链路相关性欺骗攻击与检测机制

徐佳佳[1,2] 白光伟[1] 沈 航[1,3]
(南京工业大学计算机科学与技术学院 南京 211816)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]
(南京邮电大学通信与网络技术国家工程研究中心 南京 210003)[3]

摘 要 近年来的研究工作表明,无线通信中的数据包传输在不同的链路上存在接收相关性,这一现象对无线网络环境下不同通信协议的性能都有着很大的影响。现有的链路相关性感知协议的性能提升大都依赖链路相关性度量的准确性。然而,通过分析发现,无线网络自身的移动性、射频通信等特点导致其在通信过程中存在着各种威胁与网络攻击。文中结合链路相关性,提出链路相关性感知协议的欺骗攻击机制,即当网络中的源节点发送数据包时,相应的接收节点通过恶意修改自身维持的数据包接收位图中的数据来欺骗源节点,从而达到篡改同一源节点的不同邻居节点之间的链路相关性度量值的目的,因此,该攻击机制会降低协议的传输性能。针对这一攻击机制,文中提出了对应的恶意节点检测机制,即利用 Watchdog 机制对网络中节点的行为进行检测,从而得出真实的数据包接收位图。仿真结果表明,提出的链路相关性欺骗攻击机制增加了通信协议的数据包重传次数,降低了协议传输的性能,同时基于 Watchdog 的恶意节点检测机制对这一攻击具有良好的防御力。

关键词 无线网络,链路相关性,欺骗攻击,检测机制

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.12.016

Link Correlation Spoofing Attack and Detection Mechanism

XU Jia-jia[1,2] BAI Guang-wei[1] SHEN Hang[1,3]
(College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]
(National Engineering Research Center for Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[3]

Abstract Recent studies highlight the existence of link correlation of adjacent wireless links, and this phenomenon has shown significant impact on the performance of various network protocols. The efficiency of these existing link-correlated protocols heavily relies on the accuracy of link correlation measurement. However, analysis shows that due to its features of mobility and RF communication, wireless networks is vulnerable to various threats and attacks. This paper first proposed a spoofing attack mechanism about link correlation aware protocols. When the source node broadcasts packets, some or even all of the corresponding receivers maliciously revise their packet reception bitmaps to tamper link correlation metric, thus degrading protocol performance. Against the attack, a Watchdog-based detection mechanism was proposed to capture a node's behavior with objective of inferring the real packet reception bitmaps. The simulation results show that this spoofing attack increases the retransmission counts, and degrades the performance of communication protocol, while the propoced detection mechanism can defend the spoofing attack effectively.

Keywords Wireless network, Link correlation, Spoofing attack, Detection mechanism

---

到稿日期:2017-09-11 返修日期:2017-11-13 本文受国家自然科学基金项目(61502230,61073197),江苏省自然科学基金项目(BK20150960),江苏省普通高校自然科学研究项目(15KJB520015),南京市科技计划项目(201608009),计算机软件新技术国家重点实验室(南京大学)资助项目(KFKT2017B21),通信与网络技术国家工程研究中心(南京邮电大学)资助项目(GCZX012),江苏省六大高峰人才基金资助项目(第八批)资助。

徐佳佳(1995—),女,硕士生,主要研究方向为无线链路相关性,E-mail:xujiajia@njtech.edu.cn;**白光伟**(1961—),男,博士,教授,博士生导师,CCF 高级会员,主要研究方向为移动互联网、无线传感器网络、网络体系结构和协议、网络系统性能分析和评价、多媒体网络服务质量等;**沈 航**(1984—),男,博士,讲师,硕士生导师,CCF 会员,主要研究方向为无线网络编码、移动互联网、无线多媒体通信协议等,E-mail:hshen@njtech.edu.cn(通信作者)。

1　引言

链路相关性指对于网络中同一发送节点发送的数据包，不同的邻居节点的接收情况并不是相互独立的现象。文献[1]揭示了链路相关性的潜在影响因素是交叉网络干扰和高度动态环境下引入的相关阴影衰减：在拥挤的无线频谱中，高功耗的无线网络交通会在低功耗的网络中引入有害的噪音，导致许多链路同时丢失数据包；由无线电波传播路径上的障碍物引起的信号衰退会导致邻近链路上的数据包传输存在接收相关性，即同时丢失相应的数据包。

链路相关性现象的发现挑战了传统的关于无线链路具有独立性的假设，对广播[2]、组播[3]、机会路由[4-6]以及网络编码[7-8]等不同通信协议的性能有着很大的影响，为无线网络性能的优化提供了新的机会。例如，对于机会路由来说，当候选链路之间呈正相关性时，可利用的空间多样性会减少，因此机会路由协议的性能就会降低。文献[4-5]利用链路相关性来预测网络中转发节点的工作效率，并选择相关性较弱（即空间多样性高）的链路作为下一跳候选链路，从而提高机会路由协议的性能。而对于洪泛和广播协议来说，选择负相关性的链路对作为候选链路会增加数据包的重传次数，从而降低协议的性能。Zhu 等[9]提出的 Collective ACK 利用一条链路的 ACK 来判断与之相关性高的其他链路的数据包接收情况，从而避免 ACK 风暴问题。CorLayer[2]利用链路相关性，在网络通信不断开的前提下，通过拉黑相关性较弱的链路来形成相关性较高的簇，从而减少网络中数据包的重传次数。

