一种面向体域网的数据安全混合传输机制

汪卫星

(重庆大学机械传动国家重点实验室 重庆 400030)

摘 要 无线体域网作为一种新型网络,被广泛应用到健康医疗、紧急救护等领域。然而,无线体域网收集到的数据大部分都是与用户个人有关的信息,在实际的应用部署过程中必然会面临严重的敏感隐私数据泄露或者被恶意篡改的风险。为了保证体域网环境下用户数据的隐私安全性,提出了一种数据安全混合传输机制,即基于多环模式的K匿名混合传输算法(AMT-ML),其主要思想是对通信节点进行网络划分,将其分成若干个通信环网络,并将K匿名方案应用到层次模型的感知层与传输层,通过进行多次K匿名处理来保证每一层的用户数据在概率上是相对安全的。实验结果显示,AMT-ML算法的隐私保护性优于基于单环模式的K匿名混合传输算法(AMT-SL),二层网络中多环模式的通信距离也小于单环模式的通信距离。

关键词 无线体域网,数据安全,数据传输

中图法分类号 TP393.4 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.05.018

Data Security Mix Transmission Mechanism in Body Area Network

WANG Wei-xing

(State Key Laboratory of Mechanical Transmissions, Chongqing University, Chongqing 400030, China)

Abstract Wireless body area network, as a new type of network, is widely used in health care, emergency rescue and other fields. However, the data collected by wireless body area network are mostly related to user's personal information. In the actual application of the deployment process, it is bound to face serious sensitive privacy data leakage or malicious tampering risks. In order to protect the privacy security of user data in the body area network environment, this paper proposed a data security mix transmission mechanism, which is a K-anonymous mix transmission algorithm based on single-loop model (AMT-ML). The main idea is to divide the communication nodes into several communication loop networks, and apply the K anonymous scheme to the perceptual layer and the transport layer of hierarchical model. In order to ensure that the user data in each layer are relatively safe, this paper used multiple K anonymous processing. The experimental results show that the privacy protection of AMT-ML is superior to K-anonymous mix transmission algorithm based on single-loop model (AMT-SL) algorithm, and the communication distance of the multi-loop mode in the two layer network is less than that of the single-loop mode.

Keywords Wireless body area network, Data security, Data transmission

1 简介

无线体域网[1](Wireless Body Area Network或Wireless Body Sensor Network,WBAN)是一种附着在人体身上的微型网络,主要由一些具有感知功能的传感器和一个身体主站(或称WBAN协调器)组成。协调器相当于一个网络簇头,起到媒介的作用,也是WBAN和外部网络(3G,4G,WiMAX、Wi-Fi)之间的网关,对数据进行存储并保证其安全地传送和交换。在WBAN中传感器节点不仅可以对人体的相关生理参数进行感知采集,还可以对人体周围的环境信息进行获取;然后将采集的数据信息发送到移动终端等相关设备上;最后通过互联网将采集到的数据信息发送到远程医疗服务中心等相关设备上,医疗中心根据不同的需求对数据进行相应的处理与分析。WBAN的具体体系结构[2]如图1所示。WBAN也是一种重要的公众应用网络,并在远程医疗保健、特殊人群监护和社区医疗等服务领域具有巨大的应用价值,并日渐成为研究热点[3]。

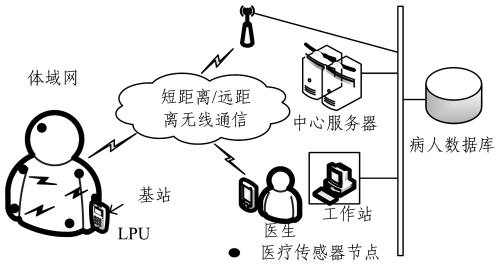

图1 无线体域网体系架构

Fig. 1 Wireless body area network architecture

无线体域网收集到的数据中大部分都是用户隐私信息,

到稿日期:2017-02-26 返修日期:2017-06-18 本文受广西高校中青年教师基础能力提升项目(KY2016YB755)资助。

汪卫星(1974-),男,博士,副教授,主要研究方向为云制造、网络安全、大数据,E-mail:wwx_ylq@126.com(通信作者)。

其在传输过程中很容易受到恶意攻击者的入侵,这些攻击者通过窃听和流量分析等手段对无线体域网的用户数据隐私的安全性造成了很大的威胁。攻击者对用户隐私数据进行攻击时,不仅可以获取网络环境中的相关参数配置,也可以获得用户个人的敏感隐私数据,从而可以潜在地获取各种服务信息,进而掌握用户的各种行为。因此,有必要对无线体域网数据传输过程中的用户数据隐私安全进行保护。为了保证体域网环境下用户数据的隐私安全性,本文针对无线体域网中数据传输方面的安全与隐私保护提出了一种数据安全混合传输机制,其主要思想是对通信节点进行网络划分,将其分成若干个通信环网络,并将 K 匿名方案应用到层次模型的感知层与传输层,通过进行多次 K 匿名处理来保证每一层的用户数据在概率上是相对安全的,使隐私数据被窃取的可能性在概率上达到最小值,进而实现无线体域网中用户隐私数据的安全传输。

