(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102111323 A
(43)申请公布日 2011.06.29

(21)申请号 200910244243.9

(22)申请日 2009.12.28

(71)申请人 北京安码科技有限公司
地址 100876 北京市海淀区学院南路 34 号

(72)发明人 白媛 辛阳 罗守山 包一兵

(51)Int.Cl.
H04L 12/56(2006.01)

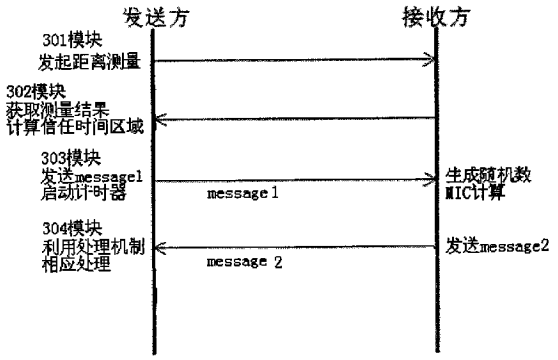
权利要求书 1 页 说明书 5 页 附图 2 页

(54)发明名称

一种 UWB 避免拒绝服务攻击的方法

(57)摘要

本发明公开了一种避免拒绝服务攻击的方法。在使用 ECMA-368 协议的 UWB 网络中存在着引发拒绝服务攻击的潜在威胁，本发明通过距离测量和时间计时的方式对正常报文和攻击报文进行区分，避免了 UWB 网络遭遇拒绝服务攻击。



CN 102111323 A

1. 一种避免拒绝服务攻击的方法，其特征在于，该方法包括：

报文传输之前，对距离进行测定，估计正常报文到来时间，报文传输之后，对事件进行计时，根据报文返回时间确定不同的操作；

其中距离测定方法具体为：启动系统自带的距离测量功能；根据测量往返时间计算距离。

根据距离测量结果设定信任区间的方法具体包括：根据报文到来时间设定四个信任区间，分别为丢弃、保存、处理和等待，落入不同信任区间的报文分别按如下方法处理：

当报文到来过早，落入丢弃信任区间的时候，认为是可疑报文，将其丢弃。

当报文落入保存的信任区间时用堆栈保存落入该区间报文，以便以后处理。

在处理阶段的收到报文送入队列中，依次处理。

在等待阶段收到的报文会被处理，等待间歇会处理保存阶段保存的报文。

一种 UWB 避免拒绝服务攻击的方法

技术领域

[0001] 本发明涉及网络通信技术，特别涉及一种保证 UWB 无线网络安全的方法。

背景技术

[0002] UWB(Ultra WideBand) 是超宽带无线通信技术的缩写。是一种使用 1GHz 以上带宽的最先进的无线通信技术，其通信速度可以达到几百 Mbit/ 秒。由于其广阔的应用前景，围绕 UWB 的标准之争从一开始就十分激烈，甚至致力于制订其标准的 IEEE 802.15.4TG3a 工作组解散。WiMedia 05 年开始与 ECMAInternational 合作，并推出了 ECMA-368 和 ECMA-369 标准。前者定义了分布式 UWB 系统的 PHY 和 MAC 层，后者则定义了 MAC-PHY 接口。上述标准于 06 年 6 月提交 ISO 讨论通过并形成 ISO_IEC_26907 和 ISO_IEC_26908 标准，成为事实上的国际行业标准。

[0003] 上述 ISO_IEC_26907 标准定义了一个完全分布式的 UWB 系统，每一个设备都是独立和对等的，没有一个中心协调器。UWB 的这种网络结构给网络安全提出很大的挑战。标准定义了相应的安全机制，提供两个安全级别 ：非安全和强安全 ；定义 3 个安全模式来控制安全级别 ；定义 4-way 握手机制进行安全信任关系的建立以及密钥生成和分发。提供的安全保护包括数据加密、消息完整性校验和重放攻击避免等。在数据加密方面，使用在 4-way 握手过程中生成的 PTK(Pair-wise Temporal Key) 对单播数据进行加密，并在已有 PTK 的基础上进行 GTK(Group Temporal Key) 请求和分发，用以对广播和组播数据进行加密。4-way 握手过程生成的 PTK 是整个上述 UWB 系统安全的基础。在两个 UWB 设备需要进行安全模式通信之前，双方需要相互认证，确认对方可靠，建立起一种安全关系之后再进行安全帧的传输。4-way 握手机制就可以实现上述功能。

