置换再交叉运算的所有权转移协议

刘宗妹 徐金成
(广东司法警官职业学院信息管理系 广东 广州 510520)

摘 要 针对标签生命周期中归属权转变过程中存在的隐私信息易泄露问题,设计一种基于置换再交叉运算的所有权转移协议。协议为保证隐私信息的安全性,采用基于大数分解难题的二次剩余定理对部分信息加密;同时协议为保证尽可能降低系统的计算量,引入基于位运算的置换再交叉运算对部分信息加密。为抵抗常见类型攻击方式,协议采用先认证再操作的机制。将该协议与其他协议进行安全性和性能分析,该协议具备安全性高、计算量小等优势。

关键词 物联网 射频识别技术 置换再交叉运算 转移协议 二次剩余定理 所有权

中图分类号 TP393.08 **文献标志码** A DOI: 10.3969/j.issn.1000-386x.2021.09.053

OWNERSHIP TRANSFER PROTOCOL ON REP-REC

Liu Zongmei Xu Jincheng
(*Department of Information Management, Guangdong Justice Police Vocational College, Guangzhou 510520, Guangdong, China*)

Abstract In order to solve the problem that privacy information is easy to leak in the process of ownership transformation in the label life cycle, a ownership transfer protocol based on Rep-Rec is designed. In order to ensure the security of privacy information, the protocol encrypted the partial information by using the quadratic residual theorem based on the big number decomposition problem. At the same time, in order to reduce the calculation of the system as much as possible, the protocol introduced the replacement and cross operation based on bit operation to encrypt partial information. In order to resist common types of attacks, the protocol adopted the mechanism of authentication before operation. This paper analyzed the security and performance of this protocol and other protocols. This protocol has the advantages of high security and small computation.

Keywords Internet of things RFID technology Rep-Rec Transfer protocol Secondary residual theorem Ownership

0 引 言

射频识别系统[1-2]因其自身特有的属性特点,在公交卡系统等各个领域中均有涉及[3]。典型的 RFID 系统由标签、读卡器、数据库组成,其中读卡器与数据库之间采用较为安全的有限方式通信,一般认定为可靠,因此常将二者看作一个整体以便于研究及建模型[4-5]。

标签在运用过程中,标签的归属者会经常发生变更,一个经典的运用链如下:嵌有标签的商品由生产商生产出来,未出场之前,商品的归属者是生产商;批发商从生产商购买商品后,商品的归属者由生产商变更为批发商;当零售商从批发购买商品后,商品的归属者由批发商变更为零售商;最终消费者会从零售商手上买得该商品,商品的归属者由零售商又变更为消费者[6-8]。在上述归属者变更过程中,存放在标签中的隐私信息需要保证其安全性,同时也需要确保信息的前向安全性和后向安全性[9-11]。

为能够保障标签在其生命过程中归属者变化时,隐私信息的安全性,文献[12]中基于 SQUASH 提出一种超轻量级所有权转移协议,同时声称能够抵抗去同

收稿日期:2019-11-07。广东省科技厅社会发展科技协同创新体系建设-基于大数据的服刑人员再犯罪风险评估研究(2019B020208001)。刘宗妹,讲师,主研领域:人工智能,信息安全。徐金成,讲师。

步化等攻击。文献[13]中对文献[12]的安全性提出了质疑,分析了协议并不具备抵抗攻击者发起的异步攻击能力,并提出了一个超轻量级协议,但该协议的安全性仍有待全面的系统验证,同时该协议无法满足重放攻击。文献[14]提出一种协议,但分析后发现,协议因使用随机数的明文传送,使得协议存在一定的缺陷,无法抵抗假冒攻击。文献[15]同样利用二次剩余设计一种协议,协议主要存在的问题在于每次通信完成后,通信实体并没有对认证用到的共享密钥进行更新,从而无法提供追踪攻击的抵抗能力。