目前已有许多关于不同的衡量链路相关性的度量的研究[2,9-11]，其中条件数据包接收（丢失）概率使用得比较广泛。例如，CF 算法[9]使用条件数据包接收概率来衡量链路相关性，而 CoCo 算法[12]使用条件数据包丢失概率作为衡量无线链路相关性的度量指标。由于上述链路相关性感知协议的研究依赖链路相关性度量的准确性对协议的性能进行提升，因此，如果链路相关性度量的衡量不准确，那么协议的性能可能不会提高甚至反而下降。然而，由于其自身具有移动性、传输媒介的开放性以及传输信号的不稳定性等特点[13-14]，无线网络面临着各种威胁和网络攻击，例如 DOS 攻击[14]、选择性转发[13]、虫洞攻击[13]等。通过分析可知，上述链路相关性感知协议的测量方法都是基于 beacon 包的接收位图进行计算的，因此恶意节点可以通过攻击数据包接收位图中的数据，来达到攻击整个链路相关性感知协议的性能的目的。

本文提出了一种针对链路相关性感知协议的欺骗攻击。在数据包的传输过程中，源节点周期性地发送 beacon 包给邻居一跳节点，对应的每一个接收节点维持一个数据包接收位图，用来记录数据包的接收情况；然后接收节点将该数据包接收位图发送给源节点，在收到数据包接收位图之后，源节点根据其中的数据计算邻居链路对之间的相关性，从而选择相应的下一跳候选节点。在此过程中，恶意节点会篡改自身维持的数据包接收位图中的数据，使源节点计算得出错误的相关性度量，从而达到影响协议性能的目的。此外，针对这一链路相关性欺骗攻击，本文提出了基于 Watchdog[6,15-16]机制的恶意节点检测方法。这一检测方法要求在每一个节点上嵌入 Watchdog 模块，在源节点发送 beacon 包之后，源节点上的 Watchdog 模块对邻居节点的转发行为进行监听，然后记录监听结果并将其反馈给源节点。源节点将对比此记录与邻居节点反馈的数据包接收位图，从而得出正确的数据包接收位图。

本文第 2 节引入链路相关性度量的计算；第 3 节提出针对链路相关性感知协议的欺骗攻击；第 4 节提出基于 Watchdog 机制的检测方法；第 5 节通过仿真实验证明本文提出的针对链路相关性欺骗攻击与基于 Watchdog 机制的检测算法的可行性与有效性；最后总结全文。

2　链路相关性度量

链路相关性感知的网络协议大都是基于 beacon 包的数据包接收位图对链路相关性度量进行计算。本文首先通过一个简单的例子来阐述链路相关性的测量过程。

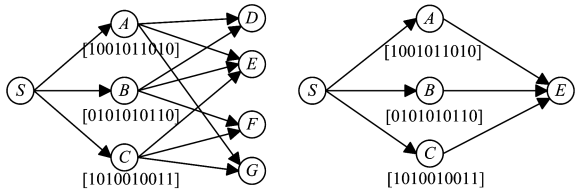

图 1　网络拓扑结构

Fig. 1　Network topology

图 1(a)给出了一个简单的广播拓扑结构，其中，节点 S 是源节点，而节点 A、节点 B 和节点 C 是对应的接收节点。基于 beacon 包的邻居节点之间的链路相关性的测量工作如下：首先，拓扑中的节点 S 周期性地向其邻居节点 A、节点 B 和节点 C 传输 beacon 信息，节点 A、节点 B 和节点 C 维持一个数据包接收位图，并将其用来记录相应数据包的接收情况；然后，在 beacon 包发送结束后，节点 A、节点 B 和节点 C 将记录的数据包接收位图返回给节点 S，当 S 接收到这些数据包接收位图后，它可以据此计算其邻居节点之间的数据包接收相关性。

1）条件数据包接收概率（Conditional Packet Reception Probability，CPRP）

CPRP 指在发送节点 S 发送数据包且节点 B 接收到节点 S 发送的数据包的情况下，节点 A 也接收到该数据包的条件概率，如式(1)所示：

$$C_{A,B}^{S}=\frac{\sum_{i=1}^{w}(b_A[i]\&b_B[i])}{\sum_{i=1}^{w}b_B[i]} \tag{1}$$

其中，w 是数据包接收位图的长度，$b[i]$ 表示数据包接收位图的第 i 位，$b[i]=1$ 表示数据包接收成功，而 $b[i]=0$ 表示对应的数据包接收失败。图 1(a)中，链路 $e\langle S,A\rangle$ 和 $e\langle S,B\rangle$ 的数据包接收位图分别是“1001011010”和“0101010110”。由式(1)可知 $C_{A,B}^{S}=\frac{3}{5}$，也就是说在节点 B 接收到节点 S 发送的数据包时，节点 A 也接收到该包的概率为 $\frac{3}{5}$。

