

货运列车车载网络轻量级身份认证协议研究

吕从东¹, 李毓才²

(1. 南京审计大学信息工程学院, 江苏 南京 211815;
2. 铁道部信息中心, 北京 100055)

摘要: 随着铁路运输不断发展, 对货运列车的安全提出了更高要求。目前的地对车安全监控体系由于技术限制, 无法满足列车实时的安全需求。车载传感器可以实时收集车辆信息, 保证列车安全运行。车载传感器通信基础是车载网络。安全车载网络组成的基础是网络节点的身份认证, 提出适用于货运列车车载网络节点身份认证的轻量级身份认证协议, 轻量级身份认证保证所有网络节点均为可信节点, 并且减少与可信第三方的交互。

关键词: 轻量级认证; 身份认证; 货运列车车载网络; 安全网络

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018089

Lightweight authentication protocol for security vehicle network of railway freight train

LYU Congdong¹, LI Yucai²

1. School of Information Engineering, Nanjing Audit University, Nanjing 211815, China
2. Information Technology Centre of Ministry of Railways, Beijing 100055, China

Abstract: With the development of railway transportation, it has put forward higher requirements for the safety of freight train. The present ground vehicle safety monitoring system, due to technical limitations, can't meet the security requirement for real time information report of the train. Vehicular sensor can collect real-time vehicle information, to guarantee the safety of the train. Vehicle network is the basic of the communications between vehicular sensors. The basic of the security vehicle network for the railway freight train is authentication. Lightweight authentication protocol for the security vehicle network was proposed. The protocol can authenticate the network nodes without CA.

Key words: lightweight authentication, authentication, vehicle network for railway freight train, Security network

1 引言

我国铁路货车检修体系是定期修^[1], 即到期车辆无论其运行吨公里数多少、车辆运行状态如

何、轴承技术状态如何, 一律执行定期修程, 这样是明显不合理的。因缺乏对车辆使用情况和状况的精确化掌控, 没能实现最理想的按车辆使用和安全状态进行修理, 这样既不能减少修理经费,

收稿日期: 2018-09-05; 修回日期: 2018-10-20

通信作者: 吕从东, lvcongdong@163.com

基金项目: 国家自然科学基金资助项目(No.61640220); 江苏省高等学校自然科学基金资助项目(No.17KJD520005)

Foundation Items: The National Natural Science Foundation of China (No.61640220), The Natural Science Research Project of Jiangsu Higher Education Institutions (No.17KJD520005)

还影响车辆使用率。

以货运车辆智能化为目标,实现检测装置的车载化,通过车载传感器对货车车辆在装车阶段和运行途中全过程实时、精确采集轴温、声音、重量与超偏载、轮对尺寸和踏伤等信息,再加上周围环境温度、速度等数据;通过车载网络传输并建立地面大数据系统,将传感系统采集充足的数据建立货运车辆全生命期的数据库,对车辆安全隐患数据和运用状况数据进行深度综合分析,提高监测体系的准确率;地面大数据系统可记录车辆及其主要部件运用中的数据,这些数据将为货运车辆实现状态修提供支持,可有效节省车辆维修成本。车载网络可以为铁路货物运输全过程追踪提供准确的信息,提高服务质量和车辆的利用率。由于需要保护列车联网的信息安全以及联网节点的可靠性^[2-3],它需要双向身份验证^[4]并要求使用安全验证协议^[8]。RFID 系统安全认证协议有很强的参考意义^[9-10]。许多其他的研究认证方案,如基于安全增强椭圆曲线密码体系的轻量级认证方案^[12]、基于射频识别的认证方案^[13]、基于组的认证方案^[14]、基于密钥协议的认证方案^[15]不适用于货运列车的认证。目前,车载列车安全检测系统主要面向乘用车,系统之间的通信主要依赖于电缆,并且系统硬件具有足够的电源保护。货运列车没有电力,因此基于 GSM 的联网算法不适用^[5]。在数据收集过程中,它需要受到隐私保护^[6-7],其中大多也是轻量级隐私保护解决方案^[11]。

货运列车车载网络具有以下特点。

1) 网络节点是不断变化。对于货运列车,车厢会根据发送货物的地点编组,所以网络节点也会因为不同的编组产生变化。但在一定范围内,例如一个铁路局内,网络节点又是相对稳定的。

2) 网络节点硬件由蓄电池供电,电力有限。由于货运列车网络的特点 1),车厢间无法使用电线相连,实现无限量供电,只能依据自身特点,使用太阳能、风能、振动能等绿色能源产生电力,供“网络节点”硬件使用。

3) 车载网络节点计算能力有限。由于货运列车网络的特点 2),网络节点的计算能力有限,通常为功率较低的嵌入式硬件。

基于以上货运列车车载网络的特点,本文提出适用于铁路货运列车车载网络节点身份认证的轻量级身份认证协议。该协议使用共享密钥和对称加密算法(对称加密算法相对于公钥加解密算法,计算量小,可以减少网络节点的计算量)进行节点身份认证,减少与可信第三方的通信(与可信第三方通信需要使用卫星通信模块,功率较大,耗电量高)。

2 安全组网中轻量级身份认证协议

列车的每节车厢对应网络中的一个组成节点。在列车编组结束后,列车车厢所组成的网络就固定为线性网络拓扑结构。将这些节点组成一个网络,需要克服 2 个难点:1) 网络节点是否为合法节点,即网络节点身份是否可以认证;2) 网络节点是否为合理节点。网络节点组成网络前提是两节车厢是物理连接的;其次网络节点判断彼此是否属于同一个网络,即两节车厢是否实际被编组为一趟列车(网络节点的合理性相对简单,本文不做进一步讨论)。