鉴于现有的大多数所有权协议存在如下缺陷: 1) 通信过程复杂; 2) 通信协议中,通信实体的计算量大; 3) 通信协议自身具备的安全缺陷,无法提供安全性。在分析众多协议基础之上,本文给出一种所有权协议。协议基于二次剩余和置换再交叉运算对信息加密,对于较为重要的隐私信息基于二次剩余进行加密,增大攻击者的破解难度,其他信息采用置换再交叉运算进行加密,这样使得在确保信息安全的前提下,也可以满足降低计算量的要求。

1　所有权协议

1.1　符号说明

对协议中出现的符号进行如下说明:

S_{old}: 标签原所有者;

S_{new}: 标签新所有者;

T_i: 第 i 个标签;

S_{old_ID}: S_{old}的标识符;

S_{new_ID}: S_{new}的标识符;

T_{ID_L}: T_i 标识符的左半部分;

T_{ID_R}: T_i 标识符的右半部分;

p_1、q_1: S_{old}随机选择的两个大素数;

n_1: p_1 和 q_1 的乘积,即 $n_1 = p_1 \times q_1$;

p_2、q_2: S_{new}随机选择的两个大素数;

n_2: p_2 和 q_2 的乘积,即 $n_2 = p_2 \times q_2$;

K_{old}: S_{old}与 T_i 之间共享的密钥;

K_{new}: S_{new}与 T_i 之间共享的密钥;

r_1、r_2、r_3: T_i 产生的三个随机数;

r_4: S_{new}产生的随机数;

⊕: 按位异或运算;

&: 按位与运算;

Rep-Rec(X,Y): 置换再交叉运算;

$X^2 \bmod n$: 模运算。

1.2　置换再交叉运算

置换再交叉运算在文中用符号 Rep-Rec(X, Y)(Replacement and Re-cross Operation)表示,其具体定义如下: X、Y、Z 均表示长度为偶数 L 位的二进制序列; 指针 $P1$、$P2$ 分别指向二进制序列 X、Y; $H_W(X)$ 表示二进制序列 X 的汉明重量。

指针 $P1$、$P2$ 分别指向二进制序列 X、Y 的第一位,然后开始进行遍历操作,当指针 $P1$ 所指向二进制序列 X 的第 i 位为 0 时,指针 $P2$ 所指向二进制序列 Y 的第 i 位数值进行取反操作,即 0 变 1、1 变 0; 当指针 $P1$ 所指向二进制序列 X 的第 i 位为 1 时,指针 $P2$ 所指向二进制序列 Y 的第 i 位数值不变。依照上述操作可得到二进制序列 Z,即完成置换操作。

$H_W(X)$ 表示二进制序列 X 的汉明重量、$H_W(Y)$ 表示二进制序列 Y 的汉明重量、$H_W(X-Y)$ 表示 $H_W(X)$ 与 $H_W(Y)$ 的差值绝对值。根据 $H_W(X)$、$H_W(Y)$ 两者具体数值大小关系进行不同的运算。具体地,当 $H_W(X) \geqslant H_W(Y)$ 时,将二进制序列 Z 的左边 $H_W(X-Y)$ 位、二进制序列 Z 的右边 $L-H_W(X-Y)$ 位进行交换,即可得到的 Rep-Rec(X, Y) 值; 当 $H_W(X) < H_W(Y)$ 时,将二进制序列 Z 的右边 $H_W(X-Y)$ 位、二进制序列 Z 的左边 $L-H_W(X-Y)$ 位进行交换,即可得到的 Rep-Rec(X, Y) 值。

为更好地描述出置换再交叉运算的实现,结合例子进行解释。此处取 $L=12$, $X=0001\ 1101\ 1111$, $Y=1101\ 1000\ 0001$,则 $H_W(X)=8$, $H_W(Y)=5$, $H_W(X-Y)=3$, $Z=0011\ 1010\ 0001$, Rep-Rec(X, Y) $=1101\ 0000\ 1001$,如图 1 所示。此处取 $L=12$, $X=1001\ 1101\ 0010$, $Y=1101\ 1111\ 0001$,则 $H_W(X)=6$, $H_W(Y)=8$, $H_W(X-Y)=2$, $Z=1011\ 1101\ 1100$, Rep-Rec(X, Y) $=0010\ 1111\ 0111$,如图 2 所示。