2）集合条件数据包接收概率

一般情况下，网络中的发送节点不可能只有两个邻居节

点，因此假设源节点 S 向非空邻居节点子集 $Y(S)$ 和邻居节点 $R(R\notin Y(S))$ 传输一个数据包，$P(Y(S))$ 为 $Y(S)$ 中的所有节点都成功接收一个数据包的概率。那么集合条件数据包接收概率表示在集合 $Y(S)$ 中的所有节点都收到 S 发送的数据包的条件下，节点 R 也收到该包的条件概率，如式(2)所示：

$$P(R|Y(S))=\frac{P(R\cap Y(S))}{P(Y(S))} \tag{2}$$

其中，$P(Y_k(S))=\frac{\sum_{i}^{w} b_{R_1}(i)\&b_{R_2}(i)\&\cdots\&b_{R_k}(i)}{w}$，$k$ 为集合 $Y(S)$ 中节点的数量。由式(2)可知，在图 1(a)的网络拓扑中，在集合 $\{A,B\}$ 接收到节点 S 发送的数据包的条件下，节点 C 也能接收到该包的概率为 $\frac{2}{3}$，即集合 $\{A,B\}$ 与节点 C 之间的链路相关性值为 $\frac{2}{3}$。

3 链路相关性欺骗攻击

第 2 节指明了现有的链路相关性感知协议都是基于接收节点反馈给发送节点的数据包接收位图来对链路相关性值进行衡量的。由式(1)和式(2)可知，一旦数据包接收位图中的数据不准确，邻居节点之间链路相关性的值就会是错误的，从而影响下一跳候选节点的选择，对协议的性能产生影响。因此，基于无线网络存在的安全问题，网络中的一些不协作节点就会利用上述缺陷对数据包位图中的数据进行篡改，从而对链路相关性感知协议的性能产生攻击。

本节提出针对链路相关性感知协议的欺骗攻击机制。该攻击方法中的恶意节点在将自己的数据包接收位图发送给源节点之前对其中的数据进行了篡改，从而实现对源节点的邻居链路对之间的相关性计算结果进行干扰欺骗。

3.1 攻击方法

本节首先通过一个简单的例子来解释链路相关性欺骗攻击方法在广播和机会路由协议中的实现原理。在图 1(a)和图 1(b)所示的两个通信场景中，假设到达目的节点 D、节点 E、节点 F 和节点 G 的链路投递率均为 1。首先我们考虑在不存在恶意节点的网络环境下，节点 S 成功发送一个数据包来覆盖两个节点所需的期望传输次数 E 为：

$$E=\sum_{i=1}^{2}\frac{1}{p(e_i)}-\frac{1}{1-p(\overline{e_1}\cap\overline{e_2})} \tag{3}$$

源节点 S 发送的一个数据包至少成功覆盖一个节点的期望传输次数 E 的计算公式如下：

$$E=\frac{1}{1-p(\overline{e_1}\cap\overline{e_2})} \tag{4}$$

其中，$p(e_1)$ 和 $p(e_2)$ 分别表示节点 S 到节点 A 和节点 B 的链路质量，而 $p(\overline{e_1}\cap\overline{e_2})$ 表示节点 A 和节点 B 均没有接收到节点 S 广播的数据包的概率。

在图 1(a)的广播场景中，节点 S 只需要在 A，B 和 C 3 个节点中任意选择两个作为最小的支配节点集合就能覆盖网络中的所有节点。由式(3)可知，节点 S 发送的数据包成功覆盖节点 A 和节点 B 所需的期望传输次数是 2.57，覆盖节点 B 和节点 C 的期望传输次数是 2.75，而覆盖节点 A 和节点 C 的期望传输次数是 2.57。因此，源节点 S 会选择节点集合 $\{A,B\}$ 或者 $\{A,C\}$ 作为支配节点集合。在图 1(b)的机会路由场景中，假设候选节点的数量为 2，其中，源节点为 S，目的节点为 E。由图 1(b)可知，链路 $e\langle S,A\rangle$，$e\langle S,B\rangle$，$e\langle S,C\rangle$ 的链路质量都是 0.5，由式(4)可知节点 A 和节点 B 至少有一个能成功接收到该包的期望传输次数是 1.43，同样可以计算出节点 B 和节点 C 至少有一个节点能够成功接收到该包的期望传输次数是 1.25，而节点 A 和节点 C 的期望传输次数是 1.43。因此，节点 S 会选择节点 B 和节点 C 作为其下一跳候选节点进行数据包转发。

