{B_{22}}, N_{B_{22}} | \{KS_1 | KS_2 | KS_3 | \dots | KS_n\} | \{ID_s\}) \\ & B_{23} \rightarrow B_{22} : Affirm, MAC(K_{B_{22}}, N_{B_{22}} | Affirm) \end{aligned}$$

(3) B_{23} 由于拥有了原基站 B_{22} 存储的组内所有节点的 ID 列表和密钥, 它通过广播自己存储的节点 ID 列表, 在 $t \leq T$ 的时间范围内, 广播范围内具有节点 ID 列表中 ID 号的节点响应消息并请求加入该基站所在的分组。

$$\begin{aligned} & B_{23} \rightarrow S : Broadcast :: (ID_s) \\ & S_i \rightarrow B_{23} : ID_{S_i}, Request, MAC(KS_i, N_{S_i} | ID_{S_i} | Request) \\ & B_{23} \rightarrow S_i : Affirm, MAC(KS_i, N_{S_i} | Affirm) \end{aligned}$$

(4) B_{23} 向远程控制设备 H 发送基站变换完毕消息, 远程控制设备 H 核对基站所提供的信息后发送确认消息。

$$\begin{aligned} & B_{23} \rightarrow H : ID_{B_{23}}, Notice, MAC(K_{B_{23}}, N_{B_{23}} | ID_{B_{23}} | Notice) \\ & H \rightarrow B_{23} : Affirm, MAC(K_{B_{23}}, N_{B_{23}} | Affirm) \quad \text{至此, 变换} \\ & \text{基站的被动防御机制就建立完成。} \end{aligned}$$

3 性能分析

本文将从安全性, 抗毁性^[12], 网络的生命周期^[13], 三个方面分析比较此通讯策略的性能。

3.1 安全性

由于无线传感器网络自身的一些特性, 如存储空间和计算能力有限、通信带宽和通信能量有限, 布置区域的物理安全无法保证, 后期节点布置的先验知识缺乏等, 使得传感器节点容易被攻击者干扰和破坏。攻击者可能会篡改、伪造路由消息; 攻击者也可利用传感器节点彼此之间需频繁交换信息这一特点, 以不同的身份连续向某一邻居节点发送路由或数据请求, 使该邻居节点资源耗尽(DoS 攻击); 攻击者还可能利用无线传感器网络大多都通过 HELLO 报文来确定邻居关系这一特点, 使用一个拥有大功率发送器的恶意节点去发送 HELLO 报文, 使得网络中很大范围内的节点都误以为这个恶意节点就是自己的邻居^[14](HELLO 泛洪攻击); 鉴于基站在网络通讯中的重要作用, 在某些重要区域(如战场)攻击者通常选取基站为目标发起攻击。

一般地, 针对篡改、伪造路由消息攻击, 相应的对策是在发送的消息后面附加一个消息验证码(Message Authentication Code, MAC)。这样接收端可通过该 MAC 来确认消息是否为伪造消息或在传输过程是否被篡改过^[15]。本文采用改进的 SPINS 安全框架协议为网络搭建主动防御机制, 基站间、基站与其组内节点间、组内节点间、不同组间的节点之间通讯建立过程都采用消息验证码(MAC)协议, 有效地解决了篡改、伪造路由消息攻击的问题; 解决 DoS 攻击最根本的方法是实行逐跳认证, 使恶意节点的 DoS 攻击包在刚进入网络时就被丢弃, 这就要求直接通信的节点之间共享密钥^[9]。本文在网络主动防御机制建立之初进行网络配置时就考虑了 DoS 攻击这一问题, 使用随机密钥预分配机制实现点到点逐跳密钥认证的安全通讯, 从而有效地抵御了 DoS 攻击; 对付 HELLO 泛洪攻击最有效的方法是依靠一个可信任的基站用身份鉴别的方式为每个节点证实它的邻居^[16], 本文所提出的安全通讯策略保证了每个节点与可信赖的基站共享唯一对称密钥, 这样, 处于单跳通讯范围内的两相邻节点可以通过基站产生一个共享密钥, 相邻节点使用这个产生的密钥鉴别彼此的身份, 从而抵御了 HELLO 泛洪攻击; 针对某些区域的基站易受攻击这一情况, 本文提出了被动防御机制—变换基站, 为此可设置变换启动指令为不定期变换。此举可使攻击者攻击基站时缺乏目标性, 从而有效地降低了基站被攻击的可能性。