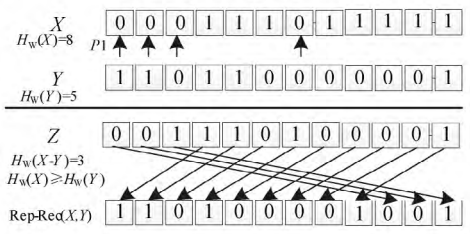

图 1　置换再交叉运算($H_W(X) \geqslant H_W(Y)$)

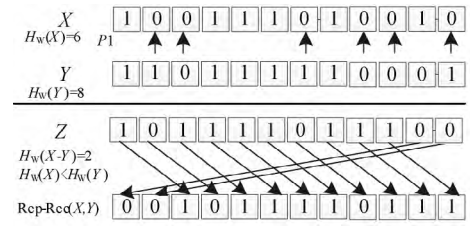

图 2　置换再交叉运算($H_W(X) < H_W(Y)$)

1.3 协议步骤

所有权转移协议共分为两个阶段: 初始化阶段; 所有权转移阶段。

(1) 初始化阶段。所有权转移协议开始之前,S_{old} 随机选择 p_1、q_1 大素数,计算两者的积,同时赋值给 n_1。将事先计算好的 B 的值,同时存放在 S_{old}、S_{new}、T_i 三者中。S_{old} 中存放 S_{old_ID}、K_{old}; S_{new} 中存放 S_{new_ID}; T_i 中存放 S_{old_ID}、K_{old}、S_{new_ID}。

(2) 所有权转移阶段。对图 3 中字符进行解释:

$A = n_1 \oplus S_{old\_ID}$;

$B = \text{Rep-Rec}(T_{ID\_L} \oplus T_{ID\_R}, T_{ID\_L} \,\&\, T_{ID\_R})$;

$B' = \text{Rep-Rec}(K_{new} \oplus x, K_{new} \,\&\, x)$;

$D = B \oplus S_{old\_ID} \oplus r_1$;

$D'' = D^4 \bmod n_1'$;

$E = S_{new\_ID} \oplus r_2$;

$F = S_{old\_ID} \oplus r_1$;

$G = B \oplus r_1'$;

$H = \text{Rep-Rec}(G \oplus n_2 \oplus r_2', G \,\&\, n_2 \,\&\, r_2')$;

$M = n_2 \oplus S_{new\_ID}$;

$N = K_{old} \oplus r_3$;

$N' = N^2 \bmod n_2$;

$N'' = N^4 \bmod n_2$;

$P = \text{Rep-Rec}(N \oplus n_2, N \,\&\, n_2)$;

$Q = K_{new} \oplus x$;

$L = r_4 \oplus x$;

$V = \text{Rep-Rec}(r_4 \oplus Q, r_4 \,\&\, Q)$。

所有权转移协议如图 3 所示。

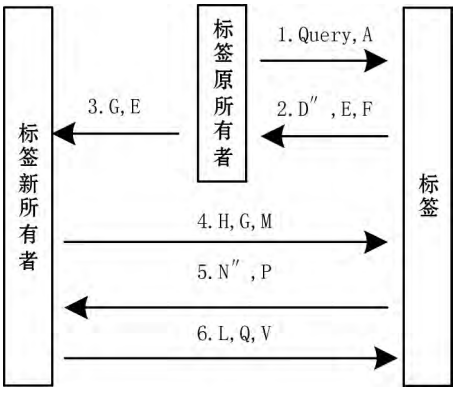

图 3 所有权转移协议

步骤 1 S_{old} 用 n_1、S_{old_ID} 来计算 A 的值,将 A 及 Query 指令传送给 T_i。

步骤 2 T_i 收到信息后,先计算 $A \oplus S_{old\_ID}$ 得到 n_1',在生成 r_1、r_2 随机数,并用 B、S_{old_ID}、r_1 计算 D 的值,用 D、n_1' 计算 D'' 的值,用 S_{new_ID}、r_2 计算 E 的值,用 S_{old_ID}、r_1 计算 F 的值,最后将 (D'', E, F) 传送给 S_{old}。

