基于计数器对称加密的无线传感器网络入侵检测算法

毛郁欣
（浙江工商大学 计算机与信息工程学院，浙江 杭州 310018）

摘 要：无线传感器网络的内在特性，使得在资源受限的环境下检测恶意节点变得十分困难。为此，提出了一种新型的面向无线传感器网络的入侵检测算法。该方法利用对称密钥进行传感数据加密，同时基于加密的计数器进行恶意节点的检测，充分利用无线传感器网络的路由功能，以达到入侵检测的目的。该方法能够在网络中存在恶意节点的情况下确保数据传输的安全，较为有效地抵御篡改型和数据分组丢弃型的内部攻击。与现有的同类研究相比，该方法更易于在资源受限的无线传感器网络中被实现和运作。

关键词：内部攻击；数据传输；对称加密；入侵检测；无线传感器网络
中图分类号：TN915.08 **文献标识码**：A **文章编号**：1000-436X(2011)9A-0211-09

Intrusion detection algorithm for wireless sensor network based on counter in symmetric encryption

MAO Yu-xin
(School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China)

Abstract: Due to some intrinsic features of wireless sensor network, it was difficult to perform efficient intrusion detection against malicious nodes in such a resource-restricted environment. A novel intrusion detection algorithm was proposed for wireless sensor networks. Symmetric key was used to encrypt sensing data and a counter with encryption was used to detect malicious nodes. The approach made full use of the routing functionality of wireless sensor network to perform intrusion detection. The approach was able to protect the data transmission in a wireless sensor network even if there were malicious nodes in the network. It was able to defend wireless sensor networks against both tampering and packet-dropping attacks. Compared with existing research efforts, the proposed approach is easy to be implemented and performed in resource-constrained wireless sensor networks.

Key words: insider attack; data transmission; symmetric encryption; intrusion detection; wireless sensor network

1 引言

无线传感器网络（WSN，wireless sensor network）是由大量（通常而言）的无线连接的异构传感器节点所组成的空间域上分布的网络系统[1]。WSN 在众多领域有着广泛的应用场景和持续的发展空间[2~3]。然而，WSN 具有无人值守的特性，使得整个网络容易遭受敌对者的恶意攻击。敌对者可以通过物理手段俘获网络中的部分传感器节点来窃取或破坏敏感数据，而这些被捕获节点（也称为恶意节点）则成为网络中数据传输的“黑洞”[4]。因此，数据传输的安全性已经成为 WSN 中的一个重要问题[5]。总体而言，WSN 的安全技术可以分为 2 大类：基于预防的技术和基于检测（例如入侵检

收稿日期：2011-07-05
基金项目：国家自然科学基金资助项目（NSFC 61003309）；浙江省科技计划重大专项基金资助项目（2010C33045）
Foundation Items: The National Natural Science Foundation of China (NSFC 61003309); The Science and Technology Program of Zhejiang Province (2010C33045)

测）的技术[6]。前者通常作为保证网络安全的第一道关卡，但是复杂的防御技术（例如数据加密）会增加整个 WSN 的开销，降低系统的性能。后者通过识别和隔离恶意节点及其内部攻击来提高网络的安全性。当预防失效时，需要进行入侵检测。入侵检测系统（IDS，intrusion detection system）通过监测节点或整个网络的可疑行为来检测恶意节点及其内部攻击[6]。目前，入侵检测已经成为 WSN 研究的热点之一，现有的 WSN 入侵检测技术总体而言还并不成熟[7]，在效果和效率方面都还存在很大的提升空间。由于 WSN 资源受限的特性，使得在 WSN 进行有效的入侵检测变得十分困难，许多传统的智能技术和算法无法直接应用于 WSN 进行入侵检测。因此，面向 WSN 的 IDS 仍然是一个值得深入的研究点。

由于 WSN 中传感器节点具有无人值守的特点，当敌对者通过物理手段捕获 WSN 中的传感器节点时，意味着节点上的安全防御机制包括部分入侵检测机制都可能被破解。当恶意节点获取或者部分获取 WSN 的安全机制的原理，就能有针对性采取措施破坏整个网络的安全性，并最大限度地伪装自身。这一问题普遍存在于各种类型的入侵检测方法，包括集中式的和分布式的。对前者而言，入侵检测的任务往往集中于某个或某几个高性能节点进行（通常是 Sink 节点），而进行检测的节点往往依赖于收集其他普通节点的反馈信息并通过分析来检测恶意节点。如果恶意节点事先了解某个被捕获节点上的安全机制，则可以通过伪造反馈信息来干扰检测节点。对后者而言，不同的传感器节点相对独立地（可能会存在一定的协作）执行入侵检测任务，因此，单个节点包含了相对完整的入侵检测算法和信息。一旦节点被捕获和破解，造成的后果会更加严重。因此，WSN 的入侵检测方法必须在方法本身被恶意节点部分破解的情况下仍然能够正常运作，最大限度地维护网络的安全性。