信任的获得方法主要有直接和间接 2 种方法。设 A 和 B 以前有过交往,则 A 对 B 的可信度可以通常考察 B 以往的表现来确定。称这种通过直接交往得到的信任值为直接信任值。设 A 和 B 以前没有任何交往,这种情况下, A 可以询问与 B 比较熟悉的实体 C 来获得 B 的信任值,并且要求实体 C 与 B 有过直接的交往经验。称之为间接信任值,或者说是 C 向 A 的推荐信任值。有时,还可能出现多级推荐的情况,这时便产生了信任链。

2.1 列车网络拓扑结构

货运列车网络拓扑结构是线性的,如图 1 所示。

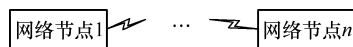


图 1 车载网络系统结构

节点分为 2 种类型:1) 主节点,处于线性网络头位置,负责网络的管理事务;2) 从节点,归属于主节点的管理。所有从节点收集的信息汇总到主节点。每个节点赋予一个独一无二的标识,称之为节点编号(UUID,此处可用车厢号)。

2.2 简单轻量级身份认证协议

前提条件: 网络节点在安装前, 已经由证书颁发机构 (CA, certificate authority) 颁发了数字证书 (digital ID/certificate)。

当网络节点 A 和网络节点 B 首次连接时, A 和 B 之间的身份认证采用第三方认证的方式, 如 PKI 等。由 CA 验证网络节点 A 和网络节点 B 的身份证书和私钥签名, 确认节点身份, 并返回两者的验证结果。在身份认证完成后, A 和 B 进行密钥协商, 协商出的密钥可以作为双方的通信会话密钥或者身份认证密钥使用。

轻量级身份认证协议 (SLAP, simple lightweight authentication protocol) 建立在首轮身份认证成功的基础上。当 A 和 B 再次相连, 使用轻量级身份认证协议, 在无须 CA 参加的情况下完成双向身份认证。该协议实施需要以下前提。

1) 协议以密钥协商生成的共享密钥 K_{AB} 作为身份认证密钥。A 和 B 将 K_{AB} 保存在具有保护措施密钥数据库内, 以 UUID 为索引。

2) 在首次认证成功后双方均保存对方的数字证书 ID_A 和 ID_B 。

3) 首次身份认证完成后必须更新双方的共享秘密 K_{AB} 。在规定的认证密钥有效期或交换一定量的数据之后, A 和 B 之间可以重新进行认证密钥的协商。

轻量级身份认证协议如图 2 所示, 具体描述如下。

1) $B \rightarrow A: \{(R_1, ID_B), K_{AB}\} \Rightarrow_{enc} msg_1$ 。

当 B 与 A 发起连接时, B 生成认证挑战随机数 R_1 , 并使用 B 与 A 的共享认证密钥 K_{AB} 加密得到消息 msg_1 , 然后将消息 msg_1 发送至 A 作为身份认证请求。

2) A 接收到 B 发送的消息 msg_1 后, 首先解密 msg_1 , $\{msg_1, K_{AB}\} \Rightarrow_{dec} \{R_1, ID_B\}$, 验证证书 ID_B , 如果证书验证正确, 生成应答消息 msg_2 , 即 $\{(R_1, R_2, ID_A), K_{AB}\} \Rightarrow_{enc} msg_2$ 。如果证书验证错误或者无法解密, 跳至步骤 7)。

3) $A \rightarrow B: \{(R_1, R_2, ID_A), K_{AB}\} \Rightarrow_{enc} msg_2$ 。

A 向 B 发送身份认证消息 msg_2 , 包含 B 发送过来的随机数 R_1 , A 生成的认证挑战随机数 R_2 , A 的身份证书 ID_A , 并使用 A 与 B 的共享

认证密钥 K_{AB} 加密得到消息 msg_2 , 然后将消息 msg_2 发送至 B 作为响应身份认证请求和身份认证。

4) B 接收到 A 发送的消息 msg_2 后, 首先解密 msg_2 , $\{msg_2, K_{AB}\} \Rightarrow_{dec} \{R_1, R_2, ID_A\}$, 验证证书 ID_A 及先前发送的认证挑战随机数 R_1 , 如果证书及随机数验证正确, 生成应答消息 msg_3 , 即 $\{R_2, K_{AB}\} \Rightarrow_{enc} msg_3$ 。如果证书或随机数验证错误或者无法解密, 跳至步骤 7)。

5) $B \rightarrow A: \{R_2, K_{AB}\} \Rightarrow_{enc} msg_3$ 。

B 向 A 发送 msg_3 , 其包含 A 发送过来的认证挑战随机数 R_2 。

6) A 接收到 B 发送的消息 msg_3 后, 首先解密 msg_3 , $\{msg_3, K_{AB}\} \Rightarrow_{dec} \{R_2\}$, 验证随机数 R_2 , 随机数验证正确, 连接成功。如果随机数验证错误或者无法解密, 跳至步骤 7)。

7) 库中并未存储二者的共享密钥时, 启动远程 CA 身份认证。

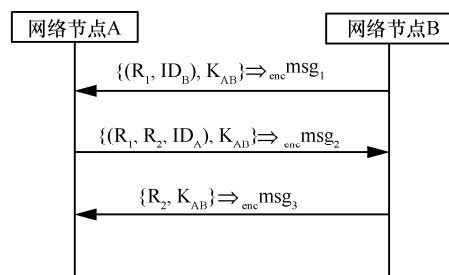


图 2 轻量级身份认证协议

2.3 带信任传递的轻量级认证协议

带信任传递的轻量级认证协议 (SLAPTT, lightweight authentication protocol with trust transitive) 的前提条件和简单轻量级认证协议基本相同。简单轻量级协议要求相连的 2 个网络节点 A 和 B 以前由 CA 进行远程身份认证, 并保存了共享密钥 K_{AB} , 但列车编组是动态变化的, 两节车厢再次相邻的概率相对较小, 而两节车厢同处于一辆车的概率较大。基于这一应用情景, 提出了带信任传递的轻量级协议, 网络节点 A 可以与网络 B 中的任意网络节点进行简单轻量级认证协议认证。网络节点 B 也可以与 A 网络中的任意网络节点进行简单轻量级认证协议认证。