2　相关工作

针对无线体域网数据传输的隐私安全问题,现阶段常使用数据加密技术来实现用户隐私数据的保护。然而由于无线体域网自身的能量、资源和数据存储能力有限,现有的密码机制已经很难满足无线体域网的需求。为了保证体域网用户隐私数据的安全性,有必要在密码技术的协同下引入其他新技术来实现用户隐私数据的安全传输。总结已有的针对无线体域网数据传输的安全与隐私保护的相关技术,其大致可分为:密码与密钥管理技术、安全传输隐私保护协议设计、认证技术、安全路由技术、入侵检测技术与生物识别技术、匿名技术、模糊技术。

目前,针对密码技术,文献[4]提出了一种基于时间和位置的密钥管理方案,为了实现无线体域网中用户隐私数据的安全传输,该协议将对称密码算法与主动秘密共享机制进行结合。针对安全传输隐私保护协议的设计,文献[5]提出了一种基于生理信号信息的密钥协议(PSKA),为体域网节点间的安全通信行为提供了保障;文献[6]提出了一种匿名认证与密钥协商的节点安全通信协议。针对安全路由技术,文献[7]提出了基于反馈信息的安全路由协议,文献[8]提出了基于地理位置信息的安全路由协议,文献[9]提出了基于密码算法的安全路由协议,文献[10]提出了基于多路径传输的安全路由协议,文献[11]提出了基于层次结构的安全路由协议,文献[12]提出了基于特定攻击的安全路由协议。针对生物识别技术和入侵检测技术的应用,文献[13]提出了基于角色的入侵检测技术并在其中融入了生物识别技术,该方案可以有效地确保 WBAN 传感器节点与簇头节点之间的数据进行安全传输。针对匿名技术,文献[14]研究了全局监听下流量分析攻击的机制,并提出了一种统计匿名保护方法 ProFit。针对模糊技术方案,文献[15]提出了一种修改的模糊库方案。

3　网络模型

针对远程医疗的实际应用场景,可以将体域网体系结构映射为三层网络模型,具体如图 2 所示。该三层网络模型从上到下依次为:应用层,一般由医疗数据中心充当,其作用主要是存储、分析收集到的所有用户数据,并将结果用于实际的医疗诊断;传输层,即簇头节点层,主要负责收集下层用户数据并将结果发送到应用层,相当于传输媒介;感知层,即采集节点层,主要负责感知采集与用户相关的信息,并将有用信息传输给上层网络。

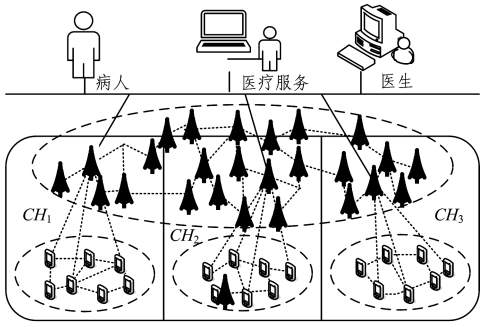

图 2　无线体域网的网络通信模型

Fig. 2　Wireless body area network communication model

网络结构的描述如下:

本文假设 WBAN 系统是由 N 个传感器节点组成的分层式系统,即所有传感器节点集合 $S=\{s_1,s_2,\cdots,s_N\}$,$N\geqslant M$。

根据传统传感器节点分簇方法,假设整个 WBAN 网络由 M 个彼此独立的传感器节点簇组成,即簇族 $CH=\bigcup_{i=1}^{M}CH_i$,其中每一个簇都是 WBAN 节点集 S 的一个非空真子集,即 $CH_i\subseteq S$,并且所有簇两两之间都是互斥分割的,即 $CH_i\cap CH_j=\emptyset(i\neq j,j=1,2,\cdots,M)$。用 $|CH_i|$ 表示簇 CH_i 中有效传感器节点的个数。

针对第二层,假设每一个节点簇 CH_i 中都有一个簇头节点 h_i,其负责存储、转发、处理来自簇内节点及其他簇头节点传送过来的用户生理体征数据,并最终将收集的结果发送到医疗数据处理中心,其簇头节点集合可表示为 $H=\{h_i,h_2,\cdots,h_M\}$。