从现有的研究工作来看，针对 WSN 的恶意节点入侵问题，主要的解决措施包括入侵容忍的路由方法和入侵检测方法。目前在面向安全数据收集的入侵容忍的路由方法方面已经有一些研究进展，例如：Shu 等人提出了一种基于 tn 门限秘密共享算法和随机多路径路由的安全数据收集方法[8]。但是，该方法在发送单个数据分组时造成的开销太大。Deng 等人提出了一种面向 WSN 的入侵容忍路由协议[9]，利用单向散列链、嵌套密钥 MAC 以及多路径路由来确保 WSN 的安全性。但是，该协议主要依赖基站（或 Sink 节点）基于整个网络的拓扑结构来构造多路径路由表。Yao 等人提出了一种面向 WSN 的多路径安全路由协议[10]，但是该协议只考虑了层次结构的 WSN 而没有考虑其他结构。Ouadjaout等人提出了一种WSN 的入侵错误容忍的路由机制[11]，利用了一种安全的多路径通信网络拓扑。但是，该方法的主要缺点在于当发生内部攻击时，不能检测和隔离恶意节点，而且没有考虑当网络的安全机制向恶意节点泄漏时，如何确保网络的安全。而在面向 WSN 的入侵检测方面，也已经有一定的研究进展。Yu 等人提出了一种 WSN 中检测选择性转发攻击的方法[12]，该方法利用多跳确认技术通过获取中继节点的反馈来发起警告。该方法没有考虑恶意节点可能通过丢弃警告包或确认包来破坏入侵检测的情况。Loo 等人提出了一种基于异常的 WSN 入侵检测机制[13]，利用聚类算法来建立正常网络行为模型，并通过模型检测网络通信异常。IDS 被安装在各个传感器节点上，并且独立运作。Da Silva 等人提出了一种构造面向 WSN 的分布式 IDS 的方法[14]，采用基于网络行为干扰的统计手段。这种类型的分布式 IDS 对于资源受限的WSN 而言会造成较大的开销。Su 等人提出了一种能量有效的面向分簇结构 WSN 的入侵防御系统[15]，该系统主要由基于验证的入侵预防子系统和基于协作的入侵检测子系统构成。现有的大部分入侵检测方法没有考虑入侵检测机制方法的原理本身有可能泄漏给恶意节点的情况。Shaikh 等人在文献[16]中注意到了类似的问题，提出 WSN 中的恶意节点有可能通过向其他节点发送虚假的异常和入侵警报来破坏整个网络的安全机制。但是，该方法不能直接处理 WSN 中的篡改或数丢弃型攻击。

针对上述问题，提出了一种新型的面向无线传感器网络的入侵检测算法。该方法利用对称密钥进行传感数据加密，同时基于加密的计数器进行恶意节点的检测，充分利用无线传感器网络的路由功能，以达到入侵检测的目的。该方法能够在网络中存在恶意节点的情况下确保数据传输的安全，较为有效地抵御篡改型和数据分组丢弃型的内部攻击。该方法为 WSN 提供了一种轻量级的相对安全可靠的安全机制。与现有的同类研究相比，该方法更易于在资源受限的无线传感器网

络中被实现和运作。无线传感器网络的路由层可能遭受多种形式的内部攻击，该方法主要针对存在数据篡改或数据分组丢弃（如选择性转发）的攻击。

2　基于对称密钥的 WSN 路由

2.1　网络模型与假设

首先设定一个相对简单的 WSN 模型，它由 2 类节点组成：传感器节点和 Sink 节点。在该模型中，每个传感器节点由独立的电池供电，具备有限的传感、计算和无线通信能力，会定期产生传感数据。此外，WSN 中的每个传感器节点都具有唯一的身份标识（ID，identity）。Sink 节点，也称为基站，是 WSN 的数据收集中心，拥有足够的能量和资源，定期从各个传感器节点收集数据。而且，Sink 节点被认为是安全可信的。假设 WSN 中的节点都是相对固定的，而不是移动的，因此在移动 ad hoc 网络中需要考虑的一些问题在本文的研究内容中将不会重点考虑。敌对者能够通过物理手段捕获并破解传感器节点（Sink 节点除外）。此外，在讨论数据传输问题时，假设产生并发送数据的传感器节点也没有被捕获。网络中的被捕获节点或恶意节点为了更好地隐蔽和伪装，只是选择性地丢弃或篡改一小部分拦截到的数据分组。此外，该模型并不严格区分恶意节点和失效节点（发生故障、能量耗尽或受到干扰的节点），因为失效节点也会导致数据分组丢失。同时，认为 WSN 中恶意节点的数量要远少于正常节点的数量。