带信任传递的轻量级身份认证协议如图 3 所示, 具体描述如下。

1) $B \rightarrow A: UUID_B \Rightarrow msg_1$ 。

B 将自身的标识号 $UUID_B$ 发送至 A 作为身份

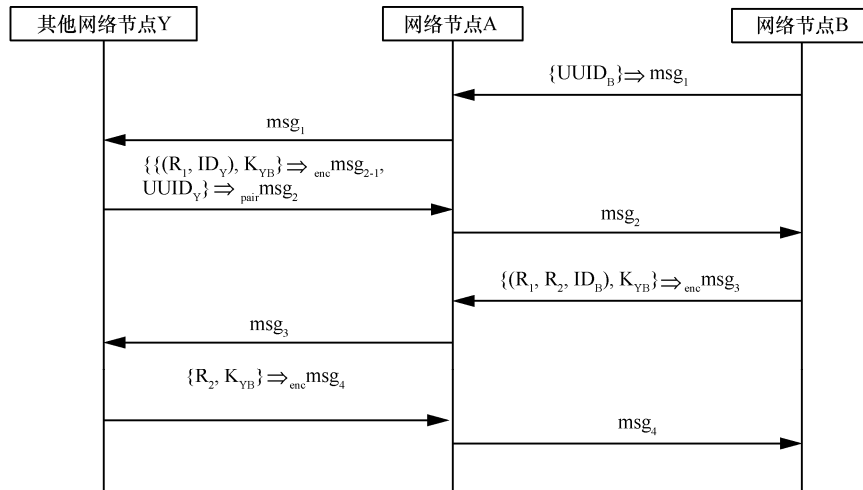


图3 带信任传递的轻量级身份认证协议

认证请求。

2) A 接受消息 msg_1 ，首先在自己的密钥库中查找 $UUID_B$ ，如果 A 存在与 B 的共享密钥 K_{AB} ，直接运行 2.2 节的协议 SLAP。否则 A 将消息 msg_1 向邻居转发，并请求验证。

3) Y 接收到消息 msg_1 ，首先在自己的密钥库中查找 $UUID_B$ ，如果 Y 存在与 B 的共享密钥 K_{YB} ，Y 生成消息 msg_2 。

4) $Y \rightarrow A: \{(R_1, ID_Y), K_{YB}\} \Rightarrow_{enc} msg_{2-1}, UUID_Y \Rightarrow_{pair} msg_2$ 。

Y 生成认证挑战随机数 R_1 ，并使用 Y 与 B 的共享认证密钥 K_{YB} 加密得到消息 msg_{2-1} ，然后将消息 msg_{2-1} 与 Y 的标识号 $UUID_Y$ 结合生成消息 msg_2 ，发送至 A 作为响应 B 身份认证请求的消息。A 接收到 Y 发送的消息 msg_2 后，将 msg_2 转发给 B。

5) B 接收到消息 msg_2 后，首先取出消息中的标识号 $UUID_Y$ ，根据标识号查找密钥库的共享密钥 K_{YB} ，然后解密 msg_2 ， $\{msg_2, K_{YB}\} \Rightarrow_{dec} \{R_1, ID_Y\}$ ，验证证书 ID_Y ，如果证书验证正确，生成应答消息 msg_3 ，即 $\{(R_1, R_2, ID_B), K_{YB}\} \Rightarrow_{enc} msg_3$ 。如果证书验证错误或者无法解密，跳至步骤 10)。

6) $B \rightarrow A: \{(R_1, R_2, ID_B), K_{YB}\} \Rightarrow_{enc} msg_3$ 。

B 向 A 发送身份认证消息 msg_3 ，包含 Y 发送过来的随机数 R_1 ，B 生成的认证挑战随机数 R_2 ，B 的身份证书 ID_B ，并使用 Y 与 B 的共享认证密钥 K_{YB} 加密得到消息 msg_3 ，然后将消息 msg_3 发送至 A 作为响应身份认证请求和身份认证。A 接收到 B 发送的消息 msg_3 后，将 msg_3 转发给 Y。

7) Y 接收到 A 发送的消息 msg_3 后，首先解密 msg_3 ， $\{msg_3, K_{YB}\} \Rightarrow_{dec} \{R_1, R_2, ID_B\}$ ，验证证书 ID_B 及先前发送的认证挑战随机数 R_1 ，证书及随机数验证正确，生成应答消息 msg_4 ，即 $\{R_2, K_{YB}\} \Rightarrow_{enc} msg_4$ 。如果证书或随机验证错误或者无法解密，跳至步骤 10)。

8) $Y \rightarrow A: \{R_2, K_{YB}\} \Rightarrow_{enc} msg_4$ 。

Y 向 A 发送 msg_4 ，其包含 B 发送过来的认证挑战随机数 R_2 。A 接收到 Y 发送的消息 msg_4 后，将 msg_4 转发给 B。

9) B 接收到 A 发送的消息 msg_4 后，首先解密 msg_4 ， $\{msg_4, K_{YB}\} \Rightarrow_{dec} \{R_2\}$ ，验证随机数 R_2 ，随机数验证正确，连接成功。如果随机数验证错误或者无法解密，跳至步骤 10)。