定义每个传感器节点 $s_i(i\in N)$在有效的采样时间 t 内根据用户需求获得的生理体征参数信息为 r_i,其映射关系可以表示为 $r_i=r(s_i,t)$。针对每一个节点簇 CH_i 中的每个节点 s_{ij},$i\in M$,$j\in|CH_i|$,通过映射函数所获得的数据信息 r_{ij} 可以构成集合 $R_i=\{r_{ij}\mid r_{ij}=(s_{ij},t),\forall s_{ij}\in CH_i\}$,为此,整个 WBAN 中采集到的生命体征信息的数据超集可表示为$R=\{R_1,R_2,\cdots,R_M\}$,可以简单表示为$\{R_i\}_{1\leqslant i\leqslant M}$。用 $|R_i|$ 来表示在采样时间 t 内数据集合 R_i 内产生的有效数据量,可以简单理解为有效数据包的个数。

4　解决方案

根据医疗体域网的实际应用场景需求,在保证用户数据隐私安全的条件下,也应最大限度地延长网络的生命周期,并减少网络时延和能量消耗,即在保证相同通信能量的条件下可以发送更多的用户数据信息。为了更好地实现节点簇之间的 K 匿名需求,引入一个可信逻辑标签作为网络隐私数据传输与交换的媒介,以提升体域网中节点的计算能力。根据前文中定义的通用网络模型,并在充分考虑 WBAN 硬件资源及能量供应有限、网络拓扑动态变化的前提下,本节将提出基于多环模式的 K 匿名混合传输算法(K-Anonymous Mix Transmit Algorithm Based on Multi-Loop model,AMT-ML)。传统的安全保护机制一般都是基于单环模式的 K 匿名混合传输

算法(K-Anonymous Mix Transmit Algorithm Based on Single-Loop model,AMT-SL)的,即对网络模型的第二层(簇头层)进行处理。将所有的簇头节点通过网络初始化形成一个通信逻辑环网,并以可信逻辑标签作为通信信令,使满足 K 匿名需求的信息元集合在环网中不断地混合传输,并根据需求不断地往上层传输用户数据。基于此,并考虑到体域网中的用户隐私安全,在满足网络通信负载的前提下进行优化,将簇头层进行分割,即根据需要将同一个大的逻辑通信环划分成若干个彼此独立的通信小环,并给每一个小环设定一个自适应的 K 值,当满足要求时即可实现用户数据的混合传输,即基于多环模式的 K 匿名混合传输算法。具体的实现过程分为 3 个阶段。

4.1 环网络初始化阶段

本文对网络拓扑的划分可以等价为一个分离网络优化模型,即假设有一个拥有 100 个传感器节点的网络环境,要实现从其中任意一个节点出发以最短路径遍历完所有节点后再回到该节点,在现阶段通过单旅行商问题就可以解决;为了实现多个小型环网的初始化,就需要对一个大型环网进行网络分离,即把一个大的环网络划分成等价的多个小的环网络(还是 100 个节点),假设划分出 10 个小环,分别为 $L_1,L_2,\cdots,L_{10}$,即由其中任意 10 个节点开始传输数据,按照最短路径原则遍历完所有节点后再回到原始出发点,每个小环中的节点个数可以表示为 $num_i(1\leqslant i\leqslant 10)$,其中 $\sum_{i=1}^{10} num_i=100$。多个小环网络与单一的大环网络相比在通信距离上有所减少,符合体域网中传输距离短的特点,也更容易实现 K 匿名,有利于保证隐私数据的安全传输。

基于多旅行商问题(MTSP)的环形网络初始化主要通过遗传算法来实现。遗传算法的基本思想是针对要解决的问题首先产生一个特殊种群,该种群代表了要解决问题的一个模糊解的集合,并且该种群主要由若干个经过基因编码的个体组成。算法在实现的过程中首先要初始化种群,之后按照自然界传统的生存法则即适者生存和优胜劣汰来进行逐代进化,并且生成越来越趋于最优化的近似解。针对其中的任何一代,都要根据所要解决问题的适应度来选择个体,并且要依托于自然遗传学的遗传算子进行组合交叉和变异,之后生成针对要解决问题的新解的种群集合。这样经过逐代进化的后代产生的种群集合总比前一代的更优秀,最后将会获得最优的种群集合,将最优种群集合中的个体解码后即可得到要解决问题的最优近似解。网络初始化流程如算法 1 所示。

算法 1 环形网络的初始化

Input:network topology of WBAN cluster heads $H=\{h_1,h_2,\cdots,h_M\}$

Output:divided network topology loop$\{L_1,L_2,\cdots,L_i\}$,$(L_1+L_2+\cdots+L_i=H)$

Step1 Initialize the populations,generate random population of possible routes popRoute[popSize]=randperm(n),generate population of possible breaks popBreak[popSize]= rand_breaks().

Step2 Generate possible solutions by popRoute and popBreak.

Step3 Calculate total notes number N_i of each population members.

Step4 If $N_i\geqslant k$,select the solutions.

Step5 Else eliminate the solutions.