综上述, 表 3 给出了传统网络与兼具主、被动防御机制的安全通讯网络在网络安全性能方面的比较。其中 Y 表示可以抵御, N 表示不可抵御。通过表 3, 可以明显看出后者的网络安全性能显著优于前者。

表3 网络安全性比较
Table 3 Comparison of network security

安全特性	传统网络	安全通讯网络
篡改	N	Y
伪造	N	Y
DoS 攻击	N	Y
HELLO 泛洪攻击	N	Y
基站攻击	无能为力	有效降低

3.2 抗毁性

本文采用改进的SPINS安全框架协议为网络搭建主动防御机制,网络主动防御机制建立过程中由于各个节点与基站间使用的密钥不相关,所以构建的网络抗毁性较好。现有的无线传感器网络中,一般都是采用基站不变的通讯策略,不仅对基站本身的性能要求较高,而且对基站过分依赖。本文提出的变换基站的被动防御策略弱化了整个网络对基站的过分依赖性,一旦基站遭受恶意节点的攻击立即停止当前基站的工作,启动基站变换过程,将当前基站在整个网络中饰演的角色交给网络中其他基站。此举降低了网络因恶意节点的攻击无法正常工作、陷入瘫痪的可能性,在很大程度上提高了网络的抗毁能力。

3.3 网络的生命周期

传统自组织方式链接成的网络和现有的分簇网络由于“热区”现象^[17]的存在容易造成网络节点能量不均衡消耗从而导致整个网络过早失效,本文构建的树状网络模型由于相邻节点、基站之间存在着多种动态通讯方式,既可以逐级向上集中通讯又可以通过相邻节点相互转发通讯,能均衡网络能量的消耗,有效延长网络的生命周期。

4 结束语

本文提出了一种兼具主、被动防御措施的无线传感器网络安全通讯策略。采用改进的SPINS安全框架协议搭建主动防御机制以及结合基站变换的被动防御机制实现了整个网络内部的安全通讯,为网络创造了一个相对安全的工作环境。此外,该策略采用的集中式与分布式相结合的通讯方式更能适用于大规模的无线传感器网络,具有较强的可行性。

参 考 文 献

- Dargie W, Poellabauer C. Fundamentals of Wireless Sensor Networks: theory and practice. New York: John Wiley and Sons Inc, 2010;3—44
- Akyildiz, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks. IEEE Communications Magazine, 2002;40(8): 102—114
- 沈玉龙,裴庆祺,马建峰,等.无线传感器网络安全技术概论.北京:人民邮电出版社,2010;2—19

- Shen Y L, Pei Q Q, Ma J F, et al. The introduction of wireless sensor network security technology. Beijing: Posts and Telecom Press, 2010;2—19
- 钱志鸿,王义君.面向物联网的无线传感器网络综述.电子与信息学报,2013;35(1): 215—227
 - Qian Z H, Wang Y J. Internet of things-oriented wireless sensor networks review. Journal of Electronics and Information Technology, 2013;35(1):215—227
 - 孙利民,李建中,陈渝,等.无线传感器网络.北京:清华大学出版社,2005: 182—188
 - Sun L M, Li J Z, Chen Y, et al. Wireless sensor network. Beijing: Tsinghua University Press, 2005;182—188
 - 高建斌,娄渊胜.面向主动防御的无线传感器网络安全框架.计算机技术与发展,2012;22(9): 228—231
 - Gao J B, Lou Y S. Security framework oriented active defense for wireless sensor network. Computer Technology and Development, 2012;22(9): 228—231
 - Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor network. Wireless Networks, 2002;8(5):521—534
 - 朱磊,吴灏,王清贤.基于可信基站的SPINS协议研究与改进.计算机应用研究,2010;27(5):2331—2334
 - Zhu L, Wu H, Wang Q X. Security research and improvement of SPINS protocol. Application Research of Computers, 2010;27 (6): 2331—2334
 - 彭志娟,王汝传,孙力娟.无线传感器网络SPINS安全协议分析与改进.无线通信技术,2007;16(1):14—16
 - Peng Z J, Wang R C, Sun L J. Security analysis and improvement of the SPINS protocol. Wireless Communication Technology, 2007;16(1):14—16
 - 敬超,常亮,古天龙.基于SPINS的无线传感器网络安全协议建模与分析.计算机科学,2009;36(10):132—136
 - Jing C, Chang L, Gu T L. Using SPIN to model and analyze security protocol in wireless sensor network. Computer Science, 2009;36(10):132—136
 - 王睿,韩芳溪,张晓丽.无线传感器网络密钥预分配与动态分配策略.计算机工程与应用,2006;42(3):120—122
 - Wang R, Han F X, Zhang X L. The scheme of key pre-distribution and dynamic distribution in wireless sensor networks. Computer Engineering and Applications, 2006;42(3):120—122
 - 李文锋,符修文.无线传感器网络抗毁性.计算机学报,2015;38(3): 27—30
 - Li W F, Fu X W. Survey on invulnerability of wireless sensor networks. Chinese Journal of Computers, 2015;38(3):27—30
 - 刘浩然,尹文晓,韩涛,等.一种优化无线传感器网络生命周期的容错拓扑研究.物理学报,2014; 63 (4): 040509-1—040509-6
 - Liu H R, Yin W X, Han T, et al. Wireless sensor network fault tolerant topology for lifetime optimization. Acta Physica Sinica, 2014; 63(4):040509-1—040509-6
 - 曾志峰,邱慧敏,朱龙海.无线传感器网络中的安全威胁分析及对策.计算机应用研究,2007;24(1): 140—143
 - Zeng Z F, Qiu H M, Zhu L H. Risk analysis and security countermeasure about wireless sensor network. Application Research of Computers, 2007;24(1):140—143

