火灾报警系统数据输出协议的形式化分析①

李志刚

(公安部 沈阳消防研究所, 沈阳 110034)

摘 要: 火灾自动报警系统数据输出通信协议的理解和实现直接影响到通讯双方的兼容性. 本文结合协议的应用环境和功能需求, 利用形式化分析方法对协议进行剖析, 给出协议的 Petri 网模型, 将标准中隐含的、影响兼容性的要求明确化, 探讨该协议的网络化应用应该注意的问题.

关键词: 消防; 火灾自动报警; 通信协议; 形式化分析

Analysis and Discussion about Fire Alarm System Output Protocol

LI Zhi-Gang

(Shenyang Fire Research Institute of MPS, Shenyang 110034, China)

Abstract: Understanding and implementation of automatic-fire-alarm-system's output communication protocol can impact on two sides' communication compatibility. This paper introduces the protocol's environment and functional requirements, analyzes it using formal analysis method, gives its Petri net model, states the requirements implied in the protocol and affecting compatibility. It makes some suggestions on using the protocol for networked applications.

Key words: fire safe; fire auto alarm; communication protocol; formal analysis

《火灾自动报警系统数据输出通信协议》(后文简称 FASP, Fire Alarm System Protocol)主要解决火灾自动报警系统与其他信息系统之间的信息共享问题[1], 目前该协议正在报批国家标准. 标准文稿在描述通讯协议时, 以文字语言描述为主, 容易出现理解上的歧义, 而形式化分析方法在指导协议实现方面具有消除歧义的作用[2]. 本文用形式化分析的方法, 对该协议进行剖析, 以便在协议实现过程中避免容易出现的问题.

1 协议环境分析

结合现阶段的消防电子产品现状[3-5]以及物联网发展趋势, FASP 可能会被用于多种设备, 其应用环境如图 1 所示.

火灾自动报警系统控制器, 泛指火灾自动报警系统内火灾报警控制器、消防联动控制器、可燃气体报警控制器、电气火灾监控设备等各类控制器(后文统称控制器), 能够采集控制器所连接的火灾探测器、联动执行器等各类消防设施的运行状态信息, 当消防设备的工作状态发生变化时(如火警、鼓掌、联动设备起动), 通过数字通讯接口输出这些状态变化信息.

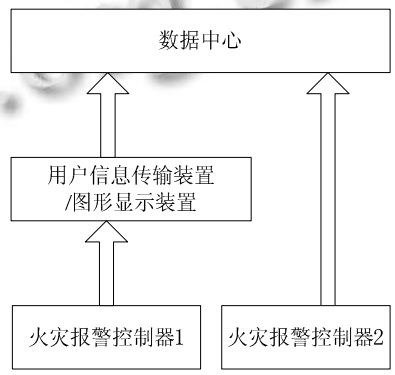

图 1 FASP 的应用环境

用户信息传输装置, 除了具有消防远程监控相关的功能外, 还收集控制器输出的消防设施状态信息, 然后传输给一个或多个数据中心; 需要将自身的工作

①基金项目:国家"十二五"科技支撑计划(2012BAK21B03)
收稿时间:2014-03-11;收到修改稿时间:2014-04-10

状态告知数据中心; 需要接收并完成数据中心下达的各种指令. 图像显示装置与此类似.

数据中心, 收集各种消防设施状态信息, 实时监测联网范围内的消防设施的运行状态, 提高消防部队对突发事件的响应速度, 并利用计算机强大的数据处理能力, 对这些信息进行汇总、分析等, 以适用于计算机、互联网处理的方式二次发布, 实现信息共享.

2 协议网络模型分析

将图 1 所示的应用环境, 抽象成如图 2 所示的通讯网络模型图为例, 介绍控制器节点、传输节点、中心节点所组成的通讯网络及相互之间的连接关系.