此外，假设每个传感器节点在加入网络前已经内置了唯一的对称密钥 K，该密钥在节点部署前和 Sink 节点共享。密钥 K 被用于加密传感数据以及产生数据的 MAC。为了进一步实现较高的安全性，每个节点并不直接使用 K 进行通信，而是通过 K 分别派生出加密密钥 K_E 和 MAC 密钥 K_M[17]。2 个能够通信的节点 A 和 B 之间共享一个加密密钥 $K_{A,B}$，以及一个 MAC 密钥 $K'_{A,B}$。

2.2　安全路由算法

基于上述的 WSN 模型，能够实现从源节点到 Sink 节点的安全数据传输。基于 SPINS 协议提出一种基于对称密钥的安全路由算法，给出算法的伪代码如下：

算法 1　Key-based secure routing algorithm for WSN

输入：A WSN with a collection of sensor nodes $\overline{S} = \{S_0, S_1, \ldots, S_n\}$, a source node S_0, and a sink node S_k, where $S_0, S_k \in \overline{S}$.

输出：

if S_0 wants to send a data packet D to S_k

S_0 selects its next hop S_t ($S_t \in \overline{S}$) from its neighbors

S_0 sends the encrypted packet E to S_t

$E_0 = [\{D \| CNT\}_{<K_0,C>}, MAC(K'_{0,t}, C \| \{D \| CNT\}_{<K_0,C>})]$

CNT++

for each intermediate node S_t

S_t receives the data packet E_{t-1} derived from S_{t-1}

S_t extracts and records CNT from E_{t-1}

S_t forwards E_t to S_{t+1}

$E_t = [\{D \| CNT\}_{<K_0,C>}, MAC(K'_{t,t+1}, C \| \{D \| CNT\}_{<K_0,C>})]$

end loop

end if

if S_k receives the data packet E_m derived from S_0

S_k extracts and records CNT from E_m

S_k decrypts E_m into D

end if

其中，K_i 表示节点 S_i 和 Sink 节点 S_k 之间的加密密钥，$K'_{i,j}$ 表示 S_i 和节点 S_j 之间的 MAC 密钥。在该算法中，源节点在发出的每个数据分组中绑定一个连续递增的序列号。使用计数器 CNT 来表示数据分组的序列号。节点在对数据本身进行加密的同时，也对 CNT 值进行加密，以防止在数据传输过程中被篡改。

在上述算法中，源节点发送到 Sink 节点的数据分组采用密钥 K_E 进行加密，同时通过 MAC 进行验证，因此，恶意节点很难对转发的数据进行篡改，即使进行篡改，也很容易被 Sink 节点检测到。另一方面，如果恶意节点选择性地丢弃数据分组，而并不进行篡改，那么 Sink 节点的入侵检测机制能够立即检测到这种攻击行为。详细的入侵检测算法，将在下一节进行阐述。

3　基于计数器的 WSN 入侵检测

3.1　攻击模式

一旦传感器节点被敌对者捕获，那么节点上内

置的安全机制的细节也会被泄漏。而恶意节点可能针对被破解或部分破解的安全机制采取应对措施来伪装自身，并欺骗其他节点。因此，当WSN的节点被捕获时，很难继续维持网络的安全性。虽然可以通过对节点的代码进行硬件加密来防止被破解，但是这种做法会提高单个节点的成本，对于大规模应用的WSN而言并不现实。为此，需要研究一种新型的WSN入侵检测方法，在部分节点被捕获的情况下仍然能够确保整个网络的安全性。

当一个传感器节点被捕获，该节点可能成为一个恶意节点。假设S_m是WSN中的一个恶意节点，基于前述的WSN模型，其可能的攻击模式包括：

1) S_m选择性地丢弃转发的数据分组；

2) S_m篡改转发的数据分组；

3) S_m篡改转发的数据分组的序列号；

4) S_m伪造用于入侵检测的反馈信息。

通过提出一种新型的入侵检测算法，能够较为有效地检测和处理上述几种攻击。在算法的具体实现上，假设恶意节点是分别发起攻击的，不考虑2个以上节点的合谋攻击（例如wormhole）。源节点发送到Sink节点的数据分组采用密钥K_E进行加密，同时通过MAC进行验证，因此，恶意节点很难对转发的数据进行篡改，即使进行篡改，也很容易被Sink节点检测到。如果恶意节点选择性地丢弃数据分组，而并不进行篡改，那么Sink节点的入侵检测机制能够立即检测到这种攻击行为，因为源节点产生的每个数据分组都带有一个连续递增的序列号。

3.2 入侵检测算法

针对WSN中存在恶意节点的情况，提出一种基于加密计数器的入侵检测算法。该算法是一种在线检测算法，能够在恶意节点发起攻击之后进行检测。给出的算法的伪代码如下：

算法2 Counter-based intrusion detection algorithm for WSN

输入：A WSN with a collection of sensor nodes $\overline{S}=\{S_0,S_1,\cdots,S_n\}$, a source node S_0, a sink node S_k and a collection of malicious nodes $\overline{S}_m=\{S_i,S_{i+1},\cdots,S_j\}$, where $S_0,S_k\ \overline{S}\ ,\overline{S}_m\ \overline{S}$