Step6 Calculate distance of each population member to evaluate fitness.

Step7 Find the best route in the population (select the shortest route).

Step8 Generate new random set of possible breaks.

Step9 Generate new solutions of possible routes by (Genetic algorithm operators which include Flip,Swap and Slide etc.)

Step10 If number of desired iterations numIter<1500 GOTO Step2.

Step11 End

4.2 可信逻辑标签的生成与维护阶段

在第一阶段已经完成环形网络的初始化,下面进入第二阶段。这里引入一个可信逻辑标签(TLT)作为协助在每一个环网络中实现 K 匿名隐私保护需求的传输介质,具体可表示为 $T(id,t\_pop)$,它是由簇头节点激发的,其中 $T.id$ 表示产生可信逻辑标签的簇头节点的 ID 号,$T.t\_pop$ 表示产生 TLT 时的系统时间。TLT 有一个有效的生命周期,将其定义为 $T.t\_idle$,倘若 TLT 闲置时间超过该数值,则 TLT 失效。

TLT 的生成过程主要涉及簇头节点、数据集合、临时 TLT、影子 TLT 等主要网络元素。在初始状态下,临时可信逻辑标签 $T_p(id,t_pop)$中没有任何数据信息,它是由簇头节点集合中的任意一个节点 $CH_i\in L_i$ 激发产生,之后将在环形网络中不断运行,不断地收集数据,并与 $R=\{R_1,R_2,\cdots,R_M\}$ 中的每一个数据集合进行混合转移处理,最终保证 $T_p(id,t_pop)$中的数据包数量满足 K 匿名需求,实现隐私数据的匿名传输。影子可信逻辑标签 $T_{tmp}(id,t_pop)$是随着 $T(id,t_pop)$的生成而产生的,其作用主要是防止 $T(id,t_pop)$的意外丢失,进而保证算法的鲁棒性。具体的 TLT 实现过程如算法 2 所示。

算法 2 K 匿名可信逻辑标签的生成

```
Input:logical ring networks topology loop Li and numi
Output:A mobile Tags T(id,t_pop) and Ttmp(id,t_pop)
        for random cluster head CHi∈Li generate initial Tags
  Tp(id,t_pop) do
  while |Tp|≤k do
     { if Ri≠Ø then |Tp|=|Tp|+|Ri| (ri∈Ri,i∈[1,|ci|])
    send Tp(id,t_pop) to next CHi+1∈Li
  wait for t_ack timeout
         {if t_ack timeout resend Tp(id,t_pop)
          else delete Tp(id,t_pop) in CHi
          end if }
       end if }
  end while
Turn Tp(id,t_pop) into T(id,t_pop)
and generate Ttmp(id,t_pop)
end for
hi.count=0
for each hi meets Ttmp(id,t_pop) do
  if hi.count=Ttmp.id {T(id,t_pop) is lost} then
requests to regenerate T(id,t_pop)
  else
delete Ttmp(id,t_pop)
  end if
end for
```

在上述实现过程中,$T_p(id,t_pop)$被激发后,将开始不断

地收集下层传感器节点发送到簇头节点的用户数据,并不断将其转发到下一个簇头节点 CH_{i+1},在这个过程中如果接收成功,簇头 CH_{i+1} 会发送确认信息到簇头 CH_i,依次循环直到 $T_p(id,t\_pop)$ 满足 K 匿名需求,则将其转为可信的 $T(id,t\_pop)$,同时生成一个影子标签 $T_{tmp}(id,t\_pop)$,它与 $T(id,t\_pop)$ 处在两个相邻的簇头节点上,并紧随其后。$T(id,t\_pop)$ 在环网中进行混合转移的过程中,在每一个簇头节点中有一个参数 $h_i.count$ 用于记录 $T(id,t\_pop)$ 经过簇头节点的 ID,当影子 $T_{tmp}(id,t\_pop)$ 发现 $h_i.count=T_{tmp}.id$ 时,则表明可信的 $T(id,t\_pop)$ 已经丢失,这时由 $T_{tmp}(id,t\_pop)$ 重新生成 $T(id,t\_pop)$ 用于实现数据的混合转移操作,反之,则清除 $T_{tmp}(id,t\_pop)$ 中的用户数据信息。最终,由这个可信的 $T(id,t\_pop)$ 在环网中不断地运行,并不断地把满足 K 匿名需求的用户隐私数据传送到医疗数据中心。

4.3　基于多环模式的 K-匿名混合传输算法

AMT-ML 算法是在 AMT-SL 的基础上做出的改进,主要是对第二层网络中簇头层中所有簇头节点形成的通信环网 L 进行划分,将其划分成若干个小环网,每一个环网有各自的可信逻辑标签,当小环网中用户数据满足给定的匿名值时,即开始与环内其他簇头节点进行混合转移处理。由于本方案中环形网络较小,数据传输耗时相对较少,当达到匿名要求时,数据开始不断地往上层网络传输,对于数据的容忍时间可以忽略。具体的 AMT-ML 算法流程如图 3 所示。