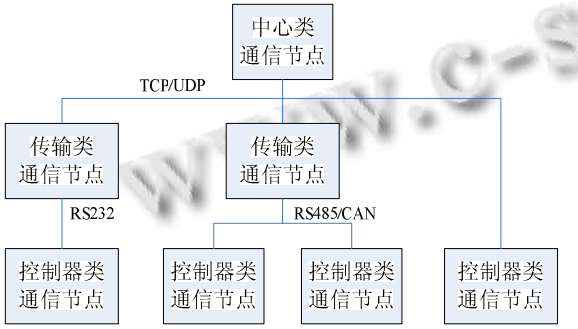

图 2 火灾自动报警系统数据输出协议网络模型例图

控制器节点代表火灾自动报警系统的各类控制器, 其输出协议遵循《火灾报警控制器数据输出协议》, 该标准未限定控制器的连接对象, 除了本文所述的用户信息传输装置、图形显示装置、数据中心之外, 还可与其他消防系统直接通讯. FASP 规定控制器应采用 RS232、TCP、UDP 接口, 但在实践过程中, RS485、CAN 等总线式接口不可避免.

传输节点代表用户信息传输装置和图形显示装置. 仅就通讯方式而言, 传输节点相当于一种通讯适配器, 将 RS232、RS485、CAN 等近距离通讯方式转换成以太网、数字无线等 TCP/UDP 网络方式, 进行远距离传输.

中心节点采用 TCP/UDP 协议接收控制器节点直接发送的或经传输节点转发的消防设施状态信息. 多个中心节点之间还可再次组网, 该网络不在本文讨论范围内.

3 协议功能需求分析

3.1 连接控制

控制器节点与其连接对象之间的通讯连接建立后, 双方均不主动断开, 通讯连接断开视为通讯故障, 应设法重新建立连接.

3.2 通信方式

控制器节点与其连接对象之间的连接方式多样, 可依据物理介质的不同, 选择全双工/半双工传输方式.

3.3 数据发送与接收

消防设施状态信息长度较短, 一般不多于 50 字节, IP 协议的 MTU(最大传输单元)因网络介质的不同介于 576～1480 字节之间, 为了优化通信效率, 在保证同一个状态信息不被分割到两次发送/接收过程的前提下, 可在单次发送/接收过程中, 整合尽可能多同一类型状态信息, 正因于此, 数据包长度是随机可变的, 要求 FASP 协议提供分段/并段服务.

3.4 数据安全与可靠

在整个网络中, 应优先传输手动报警、火警等重要信息, 并保证这些信息的可靠送达, 即使在通讯故障的情况下, 也不应丢弃重要信息(比如首次火警信息); 通信恢复后, 须重传这些信息. 网络对信息的实时性要求宽松, 一般在秒级.

由于协议双方的计算能力和内存资源各不相同, 协议应建立流量控制机制. 如有必要, 可通过丢弃不重要的信息来减轻拥塞.

3.5 寻址

网络中所传输的消防设施状态信息, 应能够区分信息来源、信息目的地. 因此, 控制器节点、传输节点、中心节点都应具有独立的地址. 整个通讯网络要求双向可寻址, 即控制器节点发出的信息应能够通过网络送达中心节点; 中心节点的控制命令应能送达传输节点, 应能直接送达或经传输节点送达控制器节点. 传输节点采用 RS485/CAN 总线与多个控制器节点相连时, 需提供地址复用/解复用服务.

4 协议的形式化分析

4.1 协议结构

FASP 的协议结构如图 3 所示, 各域的含义如下:

STA 为启动符; SEQ 为流水号; VER 为协议版本; TIM 为时间; SRC 为源地址; DST 为目的地址; LEN 为应用数据单元的长度; CMD 为命令字节; DAT 为应用数据单元; FCS 是 CRC-16 循环校验码; END 为结束符. FASP 为 STA 和 END 提供了转义机制.

FASP 的数据包为变长数据包, DAT 域可填入一个

或多个消防设施状态信息或命令, LEN 域为 DAT 域的字节长度. 除 DAT 域长度不定之外, 其他域长度固定不变.