输出：

S_0 sends a series of data packets $\overline{D}=\{D_1,D_2,\cdots,D_m\}$ to S_n with a time interval of Δt

for each intermediate node S_{mi} on a routing path from S_0 to S_k

S_{mi} caches the latest three packets passing by

end loop

for each pair of packets (D_i,D_{i+1}) S_k receives

S_k decrypts their contents by key

if S_k detects a tampered packet

S_k broadcasts an alert packet

end if

S_k verifies their sequential numbers

if S_k detects a discontinuous sequential number

S_k broadcasts an alert packet

end if

for each intermediate node S_{mi} receiving the alert

S_{mi} verifies the packets within its cache

if S_{mi} detects a missing packet

S_{mi} sends back an alert to S_k

else if S_{mi} detects a tampered packet

S_{mi} sends back an alert to S_k

else

S_{mi} sends back a normal response packet

end if

end loop

if S_k receives a collection of response packets

if an intermediate node S_{mi} does not send back a response

S_k records the identity of S_{mi}

end if

S_k analyzes the status information of the nodes on the routing path

S_k finds out the malicious nodes

S_k broadcasts the identity of malicious nodes

end if

end loop

1) Sink节点检测异常，普通节点反馈状态

根据上述算法，Sink节点内嵌的入侵检测算法对于恶意节点而言是保密的，所以即使敌对者捕获了一部分传感器节点，也无法完全获取整个网络的入侵检测机制。普通的传感器节点无法了解Sink节点如何确定一个节点是恶意节点的决策过程。当一个正常节点被捕获并成为一个恶意节点之后，该节点只能掌握节点上原有的那部分安全机制，而无法了解Sink端的决策过程（如图1所示）。因此，恶意节点也就无法有效预测Sink节点的行为。恶意节点采取的措施就是模仿正常节点，最大限度地伪

装自身，同时尽可能地破坏网络。

如前所述，恶意节点攻击 WSN 时主要采取 2 种方式：篡改或丢弃数据分组。上述入侵检测算法对于这 2 种攻击行为，都能够有效地进行处理。如果恶意节点篡改需要转发数据分组的内容，那么被篡改过的数据分组最终将会被转发到 Sink 节点。路由路径上的中继节点没有读取和验证数据分组原始内容的密钥，无法检测到数据分组被恶意节点篡改的异常行为。当 Sink 节点最终收到被篡改的数据分组时，将无法正常解密数据分组的内容（恶意节点是在无密钥的前提下进行恶意篡改的），因此 Sink 能够直接检测到这种异常。Sink 检测到篡改行为之后，会立即通过向路由路径上的所有节点以广播的形式发起入侵警告，警告包中包含了被篡改的数据分组的内容。为了有效地保护警告包的内容，Sink 节点会利用广播密钥[18]进行加密，广播加密的用户组被设定为路由路径上的所有节点。路径上的节点能够利用自身的私钥解密并读取警告包的内容。

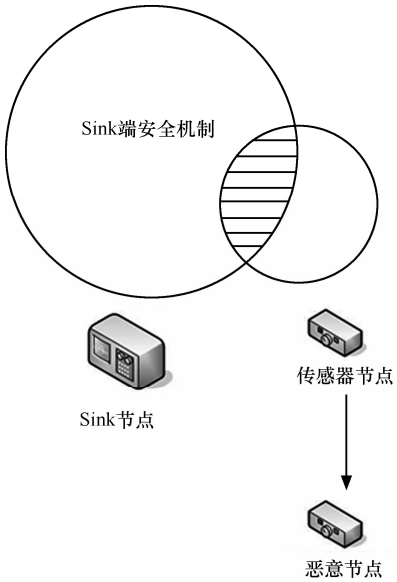

图 1　Sink 端的安全机制与恶意节点之间的关系

如果恶意节点丢弃中转的数据分组，那么该数据分组不会被转发到 Sink 节点。为了验证被丢弃或篡改的数据分组，路由路径上的每个传感器节点（包括 Sink 节点和源节点）都必须缓存最近转发的数据分组。当 Sink 节点检测到一个被丢弃或篡改的数据分组时，需要通过路由路径上的其他节点交换信息来进行验证。当 Sink 节点从接收到的数据分组中检测到不连续的数据分组序列号时，会立即通过向路由路径上的所有节点以广播的形式发起入侵警告，警告包包含了 2 个不连续数据分组的密文。例如，当 Sink 节点收到 2 个序列号不连续的数据分组 $\{D_0 \| CNT\}_{<K_0,C>}$ 和 $\{D_2 \| CNT+2\}_{<K_0,C>}$ 时，说明序列号为 CNT+1 的数据分组可能被丢弃了。因此，Sink 节点将 2 个数据分组的密文封装到一个警告包中，并向路由路径上的节点广播。为了有效地保护警告包的内容，Sink 节点也会利用广播密钥进行加密。如果恶意节点丢弃所有的中转数据分组，那么该恶意节点就成为一个“黑洞”。黑洞攻击可以被认为是一种特殊的选择性转发攻击（转发的概率为 0）。