步骤 3 S_{old} 收到信息后,先计算 $F \oplus S_{old\_ID}$ 得到随机数 r_1',用 n_1 和 D'' 通过二次剩余定理的方法,解出 D 的值,这里用 D' 表示,即 S_{old} 会解出以 n 为模的 D^2 的 D 的值,利用 p 和 q 获得 D^2 的值。

比对 $D' \oplus r_1'$ 与 $B \oplus S_{old\_ID}$ 的值。若不相等,T_i 验证不通过,协议终止; 若相等,说明 $D' = D$、$r_1' = r_1$, S_{old} 用 B、r_1' 来计算 G 的值,最后将 (G, E) 传送给 S_{new}。

步骤 4 S_{new} 收到信息后,先随机生成 p_2、q_2 大素数,并计算 $n_2 = p_2 q_2$,接着计算 $E \oplus S_{new\_ID}$ 得到随机数 r_2',然后用 G、n_2、r_2' 计算 H 的值,用 n_2、S_{new_ID} 计算 M 的值,最后将 (H, G, M) 传送给 T_i。

步骤 5 T_i 收到信息后,先计算 $M \oplus S_{new\_ID}$ 得到 n_2',接着用 r_1、B、n_2'、r_2 来计算 H' 的值,即:

$$H' = \text{Rep-Rec}((B \oplus r_1) \oplus n_2' \oplus r_2, (B \oplus r_1) \,\&\, n_2' \,\&\, r_2)。$$

比对 H' 与 H 的值。若相等,说明 $n_2' = n_2$, $r_2' = r_2$,接着 T_i 生成 r_3 随机数,用 K_{old}、r_3 来计算 N 的值,用 N、n_2' 分别计算 N'、N'' 的值,用 N、n_2' 来计算 P 的值,最后将 (N'', P) 传送给 S_{new}; 若不相等,协议终止。

步骤 6 S_{new} 收到信息后,先用二次剩余定理解出以 n_2' 为模的 N^2 的解,这里用 x 表示该解,同时利用 p_2 和 q_2 为模,识别 N^2 的值。在用 x、n_2 来计算 P' 的值,即:

$$P' = \text{Rep} - \text{Rec}(x \oplus n_2, x \,\&\, n_2)$$

比对 P' 与 P 的值。若不相等,协议终止; 若相等,说明 $x = N'$,生成 r_4 随机数,生成新的共享密钥 K_{new},用 K_{new}、x 计算 Q 的值,用 x、r_4 计算 L 的值,用 r_4、Q 计算 V 的值,用 x、K_{new} 来计算 B' 的值,并更新信息: $S_{new\_ID} = r_4$、$B = B'$,最后将 (L, Q, V) 传送给 T_i。

步骤 7 T_i 收到信息后,先计算 $Q \oplus N'$ 得到新的共享密钥 K_{new}',计算 $L \oplus N'$ 得到 r_4' 随机数,用 r_4'、Q 来计算 V' 的值,即:

$$V' = \text{Rep} - \text{Rec}(r_4' \oplus Q, r_4' \,\&\, Q)$$

比对 V' 与 V 的值。若不相等,协议终止; 若相等,说明 $r_4' = r_4$,用 N'、K_{new}' 来计算 B' 的值,T_i 更新信息: $K_{new} = Q \oplus N'$, $r_4 = L \oplus N'$, $B = B'$。此时 T_i 和 S_{new} 之间的密钥保持一致,所有权完成转移。

协议与其他此类协议比较所具备的优势如下: 在抵抗攻击者发动攻击方面,采用二次剩余对发送信息加密,在数学领域中,大素数的分解一直是无法破解的难题,因此采用二次剩余加密,能够增大攻击者的破解难度。在保证信息安全的前提下,要尽可能地降低系统的计算量,因此设计出一种基于超轻量级的采用按位运算实现的置换再交叉运算对部分信息进行加密,能够满足降低系统的计算量。