但是，由于其自身移动性、发放性以及传输信号的不稳定性等特点，无线网络面临着各种威胁和网络攻击。在图 1(a)和图 1(b)的拓扑结构中，节点 C 出于某些自私的原因，在将数据包接收位图发送给节点 S 前，会恶意篡改其中的数据为“0101011100”，当节点 S 接收到虚假的数据包位图之后，对邻居节点的链路相关性以及期望传输次数进行计算。此时，在图 1(a)中，$E^{S}_{B,C}$ 为 2.33，小于节点 S 成功传输一个数据包覆盖节点 $\{A,B\}$ 或者 $\{A,C\}$ 所需的期望传输次数 2.57。因此，节点会选择节点 B 和节点 C 作为下一跳候选节点。节点 S 成功广播一个数据包所需的期望传输次数 E_{Attack} 等于 2.75，则链路相关性欺骗攻击的攻击效果 $\bar{d}$ 为：

$$\bar{d}=E_{\text{Attack}}-E \tag{5}$$

图 1(a)的广播场景中的攻击效果 $\bar{d}$ 为 0.42。同样，在图 1(b)的机会路由中，由式(5)根据虚假的数据包接收位图计算可知，节点 S 会选择集合 $\{A,B\}$ 作为候选节点，攻击效果为 0.42 次。显然，恶意节点对自身数据包接收位图的恶意篡改会增加链路相关性感知协议的数据包重传次数，从而降低算法的传输效率。

现实中的网络拓扑不可能如图 1 所示的拓扑结构简单，网络中可能有 $M(M\geqslant 3)$ 个节点，并且在数据包的每一跳传输过程中都可能遇到一个甚至不止一个恶意节点，因此本文提出了针对链路相关性感知协议的欺骗攻击方法。在数据包的每一跳传输中，当源节点周期性地发送 beacon 包之后，恶意节点攻击自身维持的数据包接收位图中的数据，然后将篡改后的数据包接收位图发送给源节点。因此，源节点就会根据错误的数据包接收位图计算得出错误的邻居节点之间的链路相关性度量值，从而选择错误的节点作为下一跳传输节点，进而对相应的算法协议的性能和效率产生影响。

3.2 实现细节

在针对链路相关性感知的协议中，源节点周期性地发送 beacon 包，邻居节点通过记录数据包接收位图的方式记录自己的收包情况，然后将数据包接收位图返回给源节点。此时，链路相关性欺骗攻击下的恶意节点会对自己的数据包接收位图中的数据进行篡改，攻击方式包含如下两种：

1)恶意节点只对链路相关性进行欺骗。网络中的恶意节点在篡改数据包接收位图中的数据时，只篡改位图中“1”的位置而不改变其数量，从而保证链路质量的真实性。例如 3.1 节中讨论的例子，恶意节点 C 在保证链路 $e\langle S,C\rangle$ 的链路质量

不变的情况下对数据包位图进行篡改。算法 1 是该攻击方法中恶意节点的攻击过程。

算法 1 描述了恶意节点对数据包接收位图中的数据进行链路相关性欺骗攻击的过程。第 1－7 行获取数据包位图的长度以及接收到的数据包的数量。第 8－9 行定义两个变量，将其分别用来生成和存储数据包接收位图的下标。第 10－23 行表示恶意节点在不改变自己链路质量的前提下篡改自己的数据包接收位图，并将篡改后的数据包接收位图传输给发送节点。

算法 1　链路相关性的欺骗攻击

```
INPUT:B
1. W←B. length; //计算数据包接收位图的长度
2. count←0;
3. for i=1 to W do //计算数据包接收位图中 1 的数量,用 count 表示
4.     if B[i]==1 then
5.         count ++;
6.     end if
7. end for
8. Random R=new Random(); //定义一个随机变量用于生成位图下标
9. ArrayList<Integer> list=new ArrayList<>(); //定义一个列表用于存储已生成的位图下标
10. for i=1 to W do
11.     idex←R. getRandomNumber(w); //随机生成一个值,用来表示数据包接收位图的下标
12.     whilelist. Contains(idex) do
13.         idex←R. getRandomNumber(w);
14.     end while
15.     list. add(idex);
16.     if count>0 then //在不改变 1 的数量的情况下修改数据包接收位图
17.         B[idex]←1;
18.         count --;
19.     else do
20.         B[idex]←0;
21.     end if
22. end for
23. Return B
```

2)随机链路相关性欺骗。网络中的恶意节点对自身维持的数据包接收位图中的数据进行随机篡改，其中“1”和“0”的比例是随机变化的，即对应链路的链路质量也是随机变化的。然后，恶意节点将篡改后的数据包接收位图返回给源节点进行计算。

4　基于 Watchdog 的恶意节点检测机制

第 3 节提出的针对链路相关性感知协议的欺骗性攻击属于网络的内部攻击。恶意节点不需要知道网络拓扑中其他节点的数据包接收位图，仅仅在将自己的数据包接收位图返回给源节点之前对其中的数据进行篡改，即可改变邻居节点间链路相关性度量的准确值。而现有的链路相关性的感知协议大都是基于节点的数据包接收位图来计算邻居链路之间的相关性以及其他用来选择候选节点的参数，这些协议并没有考虑数据包接收位图中数据的真实性与准确性。为了进一步保证相关性感知协议的性能与效率，我们需要在计算基于节点的数据包接收位图时考虑其数据的真实性，因此，本文提出了针对链路相关性欺骗攻击的基于 Watchdog 的恶意节点检测机制。