10) 库中并未存储二者的共享密钥时，启动远程 CA 身份认证，认证 A 和 B。

2.4 以主节点为中心的轻量级认证协议

前提条件：网络节点在安装前，已经由证书颁发机构颁发了数字证书。

当网络节点 A 和网络节点 B 首次连接时，认证方式同 2.2 节的首次连接认证。

以主节点为中心的轻量级身份认证协议 (SLAPMN, lightweight authentication protocol by master node) 建立在首轮身份认证成功的基础上。当 A 和 B 再次相连，或者 A 连接 B 所在网络，或者 B 连接 A 所在网络时，实施以主节点为中心轻量级身份认证协议，无须 CA 参加的情况下完成双向身份认证。该协议实施需要以下前提。

1) 协议以密钥协商生成的身份认证密钥

K_{AB} 作为共享密钥。A 和 B 将 K_{AB} 保存在具有保护措施密钥数据库内。

2) 在首次认证成功后双方均保存对方的数字证书 ID_A 和 ID_B 。

3) 首次身份认证完成后必须更新双方的共享秘密 K_{AB} 。在规定的认证密钥有效期或交换一定量的数据之后，A 和 B 之间可以重新进行认证密钥的协商。

4) 当节点加入网络时，其将自身已经认证的节点共享密钥向主节点汇报。

基于主节点的轻量级身份认证协议如图 4 所示，具体描述如下。

1) $M_B \rightarrow B: \{(UID_{i1}, UID_{i2}), \dots, (UID_{n1}, UID_{n2}), UID_{MB}, UID_B\} \Rightarrow msg_1$ 。

主节点 M_3 将存储的标识号对 $\{(UID_{i1}, UID_{i2}), \dots, (UID_{n1}, UID_{n2})\}$ 和自身的标识号 UID_{MB} 发送至 B 作为身份认证请求，B 将消息 msg_1 转发给 A。

2) A 接受消息 msg_1 ，首先在自己的密钥库中查找 UID_B ，如果 A 存在与 B 的共享密钥 K_{AB} ，直接运行 2.2 节的协议 SLAP。否则 A 将消息 msg_1 转发给主节点 M_A ，并请求验证。

3) 主节点 M_A 接收到消息 msg_1 ，首先在自己的密钥库中查找 UID_{MB} ，如果 M_A 存在与 B 的共享密钥 $K_{MA MB}$ ，主节点 M_A 与 M_B 运行 2.2 节的协议 SLAP。 M_A 根据标识对查找密钥库，查找不成功，跳至步骤 10)；查找成功，设为节点 X 和节点 Y，共享密钥为 K_{XY} ，生成消息 msg_2 。

4) $M_A \rightarrow A: \{(R_1, ID_X), K_{XY}\}_{enc} msg_{2-1}, UID_X,$

$UID_Y\}_{pair} msg_2$ 。

M_A 生成认证挑战随机数 R_1 ，并使用 X 与 Y 的共享认证密钥 K_{XY} 加密得到消息 msg_{2-1} ，将消息 msg_{2-1} 与 X、Y 的标识号 UID_X 、 UID_Y 结合生成消息 msg_2 ，然后发送至 A 作为响应 B 身份认证请求的消息。A 接收到 M_A 发送的消息 msg_2 后，将 msg_2 转发给 B。B 接收到消息 msg_2 后，转发给主节点 M_B 。

5) 主节点 M_B 接收到消息 msg_2 后，首先取出消息中的标识号 UID_X 、 UID_Y ，根据标识号查找密钥库的共享密钥 K_{XY} ，然后解密 msg_2 ， $\{msg_2, K_{XY}\} \Rightarrow dec \{R_1, ID_X\}$ ，验证证书 ID_X ，如果证书验证正确，生成应答消息 msg_3 ，即 $\{(R_1, R_2, ID_Y), K_{XY}\} \Rightarrow enc msg_3$ 。如果证书验证错误或者无法解密，跳至步骤 10)。

6) $M_B \rightarrow \{(R_1, R_2, ID_Y), K_{XY}\} \Rightarrow enc msg_3$ 。

主节点 M_B 向 B 发送身份认证消息 msg_3 ，包含 M_A 发送过来的随机数 R_1 ， M_B 生成的认证挑战随机数 R_2 ，Y 的身份证书 ID_Y ，并使用 X 与 Y 的共享认证密钥 K_{XY} 加密得到消息 msg_3 ，然后将消息 msg_3 发送至 A 作为响应身份认证请求和身份认证。B 接收到 M_B 发送的消息 msg_3 后，将 msg_3 转发给 A，A 再将消息 msg_3 转发给主节点 M_A 。

7) 主节点 M_A 接收到 A 发送的消息 msg_3 后，首先解密 msg_3 ， $\{msg_3, K_{XY}\} \Rightarrow dec \{R_1, R_2, ID_Y\}$ ，首先验证证书 ID_Y 及先前发送的认证挑战随机数 R_1 ，证书及随机数验证正确，生成应答消息 msg_4 ，即 $\{R_2, K_{XY}\} \Rightarrow enc msg_4$ 。如果证书或随机