2　安全性分析

本文协议采用基于 GNY 逻辑形式化语言对协议进行逻辑形式化推理[16]。

(1) 协议形式化描述。

协议流程如下:

Msg1: $S_{old}\rightarrow T_i$: $Query$、A。

Msg2: $T_i\rightarrow S_{old}$: D''、E、F。

Msg3: $S_{old}\rightarrow S_{new}$: G、E。

Msg4: $S_{new}\rightarrow T_i$: H、G、M。

Msg5: $T_i\rightarrow S_{new}$: N''、P。

Msg6: $S_{new}\rightarrow T_i$: L、Q、V。

用 GNY 形式逻辑语言规范以上协议,描述如下:

Msg1: $T_i<^*\ \ Query$、A;

Msg2: $S_{old}<^*\ \ \{D''$、E、$F\}$;

Msg3: $S_{new}<^*\ \{G$、$E\}$;

Msg4: $T_i<^*\ \{H$、G、$M\}$;

Msg5: $S_{new}<^*\ \{N''$、$P\}$;

Msg6: $T_i<^*\ \{L$、Q、$V\}$。

(2) 协议初始化假设。

协议假设如下: S_{new}、T_i、S_{old}表示主体。

Sup1: $(S_{old\_ID}$、S_{new_ID}、K_{new}、K_{old}、T_{ID}、r_1、r_2、r_3、$B)\in T_i$;

Sup2: $(p_2$、q_2、n_2、r_4、S_{new_ID}、$K_{new})\in S_{old}$;

Sup3: $(S_{old\_ID}$、K_{old}、p_1、q_1、$n_1)\in S_{new}$;

Sup4: $S_{old}\mid\equiv\#(r_1$、r_2、r_3、$r_4)$;

Sup5: $T_i\mid\equiv\#(r_1$、r_2、r_3、$r_4)$;

Sup6: $S_{new}\mid\equiv\#(r_1$、r_2、r_3、$r_4)$;

Sup7: $T_i\mid\equiv S_{new}\overset{S_{new\_ID}、B}{\leftrightarrow}T_i$;

Sup8: $T_i\mid\equiv S_{old}\overset{S_{old\_ID}、K_{old}、B}{\leftrightarrow}T_i$;

Sup9: $S_{old}\mid\equiv T_i\overset{S_{old\_ID}、K_{old}、B}{\leftrightarrow}S_{old}$;

Sup10: $S_{new}\mid\equiv T_i\overset{S_{new\_ID}、B}{\leftrightarrow}S_{new}$。

(3) 协议证明目标。

目标的证明公式如下:

Goal1: $T_i\mid\equiv S_{old}\mid\sim\#\{A\}$;

Goal2: $S_{old}\mid\equiv T_i\mid\sim\#\{D''$、$E$、$F\}$;

Goal3: $S_{new}\mid\equiv S_{old}\mid\sim\#\{G$、$E\}$;

Goal4: $T_i\mid\equiv S_{new}\mid\sim\#\{H$、$G$、$M\}$;

Goal5: $S_{new}\mid\equiv T_i\mid\sim\#\{N''$、$P\}$;

Goal6: $T_i\mid\equiv S_{new}\mid\sim\#\{L$、$Q$、$V\}$。

(4) 协议证明过程。

因协议证明目标 Goal2: $S_{old}\mid\equiv T_i\mid\sim\#\{D''$、$E$、$F\}$; Goal3: $S_{new}\mid\equiv S_{old}\mid\sim\#\{G$、$E\}$; Goal4: $T_i\mid\equiv S_{new}\mid\sim\#\{H$、$G$、$M\}$; Goal5: $S_{new}\mid\equiv T_i\mid\sim\#\{N''$、$P\}$; Goal6: $T_i\mid\equiv S_{new}\mid\sim\#\{L$、$Q$、$V\}$ 的证明过程与协议证明目标 Goal1: $T_i\mid\equiv S_{old}\mid\sim\#\{A\}$ 证明过程相似,以协议证明目标 Goal1 为例。