[0004] 4-way 握手可以完成两个作用。一个是双方相互认证、鉴定，建立起一种安全关系 ；另外一个就是通过 4-way 握手双方生成一个对称临时密钥 PTK(Pair-wise Temporal Key)，通过 PTK，双方对传输的安全帧进行加密和解密。

[0005] 两个设备可以通过 4-way 握手实现认证和鉴定的基础是这两个设备持有相同的主密钥 (master key)。而这个主密钥的生成、派发是上一层完成的，我们假定其具有权威性。

[0006] 两个设备中发起 4-way 握手请求的设备被称为发送设备，接受握手请求的设备被称为接收设备。在整个 4-way 握手过程中双方共往来传输 4 个报文 (message)。正常的 4-way 握手过程简单描述如下 ：

[0007] (1) 发送设备构建、发起 message1。

[0008] 发送设备构建 message1。message1 中包括双方共享的主密钥的标志符 MKID，发送设备选取的用于生成 PTK 的标志符 PTKID，128 位随机数 I-Nonce，PTK MIC 内容为 0，表示无意义。发送设备发送 message1。

[0009] (2) 接收设备接收 message1，发送 message2。

[0010] 接收设备接收到 message1 之后，检查其合法性，验证 PTKID 是否具有唯一性。如

果不唯一通过在 message2 中设置 Status Code 位通知发送设备重新发送 message1。

[0011] 接收设备通过 MKID 获得 master key，结合其他信息进行 PTK MIC 计算，将算得的 PTK MIC 值放在 message2 中。具体计算过程和细节由于和我们的发明无关，在这里不详细描述了。

[0012] Message2 中除了状态码，MIC 值，以及与 message1 中相同的 MKID 和 PTKID 以外，还有取代 I-Nonce，message2 中相应位置为接收设备生成的随机数 R-Nonce。

[0013] (3) 发送设备接收到 message2，发送 message3。

[0014] 发送设备接收到 message2 之后，进行 MIC 计算，MIC 比较以及对状态码的检测。正常情况下，发送设备在接收到 message2 以后完成对接收设备的验证。进行新的 MIC 计算之后，重新组建 message3，发送给接收设备。

[0015] (4) 接收设备接收 message3，发送 message4。

[0016] 接收设备接收到 message3 以后，进行 MIC 计算，比较之后，如果接收设备计算的 MIC 值和发送设备发送来的 message3 中的 MIC 值相同，完成接收设备对发送设备的验证。接收设备组建 message4，同时生成 PTK。

[0017] (5) 发送设备接收 message4。

[0018] 发送设备接收 message4 以后，进行 MIC 验证之后，生成 PTK。4-way 握手结束。

[0019] 4-way 握手过程用图 1 描述。

[0020] 对于一个无线系统，黑客很容易就可以截获信息，即使这个信息不是发给该设备的。黑客截获 Message1 之后，从中可以获取有用的信息。由于标准的开放性，可以想见黑客很容易了解 4-way 握手的完整过程和 message 的格式。所以黑客完全可以在截获一个 message1 之后，立刻伪造一个 message1，发给接收设备，接收设备检验 message1 失效以后，结束握手过程，从而剥夺了正常设备发起握手请求的权利。这种攻击对于攻击者而言成本很低，而造成的危害却很大，是亟待解决的问题。

[0021] 在原 4-way 握手机制中没有考虑 DoS 攻击的问题，原 4-way 握手过程的设计都是基于系统正常的假定之下产生的。原设计中考虑到了一些例如帧丢失，传输错等系统常见问题的规避和修复技术。但是没有考虑到恶意攻击的问题，或者说对 DoS 攻击的问题考虑得不全面。

[0022] 当系统中都是正常设备的时候，4-way 握手机制是行之有效的。但对于一个开放的、分布式的网络而言，恶意设备、恶意行为是一定会存在的。尽管这部分是少数，但由于黑客的主动攻击性，对其他设备甚至整个系统造成的危害却是巨大的。黑客会研究标准的细节，发现其漏洞，伺机而动，一旦发现机会，会不断地发起攻击。