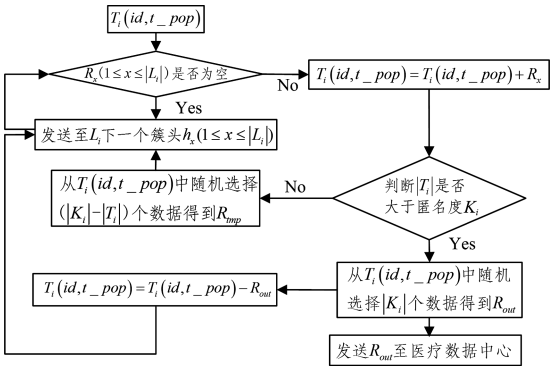

图 3　AMT-ML 算法流程

Fig. 3　Process of AMT-ML algorithm

在 AMT-ML 算法中,一共有 n 个小型环网 $L_i(0<i\leqslant n)$,每一个环网都对应一个可信逻辑标签 $T_i(id,t\_pop)$ 和一个匿名值 K_i。下面针对其中任意一个小环网来进行具体说明,当 $T_i(id,t\_pop)$ 在环网 L_i 中产生时,那么以该标签作为媒介的混合传输也同时被激活,$T_i(id,t\_pop)$ 往下一个簇头节点 $h_x\in L_i$ 传输,当节点内用户数据集合 $R_x(1\leqslant x\leqslant|L_i|)$ 不为空集时,将 $T_i(id,t\_pop)$ 和 R_x 做混合转移处理,得到一个更新后的 $T_i(id,t\_pop)$。统计其包含的数据包的数量级数 $|T_i|$,并将其与匿名值 K_i 比较,如果大于匿名值,说明已经满足 K 匿名传输条件,则从 $T_i(id,t\_pop)$ 中随机选取 K_i 个数据包发送到 Sink 节点,最后再将其剩余数据发送到相邻的下一个簇头节点开始新一轮的混合传输;如果小于匿名值,则从 $T_i(id,t\_pop)$ 中随机选取 $|K_i|-|T_i|$ 个数据包发送到下一个簇头节点重新开始下一轮的匿名混合传输。具体的 AMT-ML 算法的伪代码如算法 3 所示。

算法 3　AMT-ML 算法数据混合传输

```
Input:Li,Ki,S={CH,H,R},Ti(id,t_pop)
Output:Data set Rout
for cluster head hx∈Li received Ti(id,t_pop) do
  if Rx≠Ø(1≤x≤|Li|)
    {Ti(id,t_pop)=Ti(id,t_pop)+Rx
    if |Ti|≥Ki
      Rout=random pick |Ki| data set from Ti(id,t_pop)
      send Rout to the sink
      Ti(id,t_pop)=Ti(id,t_pop)-Rout
      send Ti(id,t_pop) to next hx+1∈Li
    else
      Rtmp=random pick |Ki|-|Ti| data set from Ti(id,t_pop)
      send Rtmp to next hx+1∈Li
    end if
else
{send Ti(id,t_pop) to next hx+1∈Li}
end if
end for
```

5　安全性分析

本文提出的体域网数据安全混合传输机制主要是把 K 匿名的思想应用到多个用户的医疗体域网场景中,实现了数据的安全传输,并满足了数据机密性、完整性、可靠性、不可否认性等安全要求。具体的安全性分析如下:

1)传统的对用户数据进行加/解密处理的方案已经很难保证用户数据在网络传输过程中的安全性,现阶段在数据传输过程中引入 K 匿名处理机制可以有效地保证隐私数据的安全传输,并且可以有效地抵御时间关联攻击和链接攻击。所谓时间关联攻击,简单来说就是攻击者对隐私数据的发送时间节点和接收时间节点在一个很长的时间段内不断地进行监听,从而获得发送节点和接收节点的相关时间序列,通过对其相关性进行分析可以猜解出通信双方的对应关系,进而获取用户隐私数据。在 K 匿名混合传输方案中,对发送端的数据进行了混合处理,而且数据的发送具有随机性,简单来讲,如果攻击者检测到发送节点发送的是数据 A,那么在接收端检测到的可能是数据 B 或者是其他的数据,而检测到数据 A 的可能性很小,因此在数据传输过程中其真实性被猜解的概率就会很小,进而可以有效地保证无线体域网用户隐私数据的安全性。