$\because$ 规则 P_1: $\dfrac{P<X}{X\in P}$和 Msg1: $T_i<^*\ \ Query$、A

$\therefore\ \{A\}\in T_i$

$\because$ 规则 F_1: $\dfrac{P\mid\equiv(X)}{P\mid\equiv(x,y),P\mid\equiv\#F(X)}$以及 Sup4: $S_{old}\mid\equiv\#(r_1$、r_2、r_3、$r_4)$

$\therefore\ S_{old}=\#\{A\}$

$\because$ 规则 P_2: $\dfrac{X\in P,Y\in P}{(X,Y)\in P,F(X,Y)\in P}$, Sup1: $(S_{old\_ID}$、S_{new_ID}、K_{new}、K_{old}、T_{ID}、r_1、r_2、r_3、$B)\in T_i$ 和 Sup2: $(p_2$、q_2、n_2、r_4、S_{new_ID}、$K_{new})\in S_{old}$

$\therefore\ \{A\}\in S_{old}$

$\because$ 规则 $F10$: $\dfrac{P\mid\equiv(X),X\in P}{P\mid\equiv\#(H(X))}$以及推导出来的 $S_{old}=\#\{A\}$、$\{A\}\in S_{old}$

$\therefore\ S_{old}\mid\equiv\#\{A\}$

$\because$ 规则 $I3$: $\dfrac{P<H(X,<S>)>,(X,S)\in P,P\mid\equiv P\leftrightarrow Q,P\mid\equiv\#(X,S)}{P\mid\equiv Q\mid\sim(X,S),P\mid\equiv Q\sim H(X,<S>)}$

又$\because$ Sup8: $T_i\mid\equiv S_{old}\overset{S_{old\_ID}、K_{old}、B}{\leftrightarrow}T_i$、Sup9: $S_{old}\mid\equiv T_i\overset{S_{old_ID}、K_{old}、B}{\leftrightarrow}S_{old}$以及 Msg1: $T_i<^*\ \ Query$、A

$\therefore\ T_i\mid=S_{old}\sim\{A\}$

$\because$ 新鲜性定义以及推导出来的 $S_{old}=\#\{A\}$、$T_i\mid=S_{old}\sim\{A\}$

$\therefore$ Goal1: $T_i\mid\equiv S_{old}\mid\sim\#\{A\}$ 得证明。

本文协议与其他协议进行安全性比较结果如表 1 所示。

表 1　协议之间的安全性比较

攻击类型	文献[12]	文献[13]	文献[14]	文献[15]	本文协议
重放攻击	√	×	√	√	√
假冒攻击	√	√	×	√	√
异步攻击	×	√	√	√	√
追踪攻击	√	√	√	×	√
后向安全	√	√	√	√	√
前向安全	√	√	√	√	√

3　性能分析

性能分析部分选择标签为对象,标签原所有者和标签新所有者中均包含数据库,数据库具备强大的存

储空间和计算能力，因此不作为性能分析的对象。以标签为对象时，主要关注于标签一端的计算量，因对于现有的无源低成本计算量的标签来说，标签具备的计算能力受到严格的限制。本文协议与其他此类协议进行性能分析如表 2 所示。

表 2 协议之间的性能比较

比较文献	计算量
文献[14]	$5a+2b+11c$
文献[15]	$6a+b+14c$
本文协议	$3a+3b+9c+3d$

对于表 2 中符号进行下面的含义约定：用 a 表示二次剩余加密方法的计算量；用 b 表示产生随机数的计算量；用 c 表示按位运算（按位运算一般包含按位或运算、按位异或运算、按位与运算、左移运算、右移运算）；用 d 表示置换再交叉运算加密方法的计算量。

在上述不同的运算中，计算量最大的是二次剩余，次之的是随机数的产生计算量，置换再交叉运算及按位运算均属于超轻量级的运算。现有的文献已证明：超轻量级的运算进行次数的多与少，对协议的计算量所带来的影响可以忽略。