4.1　检测方法

Watchdog 是无线网络中抵御内部攻击的基础安全机制，其具体过程是：当节点 S 发送了一个数据包给其邻居节点 T 之后，S 节点上的 Watchdog 系统就会检测节点 T 是否对数据包进行了转发。Watchdog 机制利用通信协议对通信范围内节点发出的数据包进行侦听，从而判断节点的行为。

由上文可知，邻居节点的数据包位图是根据源节点周期性广播的 beacon 包的接收情况生成的。在本文的检测算法的设计中，每一个节点周期性地进行两跳广播 beacon 包，其一跳邻居节点维持一个数据包接收位图用于记录固定数量的数据包的接收状态，并将该包转发给下一跳邻居节点。通过分析可知，我们只需要通过监听每一个节点是否存在转发行为来判断对应位置的数据包接收位图上的数据是否正确。因此，本文提出的检测方法是为每一个节点安装 Watchdog 监控系统并且自身维持一张用于记录邻居节点转发的记录表，后文称该表为转发记录表。在数据包的每一跳传输中，在源节点发送数据包后，我们使用 Watchdog 机制对其一跳邻居节点的行为进行监听，即判断是否存在数据包转发的情况，并将结果记录在对应的转发记录表中。例如，在图 1(a)中，当节点 S 发送了一个数据包给它的邻居节点 A 后，节点 S 上的 Watchdog 监控系统就会通过监听来检测节点 A 是否对该数据包进行了转发。随后，该 Watchdog 系统将监听到的邻居节点的数据包转发情况反馈给节点 S，并且对应地记录在转发记录表上，用“1”表示对应邻居节点的数据包转发，用“0”表示该邻居节点并无转发行为。然后，在每次接收到邻居节点反馈的数据包接收位图时，节点 S 根据自身存储的转发记录表与数据包接收位图对其进行比对，以确定真实的邻居节点的数据包接收情况，从而计算得出准确的邻居节点之间的链路相关性。例如，在图 1(a)中，在节点 S 发送数据包后，节点 A 返回给节点 S 的数据包接收位图为“1100”，而节点 S 上的 Watchdog 机制在监听节点 A 的行为后将反馈记录在转发记录表上，对应的存储条目为“1001”，因此，我们可以得出对于节点 S 发送的数据包，节点 A 的正确的数据包接收位图为“1001”。图 2 为该检测算法的工作原理图。

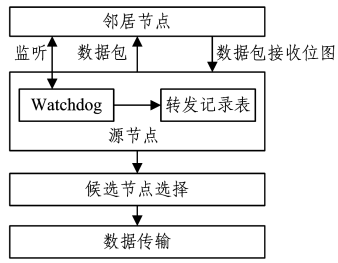

图 2　基于 Watchdog 的恶意节点检测机制的工作原理

Fig. 2　Working principle of malicious node detection mechanism based on Watchdog

4.2 实现细节

算法 2 描述了基于 Watchdog 机制的检测算法的工作过程。第 1—13 行,在接收节点使用数据包接收位图来记录数据包接收状态时,使用安装在发送节点上的 Watchdog 机制对每一个数据包是否被转发的状态进行监听,然后使用转发行为记录表来记录接收节点的转发行为状态。然后,节点 S 根据转发行为记录表与其收到的邻居节点返回的数据包接收位图之间的对比来判断是否存在链路相关性欺骗攻击,得出正确的数据包接收位图后再进行参数计算,并选择合适的候选节点进行网络数据传输。

算法 2 基于 Watchdog 机制的检测算法

```
1. keep the watchdog on;
2. while Sender send n packets to R do
3.    for i=1 to n do
4.       if R receives the packet then
5.          B[i]=1;
6.          forward it to next-hop;
7.          FRT[i]=1;
8.       else do
9.          B[i]=0;
10.         FRT[i]=0;
11.      end if
12.   end for
13. end while
14. keep off the watchdog;
15. Return B
```

5 仿真实验与结果分析

本节通过仿真实验对我们提出的链路相关性欺骗攻击机制以及基于 Watchdog 的恶意节点检测机制进行性能分析。下面介绍实验环境和参数设置,然后对实验数据进行分析。

我们在仿真实验平台上实现了链路相关性感知的多点中继器算法(CMPR),在该算法中嵌入本文提出的链路相关性欺骗攻击与基于 Watchdog 的检测机制,并设计了一系列的仿真实验。其中,Att-CMPR 算法表示链路质量不变的相关性欺骗攻击算法,RAtt-CMPR 算法指恶意调节数据包接收位图中“1”的比例的相关性欺骗攻击算法。我们在面积为 750 m * 750 m 的正方形区域内随机布置了 64 个节点,通信半径定义为 160m。如果任意两节点之间的距离小于通信半径,则它们互相为彼此的一跳邻居。因为在仿真实验平台中,我们不可能给每一条链路设置一个链路质量,所以本文仿真采用可控的方式[17-18]设置链路质量,并通过向每一个节点引入数据包相关丢失模型使其一跳邻居节点以一个可控的丢失率进行数据包丢失。表 1 列出了本文仿真实验中所用到的参数设置。

