شناسایی چالش‌های امنیتی پروتکل IEC 60870-5-104 و بررسی راه‌کارهای موجود

محمدمهدی احمدیان و مهدی شجری*

دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران
mm.Ahmadian@aut.ac.ir
mshajari@aut.ac.ir

چکیده

سامانه‌های کنترل صنعتی که در صنایع و زیرساخت‌های حیاتی مورد استفاده قرار می‌گیرند، از پروتکل‌های ارتباطی متعددی استفاده می‌کنند؛ اغلب این پروتکل‌ها به دلایل مختلف دارای چالش‌های امنیتی متعددی‌اند که امکان خراب‌کاری توسط مهاجمان را فراهم می‌سازد. یکی از پروتکل‌هایی که در شبکه‌های کنترل صنعتی برای انتقال اطلاعات و کنترل تله‌متری مورد استفاده قرار می‌گیرد IEC 60870-5-104 است که در این مقاله از نگاه امنیت سایبر-فیزیکی مورد بررسی قرارگرفته است؛ در این مقاله با هدف تسهیل فرآیند شناخت جوانب امنیتی مختلف پروتکل نامبرده، تلاش شده است تا با تحلیل و بررسی عملیاتی پروتکل هدف در بستر آزمایشگاهی، اهم آسیب‌پذیری‌های مرحله طراحی، پیاده‌سازی و تهدیدهای امنیتی آن شناسایی شده و برخی راه‌کارهای امن‌سازی مرحله طراحی پروتکل و چالش‌های درگیر در آن بررسی شود.

واژگان کلیدی: آسیب‌پذیری امنیتی، تهدید امنیتی، پروتکل کنترل صنعتی، IEC 60870-5-104، ارزیابی امنیتی، سامانه کنترل صنعتی، اسکادا

۱- مقدمه

در گذشته سامانه‌های کنترل صنعتی که در صنعت و زیرساخت‌های حیاتی کشورها مورد استفاده قرار می‌گرفتند، به‌صورت جدا از سایر سامانه‌ها، ازجمله شبکه‌های جهانی اینترنت به‌کار گرفته می‌شدند و این امر روشی در امن‌سازی این سامانه‌ها به شمار می‌آید. اتکای فراوان به این ممیزه، تولیدکنندگان و مصرف‌کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسطهای غیراستاندارد را می‌توان از نتایج این رویکرد دانست.

به‌دلیل نیازمندی‌های جدید و توسعهٔ فناوری، امروزه این قبیل سامانه‌های صنعتی، به‌تدریج با انواع جدیدتر جایگزین یا به‌روزرسانی می‌شوند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌شود که این امر موجب دسترسی مستقیم و غیرمستقیم به این سامانه‌ها از طریق شبکه‌های اختصاصی و یا اینترنت شده و آن‌ها را همانند سایر محصولات درگیر با فناوری‌های اطلاعات در مقابل تهدیدهای سایبری آسیب‌پذیر کرده است. در مواجهه با این تهدیدها که روزبه‌روز در حال افزایش هستند، اقدامات متعارفی نظیر اطلاع‌رسانی امنیتی، اتخاذ خط‌مشی‌های امنیتی مؤثر و سایر فعالیت‌های مقتضی با تأخیر به این حوزه ورود یافته و پرداختن به این قبیل موارد را اجتناب‌ناپذیر کرده است.

گسترش روزافزون شبکه‌های ارتباطی، امنیت آن‌ها به چالش مهمی برای شرکت‌ها و سازمان‌های مختلف تبدیل شده است. نصب انواع تجهیزات امنیتی نظیر ضدبدافزارها، دیواره‌های آتش، سامانه‌های تشخیص نفوذ و راه‌اندازی تونل‌های امن اختصاصی، جداسازی منطقی شبکه‌ها[1] و راه‌کارهای دیگر به این منظور استفاده می‌شوند. یکی از بخش‌هایی که به‌دلیل درگیری اجزای مختلف سایبری و فیزیکی از شبکه به شکل وسیع برای ارتباط بین تجهیزات مختلف استفاده می‌کند، محیط‌های صنعتی است. امروزه محیط‌های صنعتی به‌عنوان یکی از مهم‌ترین کاربردهای سامانه‌های سایبر-فیزیکی (CPS[2]) مطرح است [۱].