(下转第 258 页)

Big Data Network Intrusion Traces of Process Data Monitoring Method Research

ZHANG Kai

(Chongqing Meteorological Bureau, Chongqing 401147, P. R. China)

[Abstract] Big data network data size, traces the process of intrusion data monitoring efficiency is low, often some data with invasion of trace characteristics under the environment of big data, characteristic gradually fade out, under the condition of current method can't play down the characteristics of accurate gathering trace data, unable to form for monitoring data and trace data, the relationship between the monitoring efficiency and low accuracy. A kind of big data network was put forward based on fuzzy clustering probability of process data monitoring method, the trace of the collected data into frequency domain signal, the spectrum and power spectrum analysis, according to the time change amplitude convert them to change with frequency power. Using Kernel principal component analysis to trace data signal characteristic extraction, using nonlinear transformation to trace sample data signals from the input space is mapped to high-dimensional feature space, in the high dimensional feature space by PCA to trace data signal in the frequency domain feature extraction. Build a mathematical model to simulate the characteristics of fuzzy clustering probability description, treatment of monitoring data and trace data between the characteristics of the fuzzy clustering probability calculation, by comparing the measure theory makes big data in the process of network intrusion trace monitoring data is complete. The experimental results show that the proposed method is not only less time required, and monitoring of high precision.

[Key words] big data network the invasion process trace data monitoring

(上接第 253 页)

- 15 马亲民,王晓春,戴光智.无线传感器网络面临的攻击与对策.传感器与微系统,2012;31(3):8—10,14
Ma Q M, Wang X C, Dai G Z. Attacks and countermeasures faced by WSNs. Transducer and Microsystem Technologies, 2012;31(3):8—10,14
- 16 蒋云霞,符 琦.无线传感器网络(WSNs)路由安全问题的现状与对策研究.中国安全科学学报,2008;18(12):117—123
Jiang Y X, Fu Q. Current status of routing security of WSNs and its countermeasures. China Safety Science Journal, 2008; 18 (12) : 117—123
- 17 李成法,陈贵海,叶 懇,等.一种基于非均匀分簇的无线传感器网络路由协议.计算机学报,2007;30(1):27—36
Li C F, Chen G H, Ye M, et al. An uneven cluster-Based routing protocol for wireless sensor networks. Chinese Journal of Computers, 2007;30(1):27—36

A Security Communication Strategy for WSNs with both Active and Passive Defenses

SUN Jia-wen, YANG Bo, JIA Xin-chun

(School of Mathematical Sciences, Shanxi University, Taiyuan 030006, P. R. China)

[Abstract] Because of its nature features such as openly communication channel, resource-constrained nodes and randomly deployment, the problem of security is facing challenge for wireless sensor networks. In this paper, a security communication strategy which possesses both active and passive defenses is proposed, for the problem of some applications of WSNs which are always placed in dangerous environment that requires high safety. By combining the technology of active defenses which adopt encryption, decryption technique, signature certification, integrity identify, and with passive defenses of transforming the base-station to create a relatively safe operate environment for network. The performance analysis shows this strategy can reduce the possibility of the network under attack, decrease the effect of attack, improve the network anti-dilapidated ability and prolong the lifetime.

[Key words] wireless sensor networks(WSNs) security active defense passive defense