当接收到来自 Sink 节点的警告包时，每个传感器节点首先确认警告包的类型。如果该警告包是关于数据分组篡改的，那么节点会对被篡改数据分组 D 的内容和本地缓存中的数据分组内容进行比较。如果节点在缓存中能找到匹配的数据分组，则向 Sink 节点反馈一个消极报告，通知 Sink 节点在接收数据分组 D 之前该数据分组已经被篡改。如果节点在缓存中没有找到匹配的数据分组，则向 Sink 节点反馈一个积极报告，通知 Sink 节点自己接收的数据分组 D 是正常的。如果该警告包是关于数据分组丢弃的，那么节点会将不连续数据分组 D_1 和 D_2 的内容和本地缓存中的数据分组内容进行比较。如果节点在缓存中能找到一个介于两者之间的数据分组，则向 Sink 节点反馈一个积极报告，通知 Sink 节点自己拥有被丢弃的数据分组。如果节点在缓存中没有找到满足要求的数据分组，则向 Sink 节点反馈一个消极报告，通知 Sink 节点某个数据分组可能在自己接收之前已经被恶意节点丢弃了。

定理 1　如果路由路径上的某个节点为了替 Sink 节点验证丢弃的数据分组，则至少必须缓存 2 个最近中转的数据分组。

证明　首先证明充分性。如果 Sink 节点检测到一个可能被丢弃的数据分组（D_1），说明至少已经接收到了 2 个序列号不连续的数据分组（D_0 和 D_2）。D_1 和 D_2 是 Sink 节点最近接收到的 2 个数据分组。如果路由路径上的某个节点缓存了至少 2 个最近中转的数据分组，那么可能存在 2 种缓存结果（见表 1）。不论何种缓存结果，都可以验证 Sink 节点没有接收到 D_1。接着证明必要性。如果路由路径上节点缓存的最近的数据分组少于 2 个，那么说明缓存了一个最近中转的数据分组，这个数据分组必然是 D_2。因此，节点就无

法验证 Sink 节点是否接收到了 D_1。

表1 节点缓存最近中转的数据分组的2种结果

缓存结果	缓存的数据分组
数据分组被节点的上游节点丢弃	D_0 和 D_2
数据分组没有被节点的上游节点丢弃	D_1 和 D_2

通过检测本地缓存中的数据分组，传感器节点向 Sink 节点反馈关于被丢弃或被篡改的数据分组的状态信息。由于恶意节点事先部分（普通传感器节点端的）破解了网络的入侵检测机制，也可能会反馈状态信息。恶意节点通过反馈虚假的反馈报告来伪装自身和欺骗 Sink 节点。

2) Sink 检测并隔离恶意节点

当 Sink 节点接收到一系列来自于路由路径上节点的报告包之后，则试图通过分析这些报告包来找出恶意节点。可以用状态位（status bit）来表示一个节点在反馈阶段的状态信息。如果节点反馈了一个消极的报告包，那么对应的状态位为 1，如果节点反馈了一个积极的报告包，那么对应的状态位为 0，如果节点没有反馈任何报告包，那么对应的状态位为 1。Sink 节点在设定的响应周期内接收到报告包之后，可以得到一系列的状态位。路由路径上的节点在某一轮反馈中的状态可以表示为一个向量$[b_1, b_2, \cdots, b_n]$，其中"$b_i \in \{-1, 0, 1\}$。通过一轮反馈，得到一个状态位向量（简称状态向量）。Sink 节点可以通过分析状态向量来进行入侵检测。

对于一个状态向量 $B = [b_1, b_2, \cdots, b_n]$，Sink 节点首先找出所有值为 1 的状态位，并将对应的节点添加一个结果集 $\overline{S}_w$ 中。$\overline{S}_w$ 包含了所有没有向 Sink 节点反馈的节点。$\overline{S}_w$ 中的节点都被认为是可疑节点，而不是恶意节点。因为节点可能由于干扰或通信质量差等原因没有正常接收或发送数据分组，所以允许暂时性的节点失效。$\overline{S}_w$ 被称为可疑集合，其中的节点不会被立即排除在路由路径之外。但是，Sink 节点在后续的数据传输过程中，会特别注意这些可疑节点。接着，Sink 节点分析 B 中的其余部分。对于任意的 $b_{i-1}, b_i \in B$，如果 $b_{i-1}=0$ 或 1，且 $b_i=1$，那么 b_{i-1} 被称为 B 中的一个变化点。变化点代表了路由路径上的一个传感器节点，其对应的状态位的值从 0 或 1 跳变为 1。