[1] Network Logical Isolation (Air Gaps)

[2] Cyber Physical System

*نویسندهٔ مسؤول

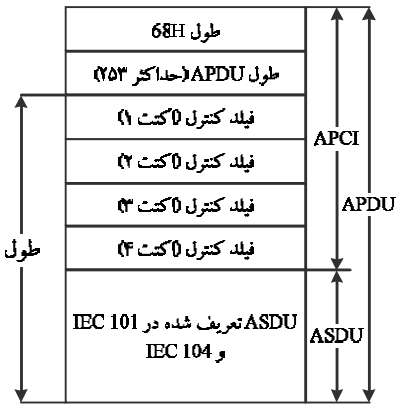
زمانی که سامانه‌های اسکادا[1] (سامانهٔ کنترل سرپرستی و گردآوری داده) طراحی و پیاده‌سازی شد، میزان ارتباطات این نوع سامانه با سایر شبکه‌ها در کمترین میزان ممکن بود یا اصلاً هیچ ارتباطی با شبکه‌های دیگر نداشت. با توسعه سامانه‌های اسکادا، تجهیزات این سامانه‌ها به سمت اتصالات متقابل و برقراری ارتباط با سایر تجهیزات نظیر فیبرهای نوری، تجهیزات رادیویی و ماکروویو، خطوط تلفنی، ماهواره‌ها و اینترانت حرکت کردند. به‌مرور این سامانه‌ها از شبکه‌های نقطه‌به‌نقطه به معماری‌های ترکیبی با ایستگاه‌های کاری فرمانده[2] منفرد، ایستگاه‌های فرمانده- فرمان‌بر[3] و RTU[4]های چندگانه توسعه پیدا کردند [۲].

استانداردهای IEC 60870 مجموعه‌ای از استانداردهای تدوین‌شده توسط IEC[5] بین سال‌های ۱۹۸۸-۲۰۰۰ است که شامل شش بخش به همراه چند استاندارد ضمیمه[6] به‌منظور فراهم‌آوردن یک استاندارد باز برای ارتباط بین سامانه‌های صنعتی است. IEC 60870 در ابتدا فقط برای برقراری ارتباط بین دستگاه‌های الکتریکی و اطلاعات فرمانی بود، اما ازآن‌جایی‌که دارای انواع داده‌های عمومی[7] بود، در نرم‌افزارها و شبکه‌های اسکادا نیز مورد استفاده فراوان قرارگرفته است؛ به تعبیر دیگر محدودیتی برای قابلیت استفاده از این استاندارد در دیگر موارد وجود ندارد. این استاندارد به‌عنوان یک گزینه پیش‌فرض در صنایع الکترونیکی کشورهای اروپایی استفاده می‌شود [۳].

به ساده‌ترین بیان IEC 60870-5 با هدف ارسال پیام‌های کنترل از راه دوربین دو سامانه طراحی‌شده است. در دهه ۱۹۹۰ میلادی دو پروتکل شبکه استاندارد باز تحت عنوان IEC60870-5-101 (در این مقاله از این به بعد به آن T101[8] اطلاق می‌شود) و DNP3[9] برای سامانه‌های اسکادا توسط سازمان IEC و شرکت DNP توسعه داده شدند. برخلاف تفاوت در لایه‌های عملکردی بالا و اشیای داده‌ای، این دو پروتکل دارای شباهت‌هایی در رویه ارتباطی در لایه ارتباط داده بودند.

پروتکل IEC 60870-5-104 که به‌صورت مخفف در این مقاله به آن T104[10] گفته می‌شود، در استاندارد مرجع با عنوان کلی «دسترسی به شبکه با استفاده از روش‌های انتقال استاندارد» مطرح است که مشخص‌کنندهٔ نحوهٔ استفاده از پروتکل TCP/IP در این استاندارد است. این استاندارد ضمیمه در سال ۲۰۰۰ میلادی جهت سامانه‌های اسکادای برق طراحی شد و به‌عنوان یک واسط باز TCP/IP برای ارتباط بین تجهیزات مختلف در شبکه‌های اینترانت و اینترنت استفاده می‌شود. T104 که به تعبیر دیگر از آن به‌عنوان پروتکل ارتباطی صنعتی استاندارد یاد می‌شود به‌طورعمومی در شبکه‌های کنترلی مورد استفاده قرار می‌گیرد [۴]. T104 در مراکز کنترل صنعتی کشور ما نیز کاربرد قابل‌توجهی دارد. حملهٔ پیشرفتهٔ بدافزاری موسوم به Crashoverride در سال ۲۰۱۶ به زیرساخت‌های برق اوکراین که منجر به قطع برق سراسری شد، نشان داد که مهاجمان به‌سادگی می‌توانند به T104 و سایر پروتکل‌های مشابه (T101، IEC61850 و OPC DA) حمله کنند و از آسیب‌پذیری‌های آن‌ها نهایت سواستفاده را ببرند.