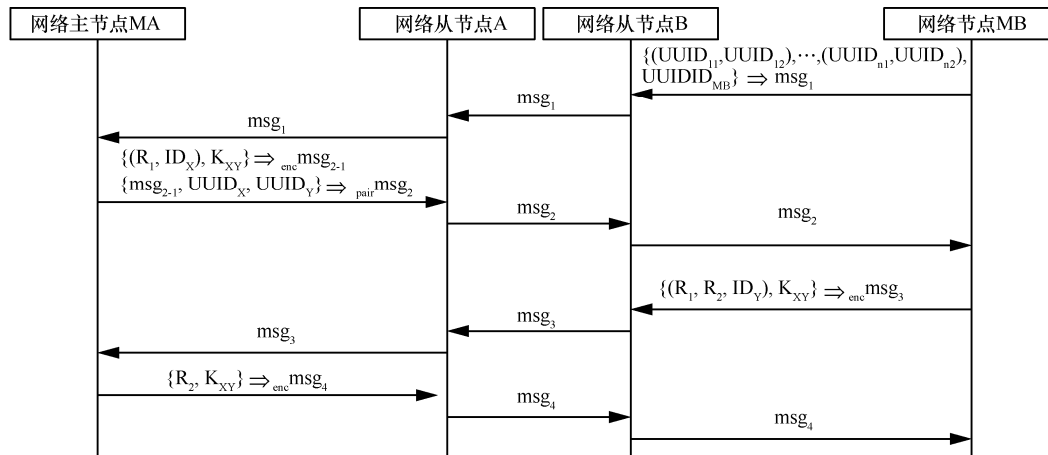


图 4 基于主节点的轻量级身份认证协议

验证错误或者无法解密, 跳至步骤 10)。

8) $M_A \rightarrow A: \{R_2, K_{XY}\} \Rightarrow_{enc} msg_4$ 。

主节点 M_A 向 A 发送 msg_4 , 其包含 B 发送过来的认证挑战随机数 R_2 。A 接收到 M_A 发送的消息 msg_4 后, 将 msg_4 转发给 B, B 再将消息 msg_4 转发给 M_B 。

9) M_B 接收到 B 发送的消息 msg_4 后, 首先解密 msg_4 , $\{msg_4, K_{XY}\} \Rightarrow_{dec} \{R_2\}$, 验证随机数 R_2 , 随机数验证正确, 连接成功。如果随机数验证错误或者无法解密, 跳至步骤 10)。

10) 库中并未存储二者的共享密钥时, 启动远程 CA 身份认证, 认证 A 和 B。

3 安全与性能分析

3.1 SLAP 的形式化分析

根据第 2 节对 SLAP 的描述, 建立协议的理想化模型。

- 1) $B \rightarrow A: \{R_1, B\} K_{AB}$ 。
- 2) $A \rightarrow B: \{R_1, A\} K_{AB}$ 。
- 3) $B \rightarrow A: \{R_2\} K_{AB}$ 。

下面考虑这个协议是否可以安全的双向身份认证。如果无论何时响应者得到发起者知道共享密钥 K_{AB} 的证据 (A 接收到 R_2), 发起者也一定得到了响应者知道共享密钥 K_{AB} 的证据 (B 接收到 R_1), 那么协议实现了发起者和响应者双向身份的认证。

SLAP 的 CryptoSPA 描述如图 5 所示。

$B(R_1, K_{AB}) \underline{\text{def}} \bar{c}_1 \text{ msg}_1 \cdot c_2(v) \cdot \text{check}_{\text{msg}_2}(v) \cdot \bar{c}_1 \text{ msg}_3 \cdot \text{done}$
$A(R_2, K_{AB}) \underline{\text{def}} \bar{c}_1(q) \cdot \text{check}_{\text{msg}_1}(q) \cdot c_2 \text{ msg}_2 \cdot c_1(u) \cdot \text{check}_{\text{msg}_3}(u) \cdot \text{done}$
$P(n, m) \underline{\text{def}} B(n, K_{AB}) \ A(m, K_{AB})$
其中: $\bar{c}_1 \text{ msg}_1 = [\langle R_1, B \rangle, K_{AB}] \Rightarrow_{enc} p \bar{c} p$ $\text{check}_{\text{msg}_1}(q) = [\langle q, K_{AB}^{-1} \rangle \Rightarrow_{dec} i] [i \Rightarrow_{fst} s] [i \Rightarrow_{snd} r] \quad [r=B]$ $\bar{c}_2 \text{ msg}_2 = [\langle s, R_2, A \rangle, K_{AB}] \Rightarrow_{enc} t \bar{c} t$ $\text{check}_{\text{msg}_2}(v) = [\langle v, K_{AB}^{-1} \rangle \Rightarrow_{dec} i] [i \Rightarrow_{fst} s] [i \Rightarrow_{snd} d] [s \Rightarrow_{fst} z] [s \Rightarrow_{snd} x] \quad [z=R_1] [d=A]$ $\bar{c}_1 \text{ msg}_3 = [x, K_{AB}] \Rightarrow_{enc} y \bar{c} y$ $\text{check}_{\text{msg}_3}(u) = [\langle u, K_{AB}^{-1} \rangle \Rightarrow_{dec} o] [o=R_2]$

图 5 SLAP 的 CryptoSPA 描述

其中, $c_1, c_2 \in \text{puAct}$, $\text{done} \in \text{prAct}$ 。利用 Casper^[23]和 FDR^[24]验证该协议安全性, Casper 文

件参见附录。验证结果如图 6 所示。

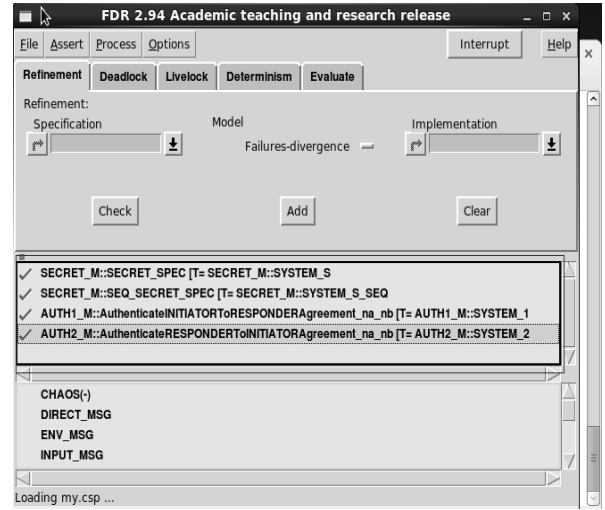


图 6 FDR 验证分析结果

敌手满足 Dolev-Yao 模型^[25], 图 6 中有 4 条验证, 均没有发现任何攻击, 表明在认证过程中, 随机消息 R_1 、 R_2 是安全的, 没有泄露加密信息; B 对 A、A 对 B 实现了双向身份认证。