定理2 如果 S_c 是一个变化点，S_{cd} 是其路由路径上最近的下游节点，那么序列(S_c, S_{cd})包含了一个恶意节点。

证明 不失一般性，假设 S_m 是路由路径上距离 Sink 节点最近的一个恶意节点。S_m 的最近上游节点是 S_{mu}，最近下游节点是 S_{md}。同时，考虑在警告/反馈阶段中的 3 个特殊节点：路由路径最后（从源节点到 Sink 节点）一个反馈积极报告包的节点 S_n，该节点向 Sink 节点反馈积极的报告包（S_n 的最近上游节点，S_n 的最近下游节点。Sink 节点在进行入侵检测时，主要针对这 3 个节点）。可以分 3 种情况进行分析：

1) S_m 通过反馈一个虚假的消极报告包来伪装自身和欺骗 Sink 节点。在这种情况下，S_n 是 S_{mu}，S_{nu} 是 S_{mu} 的最近上游节点，S_{nd} 是 S_m。

2) S_m 反馈一个正常的积极报告包。在这种情况下，S_n 是 S_m，S_{nu} 是 S_{mu}，S_{nd} 是 S_{md}。

3) S_m 不反馈任何报告包。在这种情况下，S_n 是 S_m，S_{nu} 是 S_{mu}，S_{nd} 是 S_{md}。

在上述任何一种情况下，S_m 都处于序列(S_{nu}, S_n, S_{nd})中。虽然很难进一步确定这个集合中哪个节点是真正的恶意节点，但是可以将集合中的所有节点都认定为恶意节点并隔离在路由路径之外。这样做的依据在于，对一个存在内部攻击的 WSN 而言，不必进一步区分恶意节点和受威胁的节点。受威胁的节点是指距离恶意节点很近（一跳以内），直接受恶意节点影响的正常节点。因为受威胁的节点对于路由而言也是不安全的，所有恶意节点和受威胁的节点都应该被隔离。文献[19]也已经指出，对恶意节点和受威胁的节点应该采取类似的预防措施。序列(S_{nu}, S_n, S_{nd})被称为恶意序列。对于上述的任意一种情况，都可以得到一系列的恶意序列中的节点的状态位（见表 2）。而通过表 2 可以直观地发现，S_m 始终都处于恶意序列的同一个子序列(S_n, S_{nd})中。

表2 恶意序列中的节点在不同情况下的状态位

情况	节点	S_{mu}的最近上游节点	S_{mu}	S_m	S_{md}
情况1	序列元素	S_{nu}	S_n	S_{nd}	—
	状态	0/1	0/1	1	1
情况2	序列元素	—	S_{nu}	S_n	S_{nd}
	状态	0/1	0/1	0	1
情况3	序列元素	—	S_{nu}	S_n	S_{nd}
	状态	0/1	0/1	1	1

因此，可以将恶意序列进一步精确为(S_n, S_{nd})。通过上述的入侵检测算法，总是能够得到一个长度为 2 的最小恶意序列。在情况 1 中，S_{mu} 是变化点，

而在情况 2 和情况 3 中，S_m 是变化点。最小恶意序列总是包含了一个变化点，以及变化点的最近下游节点。因此，可以同时得到一个关于发起攻击的恶意节点的状态位的信息（如图 2 所示）。图 2 给出了所有可能的变化点和恶意序列。通过定位变化点，以及变化点的最近下游节点，总能得到一个最小的恶意序列，而且该序列总是包含了一个恶意节点。入侵检测算法的主要目标就是找出路由路径上的所有的最小恶意序列。如果路由路径上存在不止一个恶意节点，那么必须执行多次分析找到所有恶意序列。

S_{mu}	S_m	S_{md}
0	1	1
-1	1	1
0	0	1
-1	0	1
0	-1	1
-1	-1	1

图 2　发起攻击的恶意节点的状态位

因此，通过上述的入侵检测算法，最终可以得到一个恶意节点集合 $\overline{S}_m = \bigcup_{i=1}^{k}\{S_n, S_{nd}\}_i$，该集合被称为恶意集合。如果 Sink 节点检测到 2 个矛盾的报告包，则认为对应的发送者都是恶意节点，并且将这些节点也添加到 $\overline{S}_m$ 中。Sink 通过在网络中广播 $\overline{S}_m$ 的节点 ID 来对它们进行隔离。

在上述算法中，数据分组在入侵检测的过程中都采用密钥进行加密，并且通过 MAC 进行验证，因此恶意节点不能直接修改（只能恶意篡改）中转的数据分组。但是，恶意节点可以选择性地丢弃一些数据分组。如果恶意节点恶意篡改了某些数据分组，对于数据分组的接收者而言，由于无法正常解密，相当于恶意节点丢弃了这个数据分组。而在入侵检测的过程中，恶意节点有 3 种机会对检测过程进行破坏。

1）恶意节点可以丢弃部分来自于 Sink 节点广播的用于验证异常的警告包。在这种情况下，恶意节点只能丢弃发送给它上游节点的警告包。如果一个上游节点没有接收到警告包，也就无法反馈报告包给 Sink 节点。但是，对于恶意节点的下游节点则没有任何影响。因此，根据定理 2，Sink 节点还是能够检测到变化点，以及包含了恶意节点的恶意集合。