T104 بر اساس مدل معماری کارایی ارتقایافته (EPA[11]) طراحی شده است. مدل EPA، لایه نمایش، نشست و انتقال را از مدل OSI حذف کرده و لایه فرایند کاربر[12] به آن اضافه شده است [۵]. ساختار پی‌آیند بسته‌های T104 به‌طورعمومی با نام APDU[13] شناخته می‌شود و دارای دو بخش ASDU[14] و APCI[15] است؛ این ساختار در شکل (۱) قابل مشاهده است.



(شکل-۱): ساختار پی‌آیند بسته T104 [۲۴]

[1] SCADA: Supervisory Control and Data Acquisition
[2] Master
[3] Slave
[4] Remote Terminal Unit
[5] International Electro-technical Commission
[6] Companion Standards
[7] Generic Data Types
[8] در این معادل T مخفف Tele-control است.
[9] Distributed Network Protocol
[10] مشابه T101 در این معادل نیز T مخفف Tele-control است.
[11] Enhanced Performance Architecture
[12] User Process
[13] Application Protocol Data Unit
[14] Application Service Data Unit
[15] Application Protocol Control Information

این پروتکل بر اساس انتقال ASDU طراحی شده است. هر ASDU دارای یک شناسه نوع[1] است. هر نوع داده دارای یک شناسه نوع منحصربه‌فرد است؛ انواع داده‌ای این پروتکل به شکل عمومی[2] بوده و مناسب انواع کاربردهای شبکه‌های اسکادا است [۵].

یکی از مهم‌ترین ویژگی‌های مورد توجه پروتکل T104 امکان ارتباط با شبکه‌های استاندارد (به‌ویژه شبکه‌های TCP/IP) است که اجازه انتقال هم‌زمان داده‌های چندین دستگاه و خدمت را می‌دهد. در زیر فهرستی را از کاربردهایی که T104 فراهم می‌کند، مشاهده می‌کنیم:

- انتقال دستورهای مستقیم
- انتقال فوری داده‌ها
- انتقال داده در صورت نیاز
- هم‌زمان‌سازی ساعت
- انتقال فایل

در ادامه در بخش دوم کارهای انجام‌شده را در زمینهٔ امن‌سازی پروتکل‌های ارتباطی سامانه‌های کنترل صنعتی معرفی خواهیم کرد. در بخش سوم تهدیدها و آسیب‌پذیری‌های امنیتی شناسایی‌شده در رابطه با T104 را معرفی خواهیم کرد. در بخش چهارم راه‌کارهای امن سازی در مرحله طراحی و پیاده‌سازی T104 بر اساس مراجع استاندارد ارائه می‌شود. در بخش پنجم بستر آزمایشی و ارزیابی را که مجموعه تحلیل‌ها و آزمون‌های مختلف خود را بر روی آن بررسی کرده‌ایم، معرفی می‌کنیم و در بخش ششم به نتیجه‌گیری در مورد دستاوردهای مقاله می‌پردازیم.

۲- کارهای مشابه

در زمینهٔ امن‌سازی پروتکل‌های مورداستفاده در حوزه سامانه‌های کنترل صنعتی کارهای مختلفی صورت گرفته است که در ادامه به برخی از آن‌ها اشاره می‌کنیم. بیشتر کارهای موجود مبتنی بر پروتکل‌های Modbus و DNP3 هستند درحالی‌که T104 نیز در مقابل تعداد زیادی از همان حملات، آسیب‌پذیر است. آسیب‌پذیری برای بیشتر این سامانه‌ها حاکی از مشکلات موجود مرتبط با احراز اصالت یا اعتبارسنجی[3] برای ارتباط داده‌ها از طریق T104 و پروتکل‌های مشابه مانند DNP3 است. اگرچه سازوکارها و استانداردهایی برای این مشکلات وجود دارند، ولی در دنیای واقعی به‌دلیل نگرانی‌های عملیاتی، محدودیت‌های قانونی و هزینه به‌ندرت از آن‌ها استفاده می‌شود.