图 3　FASP 数据包结构图

由于物理介质的多样性、加之火灾报警控制器多为嵌入式系统, 运算能力和内存资源有限, FASP 未对建立连接过程和断开连接过程做出要求, 只对建立连接后的数据传输进行要求, FASP 为上层应用提供了 1 种原语动作: 数据传输 DATA, 该原语为证实型, 包括 5 种原语类型, 详见表 1.

表 1　FASP 服务原语

发送方 服务原语	接收方 服务原语	CMD 值	CMD 定义	CMD 说明
DATA.out_request	DATA.out_indication	2	发送	发送火灾自动报警系统火灾报警、运行状态等信息
DATA.out_ack_response	DATA.out_ack_confirm	3	确认	对发送信息正确接收的回答
DATA.in_request	DATA.in_indication	4	请求	查询火灾自动报警系统的火灾报警、运行状态等信息
DATA.in_ack_response	DATA.in_ack_confirm	5	应答	返回查询的信息
DATA.out_nack_response/ DATA.in_nack_response	DATA.out_nack_confirm/ DATA.in_nack_confirm	6	否认	对发送或请求信息未正确接收的回答

4.2 服务原语和原语时序

不难看出, 数据输出接口具有两个半双工通道: 外向通道和内向通道. 两个通道各自独立, 通讯双方在这两个通道上各自独立地采用停等式 ARQ(Auto Repeat reQuest, 自动重发)协议为对方提供证实. 本协议原语时序可参照停等式 ARQ 的, 不再赘述.

本文建议, 即便数据包无校验和错误, 当出现以下异常情况时, 接收方应视为未能“正确接收”信息, 应发出否认证实(CMD=6), 令发送方能够启动故障处理机制.

①数据包版本错误, 比如双方 VER 不匹配;

②数据包地址错误, 比如 SRC、DST 无法寻址;

③不支持的自定义 CMD 命令.

4.3 PDU(协议数据单元)和 PDU 交换时序

FASP 的 PDU 为 DAT 域. DAT 域采用 TCL(DAT.Type + DAT.Count + DAT.List)三段式结构提供分段/并段服务.

外向通道主要供控制器向连接对象“主动”推送自身或所连接设备的“状态变化”. 外向通道涉及 PDU 的异常包括:

① 连接对象不兼容 DAT.Type;

② 连接对象不兼容系统类型、设备类型、状态代码等.

内向通道主要供连接对象查询控制器或后者所连接设备的“当前状态”. 内向通道涉及 PDU 的异常包括:

① 控制器不兼容的 DAT.Type;

② 控制器不兼容或不存在的系统类型、设备类型;

③ 控制器不存在系统地址、设备地址;

④ 控制器执行命令时长过长, 超过连接对象的等待时长.

对于 PDU 异常情况的处理, 有两种处理策略. 两种方式各有利弊, 控制器和连接对象可根据自身产品特性灵活选择.

第一种是畅通式. 接收方发现异常后, 发出确认证实, 然后直接丢弃或转发收到的信息, 保持通道的畅通. 优点是通道畅通有利于信息的快速传输; 缺点是发送方能够证实发出的信息被接收方正确接收, 但不能证实被后者正确处理.

第二种是堵塞式. 接收方发现异常后, 发出否认证实或不证实, 堵塞通道, 令发送方启动故障处理机制. 优点是通道堵塞有利于兼容性问题的早期发现; 缺点是为了避免出现通道堵塞需要完全兼容不同类别的所有连接对象.

外向通道正常通讯时的 PDU 交换时序, 跟连接对象采用畅通式异常处理策略的时序相同, 见图 4; 堵

塞式策略的时序见图 5.