2）恶意节点也可以丢弃来自于路由路径上其他节点的报告包。在这种情况下，恶意节点也只能丢弃它上游节点的报告包，对它的下游节点则没有任何影响。因此，Sink 节点还是能够检测到变化点，以及包含了恶意节点的恶意集合。

3）恶意节点还可以丢弃来自于 Sink 节点广播的包含了恶意节点 ID 的用于隔离的警告包。然而，当恶意节点的下游节点接收到来自于 Sink 的警告包之后，会立即将其中包含的恶意节点排除在路由路径之外，因此，恶意节点将不能再接收到数据分组。后续的数据分组会通过其他安全的路由路径发送给恶意节点的上游节点。

定理 3　如果一个恶意节点 S_m 篡改或丢弃了中转的数据分组，那么 Sink 节点能够利用基于计数器的入侵检测算法检测并隔离 S_m。

证明　首先考虑 S_m 丢弃中转的数据分组情况。根据假设，S_m 至少已经丢弃了一个数据分组（D_m）。那么，Sink 节点会接收到 2 个序列号不连续的数据分组（D_i 和 D_j，其中 $i<m$ 且 $j>m$）。Sink 节点按照基于计数器的入侵检测算法，验证 D_i 和 D_j 之间被丢弃的数据分组。经过一轮的警告广播和状态反馈之后，Sink 节点将得到一个关于被丢弃数据分组的状态矩阵（B_m）。根据检测算法，无论 S_m 向 Sink 节点反馈何种状态，S_m 都将处于一个包含了 B_m 中变化点的恶意序列。因此，Sink 节点能够直接检测出 S_m，并通过广播 ID 将其隔离在路由路径之外。如果 S_m 丢弃了 2 个以上的数据分组，那么不失一般性，假设 S_m 丢弃了 2 个数据分组（D_{m1} 和 D_{m2}）。在这种情况下，Sink 仍然会接收到 2 个序列号不连续的数据分组（D_i 和 D_j，其中 $i<m1$ 且 $j>m2$）。后续的检测过程和丢弃一个数据分组的情况完全一致。

同理，还可以证明当 S_m 篡改中转数据分组时，Sink 节点利用基于计数器的算法也能够检测并隔离 S_m。

4　性能分析

上述的入侵检测算法不足之处在于，检测恶意节点会导致额外的开销，而主要的开销来自于入侵检测过程中的额外通信。在入侵检测过程中，当 Sink 节点检测到异常时，会向路由路径上的所有节点广播警告包。而每个接收到警告包的节点必须向 Sink 节点反馈报告包。在检测到恶意节点之后，Sink

节点还需要向路由路径上所有节点广播用于隔离恶意节点的警告包。假设路由路径上有N个节点(不包括Sink节点)，路由过程中的单跳延时为Δt，那么一轮入侵检测操作的最大通信开销为

$$\Delta t(N+1)N/2+\Delta t(N+1)N/2+\Delta t(N+1)N/2=(3(N+1)N/2)\Delta t$$

这部分开销是固定的，且只和N相关。假设恶意节点丢弃或篡改数据分组的机率是λ，如果源节点向Sink节点发送了m个数据分组，那么被丢弃或被篡改的数据分组为mλ。每次发生数据分组丢弃或篡改时，Sink节点都要执行入侵检测。因此，需要执行mλ次入侵检测操作，总共的开销为mλ(3(N+1)N/2)Δt。

然而，根据定理3，当恶意节点丢弃或篡改中转的数据分组时，Sink节点就能够进行检测。因此，恶意节点会在数据传输过程的前期就被隔离在路由路径之外。实际上，Sink节点并不需要执行mλ次入侵检测操作。假设N个传感器节点中有M个恶意节点。如果恶意节点之间没有协作，那么Sink节点通过一轮入侵检测操作，至少能够检测并隔离一个恶意节点。Sink节点检测和隔离一个恶意节点所需的开销为(3(N+1)N/2)Δt。最坏情况下，Sink节点需要执行M次操作来找出所有的恶意节点。因此，实际的总体开销为(3M(N+1)N/2)Δt，与参数m和λ无关。对于一般的WSN而言，M<<N，因此这样的开销对于提高WSN的总体安全性而言是可以接受的。假设源节点向Sink节点发送一个数据分组的通信开销为NΔt，那么算法的相对通信开销为

$$\frac{(3M(N+1)N/2)Dt}{NDt}=3M(N+1)/2\sim O(N)$$

入侵检测算法的另一部分开销来自于在安全路由过程中对数据分组的加密和解密。这部分开销主要是节点的计算开销，而不是通信开销。在算法中使用的加密方法相对简单，因此和通信开销相比这部分计算开销很小。因此，主要关注如何减少入侵检测算法的通信开销。