2)用户数据在网络中传输时,也很容易遭受恶意攻击者的链接攻击。所谓链接攻击,简单的理解就是攻击者并非直接对发送者或者接收者发起攻击,而是间接地与发送者自身相关联,例如假设发送者是一个病人,病人的身份、疾病类型都属于自己的直接相关信息,病房信息、看护、亲人、主治医师信息等都属于间接的相关信息,攻击者可以对用户的间接信息实施攻击,从而进一步猜解用户本地的真实数据信息。此外,攻击者也可对多个发送者信息实施攻击,通过对彼此之间的相关性进行猜解来获取用户的隐私数据。针对此种攻击,K 匿名混合传输方案不仅通过对节点之间的隐私数据进行混合转移使得通信双方在时间节点上进行解关联化,而且通过

对数据本身的匿名化处理使得其真实数据被攻击者猜解的概率大大降低。例如，给定一个数据集，如果其满足 K 匿名需求，那么攻击者对该数据集实施攻击时其真实数据被猜解的概率小于或等于 $1/K$。

总之，本文所提出的体域网数据安全混合传输算法不仅能够有效地确保体域网用户隐私数据的安全传输，保证隐私数据的可靠性、完整性、机密性，而且还可以有效地抵御时间关联性攻击和链接攻击，从而确保了整个体域网环境下隐私数据传输的安全性。

6 性能分析

通过上文对 AMT-ML 算法的详细介绍，现已对其网络模型、算法流程及实现有了深入的了解，下面将对其性能做进一步分析。本节主要从隐私保护性分析和网络通信距离分析两个方面入手。

6.1 隐私保护性分析

在多个用户的医疗体域网场景中，用户数据的隐私安全不仅关系到用户自身的人身安全、心理安全，也关系到医护人员对病人做出诊断的及时性和有效性。本文提出了 AMT-ML 算法，该算法通过对用户数据的匿名化处理，使得真实数据在匿名集合中被攻击者猜解的概率变得模糊化，同时也使得发送者和接收者在时间节点上的关联性变得随机化。为了验证 AMT-ML 算法的隐私保护性，下面将通过概率计算来对其性能进行分析，并与 AMT-SL 算法进行比较。首先假设两种算法都是在相同的物理环境和网络环境下执行的，根据前文医疗体域网网络模型分析，具体为：整个 WBAN 系统是由 N 个传感器节点组成的分层式系统，传感器节点集合 $S=\{s_1,s_2,\cdots,s_N\}$，第一层为采集节点层，拥有 $N-M$ 个节点，其中 M 为簇头节点个数，位于网络的第二层，即簇头节点层，每一个采集节点 s_i 对应的数据集为 $r_i(1\leqslant i\leqslant N-M)$，每个簇头节点 h_j 对应的数据集为 $R_i(1\leqslant i\leqslant M)$。下面将通过分析隐私数据被猜解的概率来衡量 3 种算法的性能。

在 AMT-SL 算法中，主要是对第二层网络进行处理，即在簇头节点层实现 K 匿名混合传输，在底层采集节点层对数据不做处理而直接发送到该节点所属簇的簇头节点处，等待混合转移处理之后再随机发送到医疗数据中心。假设攻击者想要获取底层某一个采集节点的真实数据，对任意一个簇内的节点进行分析，簇内采集节点个数为 $\frac{N}{M}-1$，对每一个节点采集的数据包作归一化处理，猜解某一个数据包归属于某一个采集节点的概率为 $\frac{1}{C_{\frac{N}{M}-1}^{x}}\cdot\frac{1}{C_x^1}(1\leqslant x\leqslant\frac{N-M}{M})$，其中 x 表示采集到的有效数据的节点个数，紧接着数据被直接传输到簇头节点层，当可信逻辑标签被激活时就开始数据的混合转移，得到一个混合后的匿名数据集。如果该数据集满足设定的 K_{sl} 匿名要求，则从该匿名集合中随机选取 K_{sl} 个用户数据包发送到医疗数据中心，在此过程中攻击者想要获取的某个真实的数据包的概率为 $\frac{1}{C_M^1}\cdot\frac{1}{C_{K_{sl}+x}^{K_{sl}}}\cdot\frac{1}{K_{sl}}$。通过对整个网络传输过程的分析，可以得到在 AMT-SL 算法中用户传输的隐私数据可能被攻击者猜解的概率表示：

$$P_{sl}=\frac{1}{C_{\frac{N}{M}-1}^{x}}\cdot\frac{1}{C_x^1}\cdot\frac{1}{C_M^1}\cdot\frac{1}{C_{K_{sl}+x}^{K_{sl}}}\cdot\frac{1}{C_{K_{sl}}^1}$$
$$=\frac{x!(\frac{N}{M}-1-x)!}{(\frac{N}{M}-1)!}\cdot\frac{1}{x}\cdot\frac{1}{M}\cdot\frac{K_{sl}!\ (K_{sl}+x-K_{sl})!}{(K_{sl}+x)!}\cdot\frac{1}{K_{sl}} \tag{1}$$