表 1 实验参数设置

Table 1 Experimental parameters setting

参数名称	参数值
物理区域/m^2	750 * 750
节点数	64
通信半径/m	160
攻击节点数	5
网络节点密度	6.6

5.1 链路相关性欺骗攻击的攻击效果

为了对链路相关性欺骗攻击算法的性能进行分析,本文的仿真实验在网络拓扑中随机选择 5 个恶意节点,在 CMPR 算法运行时分别对数据包接收位图进行固定链路质量以及调节“1”的比例为 0.5 的篡改攻击,并记录 10 个不同时刻下运行该算法传输数据包所需的期望传输次数。图 3 对比了两组链路相关性欺骗攻击的结果与没有恶意节点存在时的 CMPR 算法的期望传输次数,横坐标表示 10 个不同的时刻。

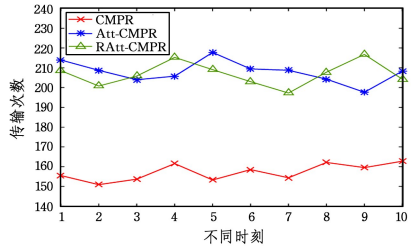

图 3 攻击效果对比

Fig. 3 Comparison of attack effects

从图 3 可以看出,在不同时刻,Att-CMPR 算法以及 RAtt-CMPR 算法传输一个数据包所需的期望传输次数都明显大于网络友好情况下的 CMPR 算法。此外,在不同时刻,Att-CMPR 算法与 RAtt-CMPR 算法传输一个数据包所需要的期望传输次数大致相同。因此,图 3 中的结果表明,本文提出的两种链路相关性欺骗攻击方法的攻击效果相似,都明显增加了链路相关性感知协议传输数据包所需的期望传输次数,降低了协议的传输效率。

5.2 不同的恶意节点比例对攻击效果的影响

在本文的仿真环境下,我们还考虑了网络中不同的恶意节点比例对链路相关性欺骗攻击效果的影响。本文通过固定节点拓扑结构来改变网络中恶意节点的数量,从而改变恶意节点的比例。图 4 给出了同一环境的网络拓扑中存在不同数量的恶意节点时所需的期望传输次数。

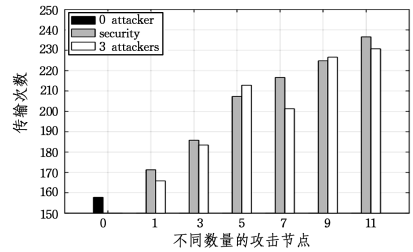

图 4 不同数量的攻击节点的效果对比

Fig. 4 Comparison of effects of different number of attack nodes

从图 4 可以看出,随着网络中恶意节点数量的增加,链路相关性欺骗攻击下的 CMPR 算法传输数据包所需的期望传输次数也增加。例如,当网络中不存在恶意节点时,CMPR 算法所需的期望传输次数最小为 157;而在同样的网络环境下,存在 11 个恶意节点时 CMPR 算法所需的期望传输次数为 236。这是因为随着网络中恶意节点比例的增大(即同一网络环境下恶意节点数的增加),被篡改的数据包接收位图的数量就会增多,因此对候选节点的选择的影响就会越大。这表明,随着网络中恶意节点比例的增加,传输数据包所需的重

传次数越多,链路相关性欺骗攻击算法的攻击效果就越明显。

5.3　不同节点度对攻击效果的影响

本文还考虑在固定的攻击节点比例下,不同密度的网络环境对攻击效果的影响。本次实验依旧是在上述仿真环境下进行的,只是通过随机改变拓扑中节点的坐标位置生成不同密度的网络拓扑。本文的网络节点密度指网络中所有节点的邻居节点数之和与总节点数之比,下文简称节点度。

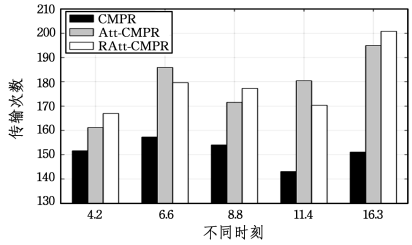

图 5　不同节点度对攻击效果的影响

Fig. 5　Influence of different node degree on attack effects

从图 5 可以看出,随着网络中节点度的增加,链路相关性欺骗攻击的攻击效果并不是单调递增的。这是因为随着节点度的增加,网络中节点的邻居节点数也在增加,因此传输一个数据包需要的期望传输次数也随之增加。此时,当攻击节点比例固定时,数据包位图的篡改会影响更多的邻居节点,但是同时,网络中的转发节点数会相应减少,因此被攻击到的转发节点的数量也会下降。