[0023] 在 UWB 网络中各节点完全对等，也就是发送设备和接收设备完全对等。因此其 4-way 握手的设计就要考虑到这点。当发送设备发送 message1 之后，等待接收 message2，收到 message2 之后，进行 MIC 验证。如果 MIC 验证无效，发送设备认为接收设备不可信，中止 4-way 握手过程。这为黑客提供了一种攻击的机会，黑客在截获 message1 之后，立刻伪造一个 message2 发给发送设备，发送设备无法识别，认为接收设备不可靠，造成正常 4-way 握手过程中止。把这种攻击命名为抢占式拒绝服务攻击。

[0024] 首先考察一下这种攻击实施的可能性。

[0025] (1) 报文被伪造的可能性

[0026] 表 1 为 PTK Command 载荷部分，四个 messages 都按下面方式组建。

[0027] 表 1PTK Command 载荷部分

[0028]

Octets:1	1	3	11	16	16	8
Message Number	Status Code	PTKID	Reserved	MKID	I-Nonce/ R-Nonce	PTK MIC

[0029] 从上表可以看出，黑客在截获 message1 之后，获取 PTKID 和 MKID 之后很容易伪造 message2，而发送设备无法识别其是否为黑客伪造。

[0030] Message1 中有黑客伪造 message2 所需要的信息 :SrcADD，DestADD，PTKID，MKID。Message2 中 R-Nonce 部分可以由黑客生成，或者黑客直接选取一个数值即可。因为黑客的目的是伪造一个错误的 message2，所以其中 PTKMIC 部分可以选取任何非 0 值。

[0031] (2) 伪造报文抢占时机可能性

[0032] 黑客可以和正常接收设备同时收到 message1 报文，但是对于正常接收设备，需要验证 PTKID 的唯一性，生成随机数，进行 MIC 计算，然后可以组建 message2。但对于黑客而言，不需要进行 PTKID 唯一性验证，不需要强调随机数的随机性，由于缺乏主密钥，MIC 计算对于黑客也无意义，所以黑客总可以比正常设备更快地组建 message2，抢在正常设备之前发出。

[0033] 综上所述，黑客根据 4- 路握手的协议漏洞发动抢占式拒绝服务攻击，剥夺正常设备的通信请求得以被响应的机会是完全可能的。图 2 为模拟的攻击过程。

[0034] 这种抢占式攻击对于黑客而言，只需要监听截获 message1 报文，伪造一个 message2 报文，就可以成功地剥夺正常设备请求通信的机会。对于黑客而言，这种攻击协议漏洞的攻击和其他的拒绝服务攻击比较，不需要发送大量的攻击报文，攻击成本最低，而攻击效果却是非常好的。

发明内容

[0035] 本发明实现一种在 UWB 网络中避免拒绝服攻击的方法，包括 :

[0036] 报文传输之前，对距离进行测定，估计正常报文到来时间，报文传输之后，对事件进行计时，根据报文返回时间确定不同的操作 ;

[0037] 其中距离测定方法具体为 :启动系统自带的距离测量功能 ;根据测量往返时间计算距离。

[0038] 根据距离测量结果设定信任区间的方法具体包括 :根据报文到来时间设定四个信任区间，分别为丢弃、保存、处理和等待，落入不同信任区间的报文分别按如下方法处理 :

[0039] 当报文到来过早，落入丢弃信任区间的时候，认为是可疑报文，将其丢弃。

[0040] 当报文落入保存的信任区间时用堆栈保存落入该区间报文，以便以后处理。

[0041] 在处理阶段的收到报文送入队列中，依次处理。

[0042] 在等待阶段收到的报文会被处理，等待间歇会处理保存阶段保存的报文。

[0043] 通过根据报文返回时间确定对接收报文的操作，本发明对抢占式拒绝服务攻击有很好的防御效果。

附图说明

[0044] 图 1 为现有技术 4 路握手过程的示意图；

[0045] 图 2 为模拟拒绝服务攻击示意图；

[0046] 图 3 为本发明实施 4 路握手的示意图。

具体实施方式

[0047] 1. 模块 301：距离测定方法

[0048] 系统本身有 range measure 功能，利用该功能在发送设备发送 message1 之前，启动该功能，对接收设备进行距离测量。

[0049] 距离测量的结果会返回 4 个时间值：

[0050] T1c = corrected RM1 send time

[0051] R1c = corrected RM1 receive time

[0052] T2c = corrected RM2 send time

[0053] R2c = corrected RM2 receive time

[0054] 利用上面四个值进行计算往返时间 Trip Time 为：

[0055] Trip Time = ((R2c-T1c)-(T2c-R1c))