当所有的底层采集节点采集到的用户数据都是有效数据时，x 的取值就趋于最大化，在这种情况下 P_{sl} 的取值也会趋于最优化。把 $x=\frac{N-M}{M}$ 代入到式(1)可以得到：

$$P_{sl}=\frac{1}{N-M}\cdot\frac{K_{sl}!\ (\frac{N-M}{M})!}{(K_{sl}+\frac{N-M}{M})!}\cdot\frac{1}{K_{sl}} \tag{2}$$

AMT-ML 算法与 AMT-SL 算法的主要区别在于，后者是基于单环模式的混合转移传输，而前者是基于多环模式的混合转移传输。在相同的网络环境下，二者在采集节点层某一节点真实数据被猜解的概率是相同的，但当到达簇头节点层时则有所不同。假设网络中拥有 L_{ml} 个小环网络，底层节点数据随机传输到一个簇头节点，该簇头也随机属于一个小环网络，再结合所形成的小环网络可能也有大小之分，那么所对应的 K 值也有所不同。假定设定的匿名度为 K_{ml}，在此过程中攻击者想要获取的某个真实的数据包的概率为 $\frac{1}{C_M^1}\cdot\frac{1}{C_{K_{ml}+x}^{K_{ml}}}\cdot\frac{1}{C_{L_{ml}}^1}\cdot\frac{1}{C_{K_{ml}}^1}$，结合底层分析结果，可以得到在 AMT-ML 算法中用户传输的隐私数据可能被攻击者猜解的概率表示：

$$P_{ml}=\frac{1}{C_{\frac{N}{M}-1}^{x}}\cdot\frac{1}{C_x^1}\cdot\frac{1}{C_M^1}\cdot\frac{1}{C_{K_{ml}+x}^{K_{ml}}}\cdot\frac{1}{C_{L_{ml}}^1}\cdot\frac{1}{C_{K_{ml}}^1}\xrightarrow{x=\frac{N-M}{M}}$$
$$\frac{1}{N-M}\cdot\frac{K_{ml}!\ (\frac{N-M}{M})!}{(K_{ml}+\frac{N-M}{M})!}\cdot\frac{1}{L_{ml}}\cdot\frac{1}{K_{ml}} \tag{3}$$

通过对 AMT-SL 和 AMT-ML 算法的分析可以得出如图 4 所示的结果，从图中可以看出两种算法的总体趋势都是：随着匿名度 K 值的不断增加，其隐私数据被攻击者猜解的概率不断减小。当 $K=15$ 时出现一个临界值；当 $K<15$ 时很明显 P_{ml} 小于 P_{sl}；当 $K>15$ 时二者的值趋于平缓，但总体趋势还是 P_{ml} 小于 P_{sl}。很明显地可以看出，AMT-ML 算法的隐私保护性优于 AMT-SL 算法。

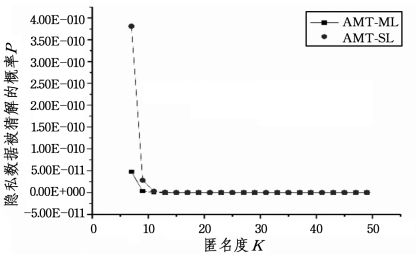

图 4 AMT-ML 与 AMT-SL 算法隐私保护性的比较

Fig. 4 Privacy protection comparison of AMT-ML and AMT-SL algorithms

6.2 网络通信距离分析

本文提出的 AMT-ML 算法对网络拓扑进行了划分，其

不仅比传统的直接点对点的传输在通信距离上有所减小,也能够更好地保护数据传输过程中的隐私安全。由前文分析可知,AMT-SL 算法与 AMT-ML 算法在底层网络的通信情况是完全相同的,主要区别在于簇头节点层。下面主要对两种算法中第二层网络拓扑的形成及通信距离做进一步分析。

为了更好地进行性能分析,在多个用户的医疗体域网场景中做如下考虑:WBAN 中所有节点数量 $N=600$,簇的个数 $M=30$,即簇头节点个数也为 30,并且每一个簇拥有的节点数目相同,即每一个簇内有 20 个节点。下面对两种算法中网络拓扑的距离进行计算,通过对网络原型执行遗传算法可以得到如图 5 和图 6 所示的结果。