منبع [۶] تعدادی از حملات ممکن را مانند حمله ارسال مجدد، مردی در میان و جعل هویت که نشان‌دهندهٔ نبود امنیت در پروتکل Modbus و DNP3 است، شرح می‌دهد و در ادامه فهرستی از حملات رایج و روش‌های جلوگیری آن‌ها را از قبیل قوانین خوب و مناسب جهت پیکربندی شبکه ارائه می‌دهد. در این منبع نویسنده در مورد سامانه‌های افزونه[4] جهت به اشتراک‌گذاشتن بار ترافیکی در زمان تعمیر سامانه اصلی برای جلوگیری از به‌هدررفتن زمان و نظارت بر سامانه در حال تعمیر بحث می‌کند. نظارت مداوم شبکه به‌خصوص منابع و محتوای بسته‌های T104 لازمه تشخیص رفتارهای غیرعادی در سامانه‌های صنعتی است.

در منبع [۷] با استفاده از پروتکل Modbus حملاتی از قبیل ارسال مجدد و تزریق مقادیر و تزریق دستور را در یک مجموعه آزمایشگاهی انجام و نتایج آن را بررسی و موشکافی شده است [۸]. این پروژه سطوح مختلفی از حملات تزریق را برای پیچیده‌شدن حمله از تزریق ساده تا مقادیر تزریق تصادفی بررسی می‌کند. همچنین پیامدهای ممکن از قبیل تغییر مقادیر گیرنده‌ها، نقشه‌های سامانه کنترلی تغییریافته و حالت عملگرهای تغییریافته را ارائه می‌کند که می‌تواند موجب اغتشاش مستقیم در ارتباطات بشود تا جایی که تجهیزات به‌طور کامل خاموش شوند.

در منبع [۹] مسائل مقدماتی را از قبیل جداسازی شبکه سامانه‌های کنترل صنعتی از اینترنت، آسیب‌پذیربودن در مقابل حملات شناخته‌شده، عدم پیکربندی دیواره‌های آتش که یک مدیر شبکه سامانه کنترل صنعتی باید مسلط باشد، بررسی می‌کند. این اشتباهات می‌تواند به مهاجمان اجازه نفوذ به شبکه را بدهد و زمانی که آن‌ها به شبکه دسترسی پیدا کنند، قادر خواهند بود تا حمله مردی در میان را اجرا کنند.

منبع [۱۰] راه‌های ممکن جهت اجرای مخفیانه یا شبه‌مخفیانه حمله مردی در میان را با استفاده از جعل بسته‌های پروتکل ARP بررسی می‌کند. به‌عنوان‌مثال اهدافی که حملات را از طریق پروتکل ARP درون جدول خود ذخیره نمی‌کنند. منبع [۱۱]، پروتکل ARP امن را شرح می‌دهد که از ساختار زوج‌کلید برای امضای رقمی پیام‌ها استفاده می‌کند تا از حملات جعل ARP جلوگیری کند. منبع [۱۲] نحوه انجام حمله جعل ARP را بر روی شبکه‌های هوشمند شرح می‌دهد. منبع [۱۳] نحوه انجام حمله تزریق دستور را با استفاده از ettercap و روش‌های دیگر نشان می‌دهد.

[1] Type Id
[2] Generic
[3] Validation
[4] Redundant

منبع [۱۴] چگونگی تشخیص تجهیزات پروتکل T104 در شبکه را توضیح می‌دهد، همچنین اسکریپت پایتونی منتشر کرده که توانایی شناسایی و برگرداندن نشانی مشترک تجهیزات این پروتکل را دارد. نشانی مشترک نشانی‌ای است که جهت شناسایی تجهیزات فیزیکی برای تمامی بسته‌های داده T104 استفاده می‌شود. با استفاده از این اسکریپت امکان پویش شبکه برای گروه خاصی از تجهیزات T104 وجود دارد. همچنین از این اسکریپت می‌توان جهت شناسایی اهداف ممکن با توجه به اینکه دستگاه در حال استفاده از پروتکل T104 است و با به‌دست‌آوردن نشانی برای حمله مردی در میان استفاده کرد.