以本文协议中 $3a$ 的产生为例说明标签一端的计算量的计算方法。1）第一次用到二次剩余。标签一端在步骤 2 中计算 D''的时候，会第一次用到二次剩余。2）第二次用到二次剩余。标签一端在步骤 5 中计算 N'的时候，会第二次用到二次剩余。3）第三次用到二次剩余。标签一端在步骤 5 中计算 N''的时候，会第三次用到二次剩余。基于上述分析，本文协议标签一端一共会有三次用到二次剩余加密方法对信息进行，因此是 3a。从表 2 中，计算量角度出发协议进行性能比较分析，可以得出本文协议与文献[14－15]中的协议计算量相当，但本文协议能够弥补文献[14－15]中的协议存在的安全缺陷问题，因此本文协议仍具备一定的使用价值。

4 结 语

标签在其生命周期中，标签的归属者经常发生变更，为确保标签所有权的完整性，设计一种标签所有权转移协议。为能够抵抗攻击者发起的攻击模型，协议采用二次剩余定理对传送的部分信息进行加密，基于数学难题大数分解的二次剩余定理，具备较高的安全性；在保证安全的前提下，为尽可能降低系统的计算量，采用置换再交叉运算对传送的另一部分信息进行加密，置换再交叉运算基于位运算实现，能够极大程度上降低系统的计算量。对协议基于 GNY 逻辑形式化推理，推理出协议具备的安全性；将协议与其他协议进行性能分析，比对出协议具备低计算量的属性。

参 考 文 献

[1] 刘道微，凌捷. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学，2016，43(8)：128－130，158.

[2] 孙子文，李松. 采用 PUF 保护位置隐私的轻量级 RFID 移动认证协议[J]. 计算机科学与探索，2019，13(3)：418－428.

[3] Wang W，Yona Y，Diggavi S N，et al. Design and analysis of stability guaranteed PUFs[J]. IEEE Transactions on Information Forensics and Security，2018，13(4)：978－992.

[4] Jannati H，Bahrak B. Security analysis of an RFID tag search protocol[J]. Information Processing Letters，2016，116(10)：618－622.

[5] 王国伟，贾宗璞，彭伟平. 基于动态共享密钥的移动 RFID 双向认证协议[J]. 电子学报，2017，45(3)：612－618.

[6] Xie R，Ling J，Liu DW. A wireless key generation algorithm for RFID system based on bit operation[J]. International Journal of Network Security，2018，20(5)：938－949.

[7] 徐扬，苑津莎，高会生，等. 基于伪 ID 的 RFID 认证协议及串空间证明[J]. 计算机科学，2017，44(10)：142－146.

[8] Xie R，Jian B Y，Liu D W. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security，2018，20(1)：149－156.

[9] 韦民，孙子文. 基于 PUF 的开环 RFID 所有权转移协议[J]. 信息安全学报，2109，4(4)：19－32.

[10] Sandhya M，Rangaswamy T R. A secure and efficient authentication protocol for mobile RFID systems[J]. Journal of Digital Information Management，2011，9(3)：99－105.

[11] Molnar D，Soppera A，Wagner D. A scalable，delegable pseudonym protocol enabling ownership transfer of RFID tags[C]//12th International Workshop on Selected Areas in Cryptography. Springer，2005：276－290.

[12] 沈金伟，凌捷. 一种改进的超轻量级 RFID 所有权转移协议[J]. 计算机科学，2014，41(12)：125－128.

[13] 苏庆，李倩，张俊源，等. 基于共享密钥的超轻量 RFID 标签所有权转移协议[J]. 计算机工程与应用，2018，54(4)：98－102，121.

[14] 谢锐，郝志峰. 基于二次剩余定理的标签所有权转移协议[J]. 电信科学，2018，34(3)：105－111.