5.4　不同“1”的比例对攻击效果的影响

表 2 列出了在固定的攻击节点比例以及固定的网络节点度下,篡改的数据包接收位图中“1”的不同比例对链路相关性欺骗攻击效果的影响结果,其中,CMPR 算法的期望传输次数是 157,而固定链路质量的欺骗攻击的 CMPR 算法的期望传输次数是 195。

表 2　位图中“1”的不同比例对攻击效果的影响

Table 2　Influence of different ratio of “1” on attack effects

数据包接收位图中“1”的比例	0.1	0.3	0.5	0.7	0.9
期望传输次数	174	186	191	201	189

从表 2 可以看出,随着数据包接收位图中“1”的比例的增加,该算法的期望传输次数并不是单调增加的。因为当“1”的比例被恶意提高后,链路质量差的链路被选择作为候选节点的概率就会提高,因此传输一个数据包所需要的期望传输次数就会增加。但是,此时由于网络中节点的链路质量越高,所需要的转发节点数量就会相应减少,因此传输一个数据包所需的期望传输次数就相应减少。

5.5　检测算法的效果

针对链路相关性欺骗攻击,我们提出了基于 Watchdog 机制的检测算法,用于监听下一跳邻居节点的转发行为,从而得出正确的数据包接收位图。图 6 将其与同一拓扑下不存在攻击节点与存在 3 个攻击节点的 CMPR 算法的期望传输次数进行对比,其中,security 表示嵌入本文提出的检测机制的 CMPR 算法。由图 6 可知,security 算法的期望传输次数明显小于存在恶意节点时 CMPR 算法的期望传输次数,而趋近于不存在恶意节点时 CMPR 算法的期望传输次数。因此,图 6 的结果表明,嵌入检测算法的 CMPR 算法的期望传输次数趋近于真实值。这是因为,在嵌入检测机制的 CMPR 算法中,源节点利用安装在自身的 Watchdog 系统对邻居节点的数据包转发情况进行监听,然后通过自身维持的邻居节点的转发记录表计算得出正确的链路相关性度量,从而选择正确的候选节点。分析结果表明,本文提出的基于 Watchdog 的恶意节点检测机制针对网络中链路相关性欺骗攻击存在明显的保护效果。

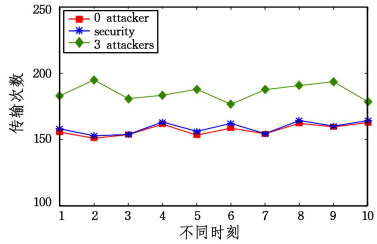

图 6　检测效果

Fig. 6　Detection effects

5.6　不同机制下的能源消耗

本次仿真是为了比较不同状态下的 CMPR 算法的能量消耗情况。在上述仿真环境下,我们使用一阶无线电能量消耗模型[19]并设置数据包的传输功率为 0.2 W,节点的初始能量为 6 J,仿真结果如图 7 所示。

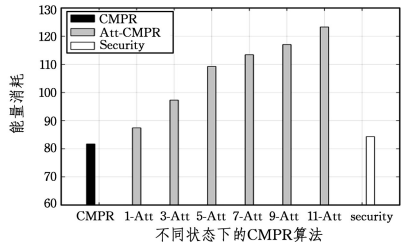

图 7　不同状态下的 CMPR 算法的能量消耗

Fig. 7　Energy consumption of CMPR algorithm in different states

由图 7 可以看出,随着恶意节点数的增加,平均能量消耗也在增加。因为恶意节点数越多,对应算法的重传次数也就越多,因此消耗的能量也会增加。我们以存在 5 个恶意节点的 Att-CMPR 算法(5-Att)为例,从图 7 中可以看出,没有恶意节点存在时的 CMPR 算法的平均能量消耗为 81.69 J,5-Att 算法的能源消耗为 109.27 J,能源消耗增加了 33.76%。这是因为恶意节点的存在会增加数据包重传次数,从而导致能量增加。而 security 算法的平均能源消耗为 84.29 J,比 CMPR 算法增加了 3.18%的能源消耗,这是因为我们的检测机制利用 Watchdog 在源节点周期性发送 beacon 包时对网络进行监听时存在能量消耗。而相对于 5-Att 算法,security 节省了 22.86%的能源消耗,因为本文的检测机制在检测出恶意节点的同时能够得到真正的数据包接收位图,从而减少数据包的重传次数。

结束语　本文提出了针对基于数据包接收位图的链路相关性感知协议的链路相关性欺骗攻击方法。恶意节点通过对

数据包接收位图中的数据在保证链路质量不变的前提下进行篡改达到对源节点的邻居节点之间的相关性进行欺骗攻击的目的。针对这一攻击算法,本文还设计并提出了基于 Watchdog 机制的恶意节点检测机制,利用节点的转发行为得出真实的数据包接收位图。仿真实验的结果表明了链路相关性欺骗攻击算法的有效性以及基于 Watchdog 的恶意节点检测机制对链路相关性欺骗攻击算法的保护效果。

参 考 文 献

[1] SONG M K,WANG S,HE T. Exploiting causes and effects of wireless link correlation for better performance [C]// Computer Communications. IEEE,2015:379-387.