حملاتی که در بالا شرح داده شد، از قبیل ارسال مجدد، مردی در میان، جعل و تزریق باوجوداین‌که برای پروتکل‌های دیگر توسعه‌یافته بودند، ولی می‌توانند برای پروتکل T104 نیز به‌کار گرفته شوند؛ زیرا پروتکل T104 مشابه Modbus و DNP3 احراز اصالت و ممیزی بسته‌ها را پشتیبانی نمی‌کند. منبع [۱۵] حملات منع خدمات را بر روی شبکه صنعتی با پروتکل T104 و دارای استاندارد امنیتی مانند VPN بررسی می‌کند. گفتنی است که سامانه ایجاد تونل سخت‌افزاری برای سامانه‌های کنترل صنعتی جهت بسته‌بندی بسته‌های مجموعه پروتکل‌های مرتبط با استانداردهای 60870-5 با استفاده از VPN توسط شرکت‌هایی نظیر Tofino توسعه یافته‌اند [۱۶].

۳- شناسایی تهدیدها و آسیب‌پذیری‌ها

به‌منظور شناسایی آسیب‌پذیری‌ها در T104 ما از دو سناریو بهره برده‌ایم. نخست به بررسی و کالبدشکافی اسناد منتشرشده از استاندارد و پروتکل هدف پرداخته‌ایم تا بتوانیم آسیب‌پذیری‌های مرحله طراحی را استخراج می‌کنیم. در سناریوی دوم با پیاده‌سازی بستر آزمایشی و بررسی اسنادی که این نوع سناریو را انجام داده‌اند، تلاش کردیم درعمل آسیب‌پذیری‌ها و حملات به این پروتکل را بررسی کنیم؛ در ادامه در بخش ۳-۱- به شکل تلفیقی از این دو سناریو آسیب‌پذیری‌های مرحله طراحی این پروتکل را تبیین می‌کنیم. در بخش ۳-۲- به بررسی آسیب‌پذیری‌های امنیتی مرحله‌ی پیاده‌سازی و عملیاتی T104 و تجهیزات مرتبط با آن می‌پردازیم.

حملات می‌توانند به سطوح مشخصی با توجه به نیازمندی اطلاعاتی و مهارت یک مهاجم طبقه‌بندی شوند؛ جدول (۱) چهار سطح حملات را نشان می‌دهد که ما در ادامه مقاله بر اساس آن حملات را معرفی کرده‌ایم.

۳-۱- آسیب‌پذیری‌های طراحی

در این بخش قصد داریم به بررسی آسیب‌پذیری‌های امنیتی مرحله طراحی استاندارد (پروتکل) T104 بپردازیم؛ اگرچه مشخص است که برخی از مواردی که در این بخش عنوان خواهد شد از چشم طراحان T104 به دور نمانده‌اند، اما به‌دلیل نبود دغدغه امنیتی در T104، این موارد در طراحی و قاعدتاً در پیاده‌سازی پروتکل لحاظ نشده‌اند. این نکته قابل‌توجه است که حل این نوع از آسیب‌پذیری‌ها بدون دست‌بردن در طراحی و پیاده‌سازی پروتکل غیرممکن است. به‌دلیل محدودیت تعداد صفحات مقاله در جدول (۲) حملات فنی ناشی از آسیب‌پذیری‌های طراحی T104 به‌شکل تجمیع‌شده و بر اساس شماره آسیب‌پذیری (V6-V1) آورده شده است.

۳-۱-۱- نبود سازوکار تصدیق هویت (V_1)

طبق استاندارد طراحی T104 هیچ‌گونه تدبیری برای تصدیق هویت موجودیت‌هایی که از این پروتکل استفاده می‌کنند دیده نشده است؛ یعنی هر موجودیتی در شبکه که بسته‌ای را در قالب پروتکل T104 ارسال می‌کند، صحت منبع ارسال‌کنندهٔ آن بررسی نشده و بنابراین امکان حملاتی ازجمله ارسال بسته از منبع غیر معتبر یا حتی انکار مبدأ وجود دارد. به‌دلیل نبود سازوکار تصدیق هویت در T104 در صورت دسترسی مهاجم به بستر شبکه و امکان وصل‌کردن تجهیز خود در شبکه ارتباطی (در محل مناسب، بعد از مرحله جمع‌آوری اطلاعات از شبکه به شکل منفعل) قادر خواهد بود خود را به‌جای هر یک از تجهیزات معتبر شبکه درگیر با پروتکل T104 جا بزند.

در سناریوی دیگر مهاجم می‌تواند با غصب‌کردن هر یک از تجهیزات معتبر درون شبکه به ارسال دستورهای جعلی که به‌ظاهر از سوی تجهیزات دیگر فرستاده شده‌اند، اقدام کند. این تغییرات می‌تواند منجر به حملات متعددی شود که در جدول (۲) آورده شده است.