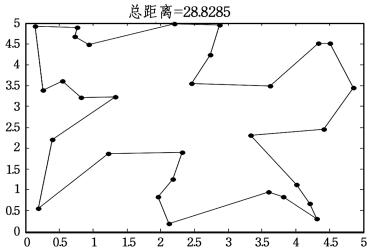

图 5　AMT-SL 算法的通信距离

Fig. 5　Communication distance of AMT-SL algorithm

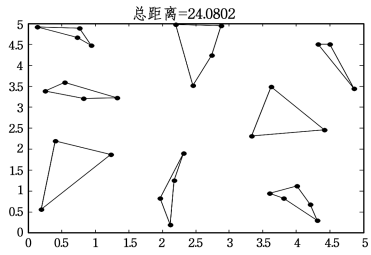

图 6　AMT-ML 算法的通信距离

Fig. 6　Communication distance of AMT-ML algorithm

图 5 示出了 AMT-SL 算法在簇头节点层的通信距离 $d_{loop1}=28.8285$,图 6 示出了 AMT-ML 算法在簇头节点层的通信距离 $d_{loop2}=24.0802$,很明显在二层网络中多环模式的通信距离小于单环模式的通信距离。

结束语　在无线体域网中针对不同的数据操作对应着不同的数据隐私保护方法。本文从数据传输隐私保护的角度出发,提出了一种数据安全混合传输机制,即基于多环模式的 K 匿名混合传输算法(AMT-ML),其主要思想是对通信节点进行网络划分,将其分成若干个通信环网络,并将 K 匿名方案应用到层次模型的感知层与传输层,通过进行多次 K 匿名处理来保证每一层的用户数据在概率上是相对安全的,即使得隐私数据被窃取的可能性在概率上达到最小值,进而实现无线体域网中用户隐私数据的安全传输。虽然目前关于无线体域网的研究大多集中在系统的架构方面,但鉴于无线体域网所传输的信息的重要性,隐私安全问题是 WBAN 系统必须要解决的问题,因此本文所提出的方案有一定的应用价值。

参 考 文 献

[1] MAINANWAL V, GUPTA M, UPADHAYAY S K. A survey on wireless body area network: Security technology and its design methodology issue[C]// International Conference on Innovations in Information, Embedded and Communication Systems. Coimbatore: IEEE Press, 2015: 1-5.

[2] GONG J B, WANG R, CUI L. Research Ddvances and Challenges of body Sensor network[J]. Journal of Computer Research and Development, 2010, 47(5): 737-753. (in Chinese)
宫继兵,王睿,崔莉. 体域网 BSN 的研究进展及面临的挑战[J]. 计算机研究与发展, 2010, 47(5): 737-753.

[3] LIU L, XUE X Q, LUO X L. Architecture and Challenges of Wireless Body Area Network[J]. Computer Knowledge and Technology, 2012, 8(29): 6918-6920. (in Chinese)
刘璐,薛秀芹,罗先露. 无线体域网的体系结构及面临的挑战[J]. 电脑知识与技术, 2012, 8(29): 6918-6920.

[4] ZHOU J, CAO Z, DONG X, et al. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks[J]. Information Sciences, 2015, 314(2): 255-276.

[5] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. PSKA: usable and secure key agreement scheme for body area networks[J]. Information Technology in Biomedicine, 2010, 14(1): 60-68.

[6] LI X, IBRAHIM M H, KUMARI S, et al. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks[J]. Computer Networks, 2017, 115(1): 1-15.

[7] GALUBA W, PAPADIMITRATOS P, POTURALSKI M, et al. Castor: scalable secure routing for ad hoc networks[C]// Proceedings of IEEE INFOCOM. San Diego: IEEE Press, 2010: 1-9.

[8] DEFRAWY K E, TSUDIK G. Privacy-preserving location-based on-demand routing in MANETs[J]. Selected Areas in Communications, 2011, 29(10): 1926-1934.

[9] JARADAT T, BENHADDOU D, BALAKRISHNAN M, et al. Energy efficient cross-layer routing protocol in Wireless Sensor Networks based on fuzzy logic[C]// Wireless Communications and Mobile Computing Conference. Sardinia: IEEE Press, 2013: 177-182.

[10] WANG H, YANG G, XU J, et al. A reliable data transmission protocol based on multipath routing for wireless sensor networks[J]. Sensor Letters, 2016, 14(9): 923-927.

[11] QUANG P T A, KIM D S. Clustering algorithm of hierarchical structures in large-scale wireless sensor and actuator networks [J]. Journal of Communications & Networks, 2015, 17(5): 473-481.

[12] REN J, ZHANG Y, ZHANG K, et al. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(5): 3718-3731.

[13] SHARMILEE K M, MUKESH R, DAMODARAM A, et al. Secure WBAN using rule-based IDS with biometrics and MAC authentication[C]// International Conference on E-Health Networking. Singapore: IEEE Press, 2008: 102-107.

[14] SHAO M, YANG Y, ZHU S C, et al. Towards statistically strong source anonymity for sensor networks[C]// The 27th Conference on Computer Communications (INFOCOM 2008). Phoenix: IEEE Press, 2008: 51-55.

[15] CHEN S L. A Power-Efficient Adaptive Fuzzy Resolution Control System for Wireless Body Sensor Networks[J]. Access IEEE, 2015, 3: 743-751.