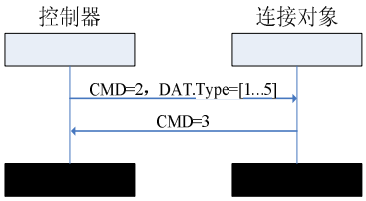

图 4 外向通道正常情况(及畅通式策略)的 PDU 交换时序

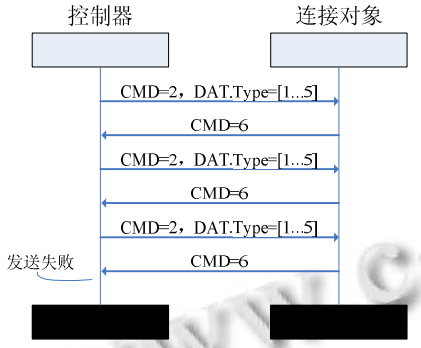

图 5 外向通道堵塞式策略的 PDU 交换时

内向通道正常通讯情况、畅通式策略、堵塞式策略的 PDU 交换时序分别见图 6、图 7、图 8.

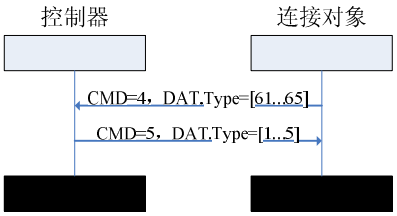

图 6 内向通道正常情况的 PDU 交换时序

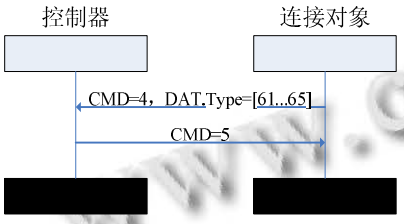

图 7 内向通道畅通式策略的 PDU 交换时序

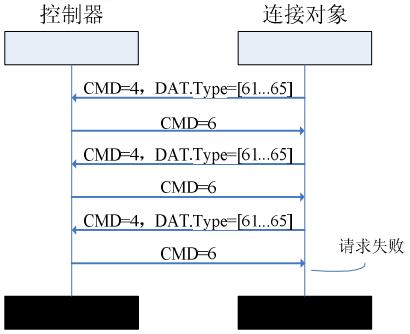

图 8 内向通道堵塞式策略的 PDU 交换时序

4.4 协议事件

FASP 的事件，除了 DATA 服务原语外，还有用于重发机制的定时器信号 TM1，等待接收方证实的最长时间.

4.5 协议变量

FASP 用到的变量是 SendTimes，数值型，取值范围 1 到 3，用来记录每个数据包的发送次数.

4.6 协议的 Petri 网模型

结合前面的论述，以内向通道为例，建立如图 9 所示的 Petri 网模型. 其中：P1~P4 为发送方的状态，P5~P7 为传输通道的状态，P8~P9 为接收方的状态，T1~T14 为各状态之间变迁，初始状态下，P1、P8 拥有初始标记，即发送方和接收方均处于就绪态.

各状态及变迁的具体含义如下:

P1: 发送方就绪，等待上层应用给出新“命令”;

P2: 发送方等待对方证实(确认证实或否认证实);

P3: 发送方收获对方“否认证实”后的处理;

P4: 发送方收获对方“确认证实”后的处理;

P5: 通道正在传输“命令”;

P6: 通道正在传输“否认证实”;

P7: 通道正在传输“确认证实”;

P8: 接收方就绪，等到接收对方“命令”;

P9: 接收方收获对方“命令”后的处理;

T1: 发送方发送“命令”，且 SendTimes 置为 1，通讯过程开始;

T2: 发送方等待对方证实超时(TM1 超时)，若 SendTimes<3，则重新发送“命令”,且 SendTimes 加 1;

T3: 在传输过程中，“命令”丢失或出错;

T4: 接收方收取“命令”;

T5: 发送方收获“否认证实”后，若 SendTimes<3，则重新发送“命令”,且 SendTimes 加 1;

T6: 接收方收获的“命令”异常，发出“否认证实”;

T7: 在传输过程中，“否认证实”丢失或出错;

T8: 发送方收取“否认证实”;

T9: 发送方收获“否认证实”后，若 SendTimes>=3，则进行发送命令失败后的处理，通讯过程结束;

T10: 接收方收获的“命令”正常，发出“确认证实”;

T11: 在传输过程中，“否认证实”丢失或出错;

T12: 发送方收取“确认证实”;

T13: 进行发送命令“成功”的处理，通讯过程结

束;

T14: 发送方等待证实超时(TM1 超时), 若SendTimes>=3, 则进行发送命令“失败”的处理, 通讯过程结束.