3.2 SLAPTT 的形式化分析

根据第 2 节对 SLAPTT 的描述, 建立协议的理想化模型。

- 1) $B \rightarrow A: \text{UID}_B \text{ msg}_1$;
- 2) $A \rightarrow Y: \text{msg}_1$;
- 3) $Y \rightarrow A: \{ \{ (R_1, \text{ID}_Y), K_{YB} \} \Rightarrow_{enc} \text{msg}_{2-1}, \text{UID}_Y \} \Rightarrow_{pair} \text{msg}_2$;
- 4) $A \rightarrow B: \text{msg}_2$;
- 5) $B \rightarrow A: \{ (R_1, R_2, \text{ID}_B), K_{YB} \} \Rightarrow_{enc} \text{msg}_3$;
- 6) $A \rightarrow Y: \text{msg}_3$;
- 7) $Y \rightarrow A: \{ R_2, K_{YB} \} \Rightarrow_{enc} \text{msg}_4$;
- 8) $A \rightarrow B: \text{msg}_4$ 。

下面考虑这个协议是否可以安全的双向身份认证。如果无论何时响应者所在网络有节点得到发起者知道共享密钥 K_{YB} 的证据 (Y 接收到 R_1), 发起者所在网络有节点也一定得到了响应者知道共享密钥 K_{YB} 的证据 (B 接收到 R_2), 那么协议实现了发起者和响应者双向身份的认证。

SLAPTT 的 CryptoSPA 描述如图 7 所示。

其中, $c_1, c_2, c_3, c_4 \in \text{puAct}$, $\text{done} \in \text{prAct}$ 。

3.3 SLAPMN 的形式化分析

根据第 2 节对 SLAPMN 的描述, 建立协议的理想化模型。

$B(msg, R_2) \stackrel{\text{def}}{=} \bar{c}_1 \text{ msg}_1 \cdot c_4(u) \cdot \text{check}_{\text{msg}_2}(u) \cdot \bar{c}_1 \text{ msg}_3 \cdot c_4(t) \cdot \text{check}_{\text{msg}_4}(t) \overline{\text{done}}$
$A \stackrel{\text{def}}{=} c_1(q) \cdot \bar{c}_2 q \cdot c_3(u) \cdot \bar{c}_4 u \cdot c_1(s) \cdot \bar{c}_2 s \cdot c_3(t) \cdot \bar{c}_4 t \overline{\text{done}}$
$Y(R_2) \stackrel{\text{def}}{=} c_2(q) \cdot \text{check}_{\text{msg}_1}(q) \cdot \bar{c}_3 \text{ msg}_2 \cdot c_2(s) \cdot \text{check}_{\text{msg}_3}(s) \cdot \bar{c}_3 \text{ msg}_4 \overline{\text{done}}$
$P(n, m) \stackrel{\text{def}}{=} B(msg, R_2) \ A \ Y(R_2)$
其中: $\bar{c}_1 \text{ msg}_1 = [\text{msg} \Rightarrow p] \bar{c} p$ $\text{check}_{\text{msg}_1}(q) = [\text{msg} \Rightarrow_{\text{find}} i]$ $\bar{c}_2 \text{ msg}_2 = [\{ \langle (R_1, Y), i \rangle \Rightarrow_{\text{enc}} p_1, \text{UUID}_Y \} \Rightarrow_{\text{pair}} p] \bar{c} p$ $\text{check}_{\text{msg}_2}(u) = [\text{UUID}_Y \Rightarrow_{\text{find}} k][\langle u, k \rangle \Rightarrow_{\text{dec}} j][j \Rightarrow_{\text{fst}} s][j \Rightarrow_{\text{snd}} r][r = Y]$ $\bar{c}_1 \text{ msg}_3 = [(s, R_2, B), k \Rightarrow_{\text{enc}} t] \bar{c} t$ $\text{check}_{\text{msg}_3}(s) = [\langle s, i \rangle \Rightarrow_{\text{dec}} m][m \Rightarrow_{\text{fst}} s][m \Rightarrow_{\text{snd}} d][s \Rightarrow_{\text{fst}} z][s \Rightarrow_{\text{snd}} x][z = R_1][d = B]$ $\bar{c}_3 \text{ msg}_4 = [\langle x, i \rangle \Rightarrow_{\text{enc}} y] \bar{c} y$ $\text{check}_{\text{msg}_4}(t) = [\langle t, k \rangle \Rightarrow_{\text{dec}} o][o = R_2]$

图 7 SLAPTT 的 CryptoSPA 描述

- 1) $M_B \rightarrow B: \{(\text{UUID}_{11}, \text{UUID}_{12}), \dots, (\text{UUID}_{n1}, \text{UUID}_{n2}), \text{UUID}_{M_B}, \text{UUID}_B\} \Rightarrow \text{msg}_1;$
- 2) $B \rightarrow A: \text{msg}_1;$
- 3) $A \rightarrow M_A: \text{msg}_1;$
- 4) $M_A \rightarrow A: \{ \{ (R_1, \text{ID}_X), K_{XY} \} \Rightarrow_{\text{enc}} \text{msg}_{2-1}, \text{UUID}_X, \text{UUID}_Y \Rightarrow_{\text{pair}} \text{msg}_2;$
- 5) $A \rightarrow B: \text{msg}_2;$
- 6) $B \rightarrow M_B: \text{msg}_2;$
- 7) $M_B \rightarrow B: \{ (R_1, R_2, \text{ID}_Y), K_{XY} \} \Rightarrow_{\text{enc}} \text{msg}_3;$
- 8) $B \rightarrow A: \text{msg}_3;$
- 9) $A \rightarrow M_A: \text{msg}_3;$
- 10) $M_A \rightarrow A: \{ R_2, K_{XY} \} \Rightarrow_{\text{enc}} \text{msg}_4.$
- 11) $A \rightarrow B: \text{msg}_4;$
- 12) $B \rightarrow M_B: \text{msg}_4.$