[0056] 这个值是 message 在发送设备和接收设备之间往返一次的时间。

[0057] 2. 模块 302：信任区间设定

[0058] Expected Time 指的是发送设备发出 message1 之后预期可以收到 message2 的时间。Expected Time 由两部分组成，一部分是 Construct Time 指的是接收设备组建 message2 需要的时间；另一部分是 Trip Time 指的是 message 在接收设备和发送设备往返一次时间。

[0059] Expected Time = construct Time+Trip Time

[0060] Construct Time 是由生成随机数所需时间，KCK，PTK，MIC 计算所需时间构成，这个时间对于所有设备都是相同的。而 Trip Time 值是上面计算得出的，这个值相对于不同设备有所区别。

[0061] 发送设备发送 message1 同时启动定时器，此时刻为 0。从 0 时刻到系统设置的发送设备 timeout 时间段里，共分为 4 个信任时间区间：discarding，storing，processing，waiting。

[0062] [0,3/4Trip Time) 为 discarding 时间区间。

[0063] [3/4Trip Time，Trip Time) 为 storing 时间区间。

[0064] [Trip Time，1/3(Timeout+2expected)) 为 processing 时间区间。

[0065] [1/3(Timeout+2expected)，Timeout] 为 waiting 时间区间。

[0066] 3. 模块 304：信任区间的处理机制

[0067] Discarding 信任时间区间收到的 message2 被认为信任度最低，直接丢弃。

[0068] Storing 信任时间区间内收到的 message2 送入 SBuffer 中保存。SBuffer 为固定长度为 buffersize 的堆栈，其中保存收到的 message2 的 R-Nonce 和 PTKMIC。SBuffersize 建议保存 5 个 message2. 收到的 message2 依次压入堆栈，如果溢出，则从栈底部分丢弃。处理的时候从栈顶部分开始。Storing 部分只保存不处理。

[0069] Processing 信任时间区间为最有可能收到正常 message2 的时间段。在此时间段收到的 message2 送入 PBuffer，PBuffer 为可变长度队列。PBuffer 中 message2 将依次被处理验证，收到 MIC 验证符合的 message2 之后，SBuffer 和 PBuffer 缓冲区清零，拒绝接受其他的 message2，进入后续处理。

[0070] Waiting 信任时间区间收到的 message2 也会被处理，在处理的间歇，也就是发送设备等待的时候，发送设备会处理 SBuffer 中保存 message2。在此期间收到 MIC 验证符合的 message2，缓冲区清零，拒收以后的 message2，进入后续处理。

[0071] 在 timeout 时间段里处理的 message2 没有 MIC 验证符合的，握手中止，不再继续处理。

[0072] 4. 模块 303 :计时器的使用

[0073] 发送设备在发送 message1 的同时，启动计时器。发送设备计算信任时间区间，在整个系统定义的 timeout 时间段内划分四个时间区间 :discarding，storing，processing，waiting。发送设备在接收 message2 之后，获取计时器值。每收到一个 message2，获取计时器值，判断一下 message2 所落的区域。按照处理机制处理。