（下转第 349 页）

序列表,这样能更精准地为网站搜索用户服务。

4 结　语

本文提出一种基于实体行为间语义关联分析的用户行为意图挖掘方法。通过实体检索词构建以社交网络用户发布的实时信息以及传统互联网中大量丰富信息作为资源的用户行为样本池,进而在对样本池中潜在行为动词及修饰短语与实体检索词语义关联程度的排序算法中提出以词频统计和语义空间表示为基础的行为样本的显著性、代表性和多样性指标,以迭代的方式实现对用户行为意图的挖掘。实验结果表明,提案方法可以准确地提取丰富且有效的用户行为意图,行为意图排序的 nERR 和 nDCG 指标较 NTCIR-13 AKG 评测的最优结果有显著提升。

参 考 文 献

[1] Joshi D B, Thrall J J. Discovering query intent from search queries and concept networks: US7840538 [P]. 2010-11-23.

[2] Radlinski F, Szummer M, Craswell N. Inferring query intent from reformulations and clicks [C]//Proceedings of the 19th International Conference on World Wide Web. ACM, 2010: 1171 - 1172.

[3] Guo J, Xu G, Cheng X Q, et al. Named entity recognition in query [C]//Proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2009: 267 - 274.

[4] Lin T, Pantel P, Gamon M, et al. Active objects: Actions for entity-centric search [C]//Proceedings of the 21st International Conference on World Wide Web. ACM, 2012.

[5] Hashemi H B, Asiaee A, Kraft R. Query intent detection using convolutional neural networks [C]//International Conference on Web Search and Data Mining, Workshop on Query Understanding, 2016.

[6] Jiang D, Leung W T, Ng W. Query intent mining with multiple dimensions of web search data [J]. World Wide Web, 2016, 19(3): 475 - 497.

[7] Hu J, Wang G, Lochovsky F, et al. Understanding user's query intent with Wikipedia [C]//Proceedings of the 18th International Conference on World Wide Web. ACM, 2009: 471 - 480.

[8] Delli Santi J W, Demir R, Stipp E. System for determining local intent in a search query: US 7788252 [P]. 2010-08-31.

[9] Cheyer A J, Brigham C D, Guzzoni D R. Determining user intent based on ontologies of domains: US8942986 [P]. 2015-01-27.

[10] Xiao L, Wang Y Y, Alex A. Learning query intent from regularized click graphs [C]//Proceedings of the 31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2008: 339 - 346.

[11] Blanco R, Joho H, Jatowt, et al. Overview of Ntcir-13 actionable knowledge graph (akg) task [EB/OL]. [2019-11-22]. http://research.nii.ac.jp/ntcir/workshop/OnlineProceedings13/pdf/ntcir/01-NTCIR13-OV-NAILS-HealyG.pdf.

[12] Rahman M M, Takasu A. TLAB at the NTCIR-13 AKG task [EB/OL]. [2019-11-22]. http://research.nii.ac.jp/ntcir/workshop/OnlineProceedings13/pdf/ntcir/04-NTCIR13-AKG-RahmanM.pdf.

(上接第 332 页)

[12] Cui J, Zhang J, Zhong H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks [J]. Information Sciences, 2018, 451/452: 1 - 15.

[13] Rajput U, Abbas F, Eun H, et al. A hybrid approach for efficient privacy-preserving authentication in VANET [J]. IEEE Access, 2017, 5: 12014 - 12030.

[14] Kamil I A, Ogundoyin S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks [J]. Journal of Information Security and Applications, 2019, 44: 184 - 200.

(上接第 337 页)

[17] 徐扬,苑津莎,高会生,等. 基于伪 ID 的 RFID 认证协议及串空间证明 [J]. 计算机科学, 2017, 44(10): 142 - 146.

[18] 张兴,李畅,韩冬,等. 基于 Hash 轻量级 RFID 安全认证协议 [J]. 计算机工程与设计, 2018, 39(5): 1269 - 1275, 1309.

[19] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols [C]//IEEE Computer Society Symposium in Security and Privacy. IEEE, 1990: 234 - 248.

(上接第 342 页)

[15] 李晓东,徐金成. 基于二次剩余的 RFID 标签所有权动态转移协议 [J]. 计算机应用研究, 2018, 35(11): 3441 - 3444.

[16] Bertoni G, Daemen J, Peeters M, et al. On the indifferentiability of the sponge construction [C]//Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology. ACM, 2008: 181 - 197.