下面考虑这个协议是否可以安全的双向身份认证。如果无论何时响应者的主节点得到发起者主节点知道共享密钥 K_{XY} 的证据 (M_A 接收到 R_1), 发起者的主节点也一定得到了响应者的主节点知道共享密钥 K_{XY} 的证据 (M_B 接收到 R_2), 那么协议实现了发起者和响应者双向身份的认证。

轻量级身份认证协议的 CryptoSPA 描述如图 8 所示。

其中, $c_1, c_2, c_3, c_4, c_5, c_6 \in \text{puAct}$, $\text{done} \in \text{prAct}$ 。

3.4 安全性能分析

在 SLAP 协议中

- 1) B 和 A 拥有首轮身份认证之后的共享认证密钥 K_{AB} 。在认证过程中, 利用共享密钥 K_{AB} 、

$M_B(msg, R_2) \stackrel{\text{def}}{=} \bar{c}_1 \text{ msg}_1 \cdot c_5(u) \cdot \text{check}_{\text{msg}_2}(u) \cdot \bar{c}_1 \text{ msg}_3 \cdot c_6(t) \cdot \text{check}_{\text{msg}_4}(t) \overline{\text{done}}$
$B \stackrel{\text{def}}{=} c_1(q) \cdot \bar{c}_2 q \cdot c_3(u) \cdot \bar{c}_4 u \cdot c_1(s) \cdot \bar{c}_2 s \cdot c_3(t) \cdot \bar{c}_6 t \overline{\text{done}}$
$A \stackrel{\text{def}}{=} c_2(q) \cdot \bar{c}_3 q \cdot c_4(u) \cdot \bar{c}_5 u \cdot c_2(s) \cdot \bar{c}_3 s \cdot c_4(t) \cdot \bar{c}_5 t \overline{\text{done}}$
$M_A(R_2) \stackrel{\text{def}}{=} c_3(q) \cdot \text{check}_{\text{msg}_1}(q) \cdot \bar{c}_4 \text{ msg}_2 \cdot c_3(s) \cdot \text{check}_{\text{msg}_3}(s) \cdot \bar{c}_4 \text{ msg}_4 \overline{\text{done}}$
$P(n, m) \stackrel{\text{def}}{=} M_B(msg, R_2) \ A \ B \ M_A(R_2)$
其中: $\bar{c}_1 \text{ msg}_1 = [\text{msg} \Rightarrow p] \bar{c} p$ $\text{check}_{\text{msg}_1}(q) = [\text{msg} \Rightarrow_{\text{find}} i]$ $\bar{c}_4 \text{ msg}_2 = [\{ \langle (R_1, Y), i \rangle \Rightarrow_{\text{enc}} p_1, \text{UUID}_X, \text{UUID}_Y \} \Rightarrow_{\text{pair}} p] \bar{c} p$ $\text{check}_{\text{msg}_2}(u) = [\langle \text{UUID}_X, \text{UUID}_Y \rangle \Rightarrow_{\text{find}} k][\langle u, k \rangle \Rightarrow_{\text{dec}} j][j \Rightarrow_{\text{fst}} s][j \Rightarrow_{\text{snd}} r][r = X]$ $\bar{c}_1 \text{ msg}_3 = [(s, R_2, B), k \Rightarrow_{\text{enc}} t] \bar{c} t$ $\text{check}_{\text{msg}_3}(s) = [\langle s, i \rangle \Rightarrow_{\text{dec}} m][m \Rightarrow_{\text{fst}} s][m \Rightarrow_{\text{snd}} d][s \Rightarrow_{\text{fst}} z][s \Rightarrow_{\text{snd}} x][z = R_1][d = B]$ $\bar{c}_4 \text{ msg}_4 = [\langle x, i \rangle \Rightarrow_{\text{enc}} y] \bar{c} y$ $\text{check}_{\text{msg}_4}(t) = [\langle t, k \rangle \Rightarrow_{\text{dec}} o][o = R_2]$

图 8 SLAPMN 的 CryptoSPA 描述

认证双方生成的随机数 R_1 、 R_2 以及认证双方的平台证书 ID_A 生成认证消息 $V_1 = \{R_1, ID_B\}_{K_{AB}}$, $V_2 = \{R_1, R_2, ID_A\}_{K_{AB}}$, $V_3 = \{R_2\}_{K_{AB}}$ 。认证消息 V_1 、 V_2 、 V_3 作为认证双方的签名, 为验证双发提供身份认证证据。

2) 双方的认证消息 V_1 、 V_2 、 V_3 的新鲜性可以通过随机数 R_1 、 R_2 验证, 保证本次消息的认证值和上次认证值没有关系, 可以有效抵抗重放攻击。

在 SLAPTT 协议中, B 和 Y 拥有首轮身份认证之后的共享认证密钥 K_{YB} , 其他步骤与 SLAP 类似。

在 SLAPMN 协议中, M_B 和 M_A 拥有网络节点 X 和网络节点 Y 身份认证之后的共享认证密钥 K_{XY} 。其他步骤与 SLAP 类似。

为有效说明轻量级身份认证协议的性能优势, 将首次接入时采用的原 TCA 身份认证^[26]与 SLAP、SLAPTT 和 SLAPMN 协议进行分析对比, 如表 1 所示。TCA 首次身份认证协议中只分析身份认证协议本身, 不包含密钥协商部分。发送或接受 1 次消息为 1 次交换。轻量级身份认证协议与原协议相比, 在完成相同任务的前提下, 通信和计算效率优势明显。