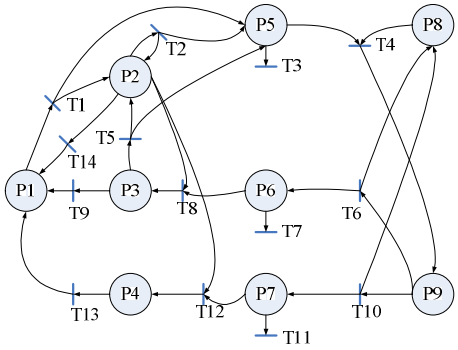

图 9　FASP 的 Petri 网模型

在上述模型中, 以初始标记状态(1, 8)作为可达树的根, 遍历所有可能的变迁和所有可能生成的状态, 并且所有的树叶都成为重复的, 生成的可达树如图 10 所示. 从可达树可以看出:

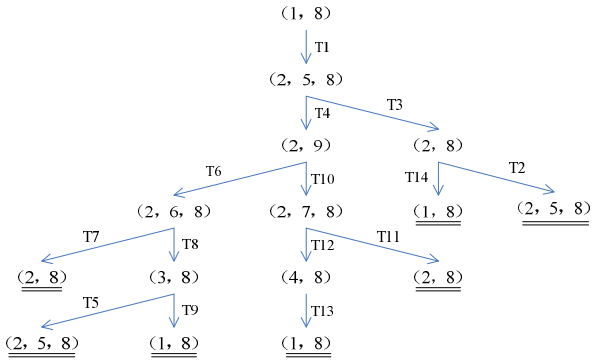

图 10　FASP 的 Petri 网可达树

① 点火序列{T1, T4, T10, T12, T13}代表通讯正常的情况下, Petri 网可回归初始状态; 在通讯不正常的情况下, 点火序列{T1, T3, T14}代表数据包丢失自动重发机制, 点火序列{T1, T4, T6, T8, T9}代表接收方否认证实的自动重发机制, 均能使 Petri 网回归初始状态. 在通讯双方的正常和不正常的情况下, 本 Petri 网都是可逆的, 说明异常事件如数据包丢失(T3、T7、T11)、否认证实(T6), 都得到了妥善处理.

② 可达树中, 只要状态 P2 中有标记, 那么 T2 始终可点火, 所以, 需要限制 T2 的点火时间间隔, 以保持 Petri 网的有界性(或安全性). 这说明协议的发送方须控制重发的时间间隔, 避免接收方溢出.

③ 协议的所有可能状态从初始状态开始都是可达的. 可达树的所有叶子均重复, 不存在死锁. 不过, 树中存在两个循环序列{T4, T6, T8, T5, T4}、{T3, T2, T3}, 在上述序列中, 通过限制 T5、T2 的在循环过程中的点火次数, 即引入 T9、T14, 避免出现“活锁”. 这说明协议的发送方需要对重发次数进行限制, 否则可能导致死循环.

④ 第②条所述的两个循环队列均可到达标记状态(2, 5, 8), 其输入变迁包括 T2 和 T5, 输出变迁包括 T4. 在同一次通讯过程中, T2 和 T5 的多次点火, 使得 T4 的多次点火成为可能, 导致接收方可多次到达状态 P9. 这说明协议的接收方收获的“命令”有重复的可能.

对可达树的分析说明, 本协议是可逆的、有界的、活性的, 能够满足通讯双方的要求.