[0074] 本发明利用 UWB 自身所有的距离测量功能，增加少量的处理存储部件，成功解决了 ECMA-368 容易受到抢占式拒绝服务攻击的问题。

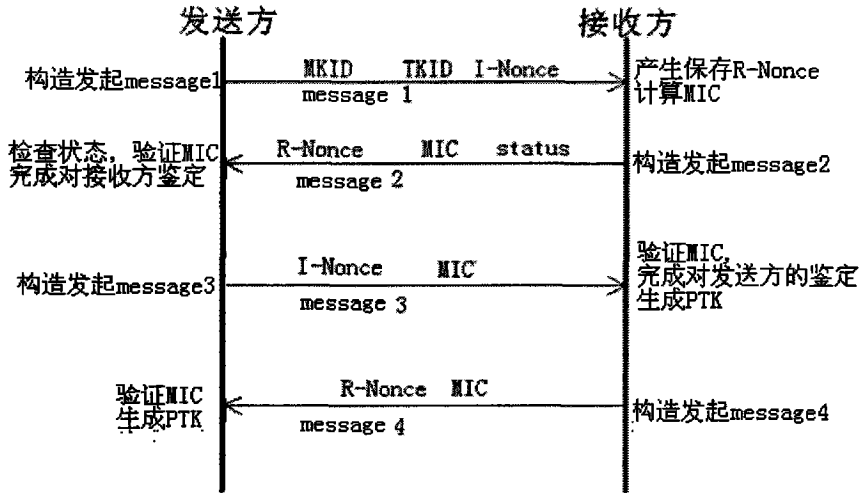

发送方
接收方
构造发起message1
MKID TKID I-Nonce
message 1
产生保存R-Nonce
计算MIC
检查状态，验证MIC
完成对接收方鉴定
R-Nonce MIC status
message 2
构造发起message2
构造发起message3
I-Nonce MIC
message 3
验证MIC，
完成对发送方的鉴定
生成PTK
验证MIC
生成PTK
R-Nonce MIC
message 4
构造发起message4

图 1

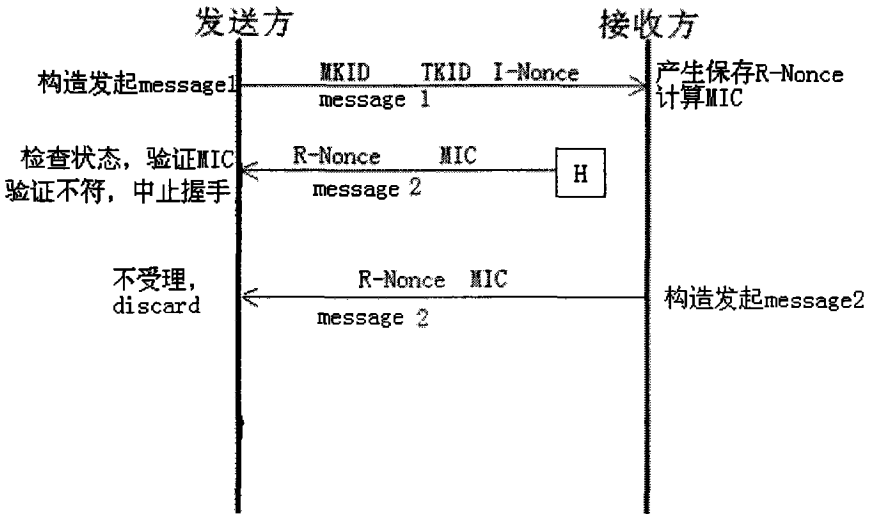

发送方
接收方
构造发起message1
MKID TKID I-Nonce
message 1
产生保存R-Nonce
计算MIC
检查状态，验证MIC
验证不符，中止握手
R-Nonce MIC
message 2
H
不受理，
discard
R-Nonce MIC
message 2
构造发起message2

图 2

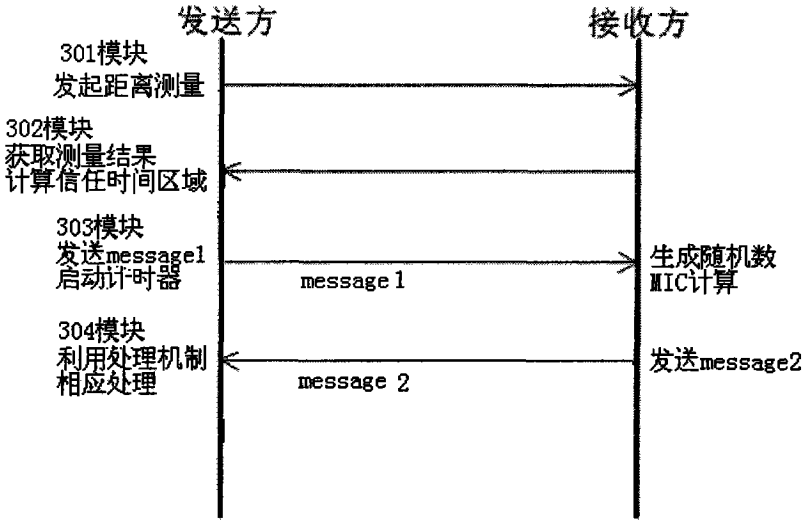

发送方
接收方
301模块
发起距离测量
302模块
获取测量结果
计算信任时间区域
303模块
发送message1
启动计时器
message 1
生成随机数
MIC计算
304模块
利用处理机制
相应处理
message 2
发送message2

图 3