其中, A 和 B 为参加身份认证的双方, PM 为 TCA 中的策略管理器, Y 为网络中可信任节点, M_A 和 M_B 为网络的主节点。S 为 RSA-1024 bit 签名运算; V 为 RSA-1024 bit 验证签名运算; E 为 128 bit 分组加密运算; D 为 128 bit 分组解密运算。

1) 通信负载

SLAP 数据交换由 5 次降为 3 次, 在交互步骤减少的同时能完全实现 A 与 B 双向的身份认证, 数据交换次数减少直接导致身份认证协议性能的提高; SLAPTT 和 SLAPMN 协议的数据交换

分别为 8 次和 12 次, 但它们提高了认证的概率, 进一步减少可信第三方参与的概率; SLAP、SLAPTT 和 SLAPMN 将大量的公私钥运算改为加解密运算, 在协议执行过程中占用更少的网络通信带宽, 提高了协议的可用性, 并且这 3 个协议都不需要可信第三方参与。

2) 计算负载

与原 TCA 身份认证协议相比, SLAP、SLAPTT 和 SLAPMN 协议的计算量更低。B 和 A 的 1 次签名运算和 1 次验证签名运算降低为 1 次加密运算和 1 次解密运算, 减少了可信第三方的参与, 性能优势明显。

4 结束语

本文提出了 3 种身份认证协议: SLAP、SLAPTT 和 SLAPMN。它们适用类似于货运列车车载网络这样的环境, 网络中的节点可能在断开后的一段时间内重新连接在一起。利用初次基于可信第三方的身份认证时协商的共享密钥, 再次身份认证时就不需要可信第三方的参与。SLAP、SLAPTT 和 SLAPMN 均使用对称加解密算法进行身份认证, 减少计算复杂度, 使认证协议更加高效。

附录

```
#Free variables
A, B : Agent
na, nb : Nonce
SK : Agent ->SecretKey
InverseKeys = (SK, SK)
#Processes
INITIATOR(A,na) knows SK(A)
```

表 1 身份认证协议对比

协议	数据交换次数	计算量				
		A	B	PM	M_A (Y)	M_B
TCA 身份认证协议	5	1S+1V	1S+1V	1S+1V	0	0
SLAP	3	1E+1D	1E+1D	0	0	0
SLAPTT	8	0	1E+1D	0	1E+1D	0
SLAPMN	12	0	0	0	1E+1D	1E+1D

RESPONDER(B,nb) knows SK(A)

#Protocol description

0. $\rightarrow A : B$

1. $A \rightarrow B : \{na, A\} \{SK(A)\}$

2. $B \rightarrow A : \{na, nb, B\} \{SK(A)\}$

3. $A \rightarrow B : \{nb\} \{SK(A)\}$

#Specification

Secret(A, na,[B])

Secret(B, nb,[A])

Agreement(A,B,[na,nb])

Agreement(B,A,[na,nb])

#Actual variables

Alice, Bob, Mallory : Agent

Na, Nb, Nm : Nonce

#Functions

symbolic SK, SK

#System

INITIATOR(Alice, Na)

RESPONDER(Bob, Nb)

#Intruder Information

Intruder = Mallory

IntruderKnowledge = {Alice, Bob, Mallory, Nm, SK(Mallory)}

参考文献:

- [1] 赵长波, 陈雷. 铁路货车安全监测与应用概论[M]. 中国铁道出版社, 2010.
- [2] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学: 技术科学, 2007, 37(2): 129-150.
- [3] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010(2): 139-166.
- [4] 刘丹, 郭丽敏, 俞军, 等. 一种基于 SRAM PUF 的安全双向认证协议[J]. 密码学报, 2017, 4(4): 360-371.
- [5] 孙斌, 丁建文, 蒋文怡, 等. 面向西部铁路基于 GSM-R 的车-地数据传输方案[J]. 铁道通信信号, 2017, 53(S1).
- [6] 马鑫迪, 李辉, 马建峰, 等. 轻量级位置感知推荐系统隐私保护框架[J]. 计算机学报, 2017, 40(5): 1017-1030.
- [7] XIN Y, FENG X, LI T. Position-dependent lightweight Sybil attack detection method in VANET[J]. Journal of Communications, 2017, 38(4): 110-119.
- [8] 魏国珩, 秦艳琳, 张焕国. 基于 ECC 的轻量级射频识别安全认证协议[J]. 华中科技大学学报(自然科学版), 2018(1): 49-52.
- [9] 杨玉龙, 彭长根, 郑少波, 等. 基于移动智能终端的超轻量级移动 RFID 安全认证协议[J]. 信息网络安全, 2017(5): 22-27.
- [10] 夏戈明, 史立哲, 周文, 等. 轻量级 RFID 双向通信认证协议优化方案[J]. 信息网络安全, 2014(2): 58-62.
- [11] ABDALLAH A, SHEN X S. Lightweight authentication and privacy-preserving scheme for V2G connections[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2615-2629.
- [12] ABBASINEZHAD-MOOD D, NIKOOGHADAM M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications[J]. Future Generation Computer Systems, 2018, 84: 47-57.
- [13] ARAFIM M T, GAO M, QU G. VOLT: Voltage over-scaling based lightweight authentication for IoT applications[C]//Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific. IEEE, 2017: 336-341.
- [14] LAI C, LU R, ZHENG D, et al. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications[J]. Computer Networks, 2016, 99: 66-81.
- [15] REDDY A G, YOON E J, DAS A K, et al. Lightweight authentication with key-agreement protocol for mobile network environment using smart cards[J]. IET Information Security, 2016, 10(5): 272-282.

[作者简介]



吕从东 (1987-), 男, 江苏连云港人, 博士, 南京审计大学讲师, 主要研究方向为信息安全。

李毓才 (1963-), 男, 北京人, 铁道部信息中心高级工程师, 主要研究方向为信息安全。