[2] WANG S,KIM S M,LIU Y H,et al. CorLayer:A transparent link correlation layer for energy efficient broadcast [J]. In MobiCom,2013,23(6):1970-1983.

[3] SINGH G. A Survey of Multicast Routing Protocols in MANETS[C]// International Conference on Futuristic Trends in Engineering & Management. 2014.

[4] WANG S,BASALAMAH A,SONG M K,et al. Link-Correlation-Aware Opportunistic Routing in Wireless Networks [J]. IEEE Transactions on Wireless Communications,2015,14(1):47-56.

[5] WANG H,LIU Y,XU S. An Opportunistic Routing Protocol Based on Link Correlation for Wireless Mesh Networks [M]// Wireless Communications, Networking and Applications. Springer India,2016.

[6] SALEHI M,BOUKERCHE A,DAREHSHOORZADEH A. Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks [J]. Ad Hoc Networks,2016,50(C):88-101.

[7] LI L,RAMJEE R,BUDDHIKOT M,et al. Network Coding-Based Broadcast in Mobile Ad-hoc Networks[J]. Proceedings - IEEE INFOCOM,2007,5(8):1739-1747.

[8] WANG S,KIM S M,YIN Z,et al. Encode When Necessary:Correlated Network Coding Under Unreliable Wireless Links [J]. Acm Transactions on Sensor Networks,2017,13(1):1-22.

[9] ZHU T,ZHONG Z,HE T,et al. Exploring link correlation for efficient flooding in wireless sensor networks[C]// Proceedings of the First USENIX/ACM Symposium on Network Systems Design and Implementation (NSDI). 2010.

[10] WANG S,BASALAMAH A,SONG M K,et al. A Unified Metric for Correlated Diversity in Wireless Networks [J]. IEEE Transactions on Wireless Communications,2016,15(9):6215-6227.

[11] SRINIVASAN K,JAIN M,CHOI J I,et al. The κ-factor:Inferring protocol performance using inter-link reception correlation [C]// Proceedings of ACM MOBICOM. 2010.

[12] ZHAO Z,DONG W,BU J,et al. Exploiting link correlation for core-based dissemination in wireless sensor networks [C]// Eleventh IEEE International Conference on Sensing,Communication,and Networking. IEEE,2014:372-380.

[13] TIAN B. Attack Detection and Defense Technologies in Wireless Sensor Networks[D]. Beijing:Beijing University of Posts and Telecommunications,2012. (in Chinese)
田斌. 无线传感器网络中攻击检测和防御技术研究[D]. 北京:北京邮电大学,2012.

[14] CHO Y,QU G. Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs [J]. International Journal of Distributed Sensor Networks,2013,2013(3):264-273.

[15] BORA S,SINGH S,MOHAMAD A S,et al. Watchdog:A Study on Examining and Eliminating Misbehaviour[J]. International Journal of Computer Applications,2014,87(3):1-3.

[16] AGRAWAL S,JAIN S,SHARMA S. A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks [J]. 2011,4(1):41-48.

[17] MACKE J H,BERENS P,ECKER A S,et al. Generating spike trains with specified correlation coefficients [J]. Neural Computation,2009,21(2):397-423.

[18] HIGHAM N J. Computing the near est correlation matrix—a problem from finance [J]. Ima Journal of Numerical Analysis,2002,22(3):329-343.

[19] HEINZELMAN W B,CHANDRAKASAN A P,BALAKRISHNAN H. An Application Specific Protocol Architecture for Wireless Microsensor Networks[C]// IEEE Transactions on Wireless Communication. 2002:660-670.

(上接第 97 页)

[22] WAN Z G,DENG R H. VPSearch:Achieving Verifiability for Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data[J]. IEEE Transactions on Dependable & Secure Computing,2016,PP(99):1-1.

[23] ZHU X Y,HAO R P,JIANG S R,et al. Verification of Boolean Queries over OutsourcedEncrypted Data Based on Counting Bloom Filter[C]// IEEE Global Communications Conference. 2015:1-6.

[24] SUN W H,LIU X F,LOU W J,et al. Catch You If You Lie to Me:Efficient Verifiable Conjunctive Keyword Search over Large Dynamic Encrypted Cloud Data[C]// IEEE Conference on Computer Communications. 2015:2110-2118.

[25] JIANG S R,ZHU X Y,GUO L K,et al. Publicly Verifiable Boolean Query Over Outsourced Encrypted Data[C]// IEEE Global Communications Conference. 2016:1-6.

[26] PALLIPAMU V,REDDY K,VARMA P. ASH-160:A novel algorithm for secure hashing using geometric concepts [J]. Journal of Information Security and Applications,2014,21:52-63.

[27] LICHMAN M. UCI Machine Learning Repository [OL]. http://archive.ics.uci.edu/ml.