5　FASP组网应用的应注意的问题

FASP 的形式化分析有利于理解控制器与其连接对象之间通讯过程. 当FASP 用于图 2 所示的多个通讯主体组成的通讯网络时, 还应注意以下问题:

① 时间同步. 整个网络应使用同一个时间源.

② 火警优先传输. FASP 对时间要求较宽松, 按重发 3 次、间隔 3 秒计算, 发送方等待对方证实的时间, 可长达 9 秒. 若需网络多次中转, 则时间成倍增长. 当火警等高优先级信息出现时, 应中止当前通信过程, 改为传输高优先级信息. 高优先级信息全部传输完成后, 重启之前被中止的通信过程.

③ 除非必要, 不要使用自定义协议. 使用自定义协议, 除了会带来兼容问题外, 对于含有重要信息的自定义协议, 在不同类型实体间多次传输过程中, 可能会丧失优先传输的特性.

④ 在网络传输过程中, 尽可能不更改数据包的结构和内容, 尤其是 SEQ、SRC、DST 等. 传输节点可采取复用机制为网络通讯的双方提供透明传输.

⑤ 数据包重复的判定和处理. 如前所述, 接收方收到重复的数据是难免的. 数据包中的 SEQ 被定义为“业务流水号”, 而不是“数据包流水号”、“通讯流水号”. 在连续的多个数据包中, 重复的 SEQ 均应视为同一个业务(SEQ 溢出除外). 控制器节点和中心节点处于网络末端位置, 收到重复数据包后, 可发送证实然后丢弃收到的重复数据; 传输节点处于中转位置, 收到重复数据后, 也应发送证实, 而跟本机相关的处理可不

重复进行, 并根据 DST 域不同, 选择是否继续中转数据包给下级.

⑥ 多个中心节点问题. 控制器节点的信息如需发送给多个中心节点, 有两种处理策略.

第一种是由控制器节点自行完成与多个中心节点的通讯过程. 控制器节点负责证实送达各个中心节点. 以外向通道为例, 控制器节点发出的数据包的 DST 域应填写中心节点地址, 传输节点可采取信道复用机制为网络通讯的双方提供透明传输.

第二种是由传输节点完成与多个中心节点之间的通讯过程. 控制器节点负责证实送达传输节点, 传输节点负责证实送达各个中心节点. 以外向通道为例, 控制器节点发出的数据包的DST域应填写传输节点地址, 传输节点收到数据包后, 为每个中心节点分别产生新的数据包, 并将这些新产生的数据包送达各个中心节点.

6 结语

通过制定规范、统一的通信标准, 本协议为解决火灾报警系统互不兼容奠定了基础, 有利于实现信息共享, 增强火灾自动报警系统与其他系统的互动, 减少重复投资.

通过本文的分析, 可以看出, FASP 被设计为一种忽略物理介质差异的、链路层与应用层合一的单层协议. 在结构设计方面, FASP 的数据包采用十六进制格式, 存储效率较高. 在通讯流程方面, 控制器与其连接对象采用双通道的半双工停等式 ARQ, 实现可靠通信, 在信道正常和不正常的情况下, 本协议都能正常工作, 各种异常事件都得到了妥善处理. 总的来说, FASP 是一个设计优良、考虑周全的通信协议, 能满足通讯双方的通信要求.

不过, 物联网的发展背景下, “开放、共享、互联互通”成为主流趋势, 这要求控制器尽量与各种连接对象完全兼容, 能够用于网络化应用环境, 在这方面, 通过小心谨慎的处理前述问题, FASP 也能够满足网络中各方的通信要求.

参考文献

1 火灾自动报警系统数据输出通信协议(报批稿).

2 吴礼发.网络协议工程.北京:电子工业出版社,2011.

3 GB 4717-2005,火灾报警控制器.

4 GB 26875.1-2011.城市消防远程监控系统.第 1 部分:用户信息传输装置.

5 GA/T 847-2009.消防控制室图形显示装置软件通用技术要求.