5 结束语

入侵检测作为WSN的一个新兴研究方向，既是研究热点，也是研究难点。在WSN中存在恶意节点并且安全机制本身可能部分泄露的前提下，如何通过尽可能小的网络开销维持整个网络的数据传输安全，是本文重点研究和解决的问题。为此，提出了一种新型的面向无线传感器网络的入侵检测算法。该算法主要利用对称密钥进行传感数据加密，实现WSN中的安全路由；同时，采用基于加密的计数器对恶意节点的攻击行为进行检测，充分利用WSN的路由功能，达到入侵检测的目的。该方法能够在WSN中存在恶意节点的情况下确保数据传输的安全，较为有效地抵御篡改型和数据分组丢弃型的内部攻击。与现有的同类研究相比，该方法更易于在资源受限的WSN中被实现和运作。当然，该算法仍然存在一定的不足，例如，能够处理的攻击类型较少，目前只针对篡改和选择性转发；会造成一定的额外通信开销；目前针对的WSN模型较为简单等，有待进一步改进与完善。

参考文献：

[1] LOW K, WIN W, ER M. Wireless sensor networks for industrial environments[J]. Mater Sci Forum, 1992, 119: 83-87.

[2] AKYILDIZ I, SU W, SANKARASUBRAMANIAM Y, et al. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[3] 崔莉，鞠海玲，苗勇等. 无线传感器网络研究进展[J]. 计算机研究与发展, 2005, 42(1): 163-174.
CUI L, JU H L, MIAO Y, et al. Overview of wireless sensor network[J]. Journal of Computer Research and Development, 2005, 42(1): 163-174.

[4] AKYILDIZ I, SU W, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[5] 彭清泉，裴庆祺，马建峰等. 无线传感器网络中自治愈的群组密钥管理方案[J]. 电子学报, 2010, 38(1): 123-128.
PENG Q Q, PEI Q Q, MA J F, et al. A self-healing group key management scheme in wireless, sensor networks[J]. Acta Electronica Sinica, 2010, 38(1): 123-128.

[6] WOOD A, STANKOVIC J. Denial of service in sensor networks[J]. IEEE Computer, 2002, 35(10): 54-62.

[7] WANG Y, ATTEBURY G, RAMAMURTHY B. A survey of security issues in wireless sensor networks[J]. IEEE Commun Surveys Tutorials, 2006, 8(2): 2-23.

[8] SHU T, LIU S, KRUNZ SECURE M. Secure data collection in wireless sensor networks using randomized dispersive routes[A] Proc.

IEEE INFOCOM Conference[C]. Rio de Janeiro, 2009, 2846-2850.

[9] DENG J, HAN R, MISHRA S. INSENS: Intrusion-tolerant routing for wireless sensor networks[J]. Computer Communication, 2006, 29(2): 216-230.

[10] YAO L, LUO L, GAO F. A multipath secure routing protocol based on malicious node detection[A]. Proceeding of 48th IEEE Conference on Control and Decision Conference[C], Guilin, 2009.4323-4328.

[11] OUADJAOUT A, CHALLAL Y, LASLA N, et al. SEIf: secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks[A]. Third International Conference on Availability, Reliability and Security[C], Barcelona, 2008.503-508.

[12] YU B, XIAO B. Detecting selective forwarding attacks in wireless sensor networks[A]. Proc. International Parallel and Distributed Processing Symposium [C]. Rhodes Island, 2006.351-358.

[13] LOO C, NG Y, LECKIE C, et al. Intrusion detection for routing attacks in sensor networks[J]. Inter J Distrib Sensor Netw, 2006, 2: 313-332.

[14] SILVA A, MARTINS M, ROCHA B, et al. Decentralized intrusion detection in wireless sensor networks[A]. Proc of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet 05)[C]. Montreal, Quebec, 2005.16-23.

[15] SU W, CHANG K, KUO Y. eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks[J]. Comput Netw, 2007, 51: 1151-1168.

[16] SHAIKH R, JAMEEL H, D AURIOL B, et al. Intrusion-aware alert validation algorithm for cooperative distributed intrusion detection schemes of wireless sensor networks[J]. Sesnors, 2009, 9: 5989-6007.

[17] PERRIG A, SZEWCZYK R, WEN V, et al. Spins: security protocols for sensor networks[A]. Seventh Annual International Conference on Mobile Computing and Networking[C]. Rome, Italy, 2001.189-199.

[18] HORWITZ J. A survey of broadcast encryption[EB/OL]. http://math.scu.edu/~jhorwitz/pubs/broadcast.html.

[19] DENG J, HAN R, MISHRA S. INSENS: intrusion-tolerant routing in wireless sensor networks[A]. In the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS 2003)[C]. Palo Alto, CA, 2003.349-264.

作者简介：

毛郁欣（1980-），男，浙江龙泉人，博士，浙江工商大学副教授，主要研究方向为语义 Web、无线传感器网络。