۳-۱-۲- فقدان سازوکارهای رمزنگاری (V_2)

در T104 هیچ‌گونه تدبیری برای رمزنگاری پیام‌ها دیده نشده است؛ ازاین‌رو بسته‌های نظارتی و کنترلی به‌شکل واضح ارسال شده و هر موجودیتی که بسته‌های عبوری را مشاهده کند می‌تواند از محتوای کنترلی و نظارتی اطلاع کامل پیدا کند. حملات مبتنی بر این آسیب‌پذیری در جدول (۲) آورده شده است.

(جدول-۱): سطوح حمله

سطح حمله	شماره تهدید
پیشرفته	۴
باتجربه	۳
عادی	۲
تصادفی	۱

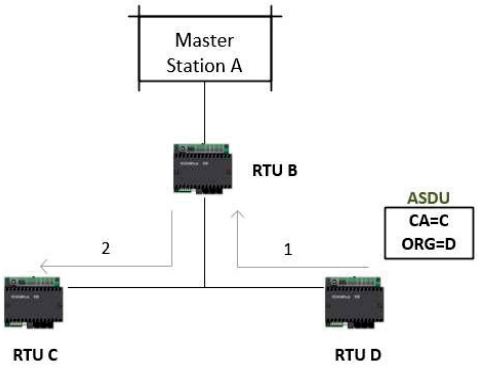
(جدول-۲): کل حملات فنی به فیلدهای T104

فیلد	نوع حمله
بایت آغاز (0x68)	تخریب غیر فیزیکی[1] (V_4)، ممانعت از کیفیت خدمات[2] (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)
طول APDU	تخریب غیر فیزیکی (V_4)، استراق سمع منفعل[3] (V_2)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، داده‌ای[4] (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی تزریق بسته شود (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی ربایش جریان کنترلی شود (V_1,V_4)، مردی در میان غیرفعال (V_1)، مردی در میان فعال (V_1)، جعل هویت (V_1)
فیلد کنترلی ۱	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)
فیلد کنترلی ۲	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)
فیلد کنترلی ۳	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1, V_4)
فیلد کنترلی ۴	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)
شناسه نوع (TypeID)	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، تزریق بسته (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی ربایش جریان کنترلی (V_1,V_4)، مردی در میان غیرفعال (V_1)، مردی در میان فعال (V_1)
تعداد اشیا (NumIX)	تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، تزریق بسته (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی ربایش جریان کنترلی (V_1,V_4)
SQ	تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله تزریق بسته (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی ربایش جریان کنترلی (V_1,V_4)
علت انتقال (COT)	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله تزریق بسته (V_1,V_4)، می‌تواند پیش‌زمینه‌ی حمله‌ی ربایش جریان کنترلی (V_1,V_4)
P/N	تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)
T	تخریب غیر فیزیکی (V_4)، دست‌کاری غیرمجاز (V_1,V_4)
آدرس منبع (ORG)	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، مردی در میان غیرفعال (V_1,V_4)، شنود فعال (V_1,V_4)، مردی در میان فعال (V_1,V_4)، جعل هویت (V_1,V_4)، ارسال مجدد پیام[5] (V_1, V_3)
فیلدهای آدرس مشترک	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، مردی در میان غیرفعال (V_1,V_4)، شنود فعال (V_1,V_4)، مردی در میان فعال (V_1,V_4)، جعل هویت (V_1,V_4)، ارسال مجدد پیام (V_1,V_3)
ASDU (CA)	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، مردی در میان غیرفعال (V_1,V_4)، شنود فعال (V_1,V_4)، مردی در میان فعال (V_1,V_4)، جعل هویت (V_1,V_4)، ارسال مجدد پیام (V_1,V_3)
فیلدهای آدرس اشیا اطلاعاتی (IOA)	استراق سمع منفعل (V_2)، تخریب غیر فیزیکی (V_4)، ممانعت از کیفیت خدمات (V_1,V_4)، دست‌کاری غیرمجاز (V_1,V_4)، مردی در میان غیرفعال (V_1,V_4)، شنود فعال (V_1,V_4)، مردی در میان فعال (V_1,V_4)، جعل هویت (V_1,V_4)، ارسال مجدد پیام (V_1,V_3)
سایر فیلدها	تخریب غیر فیزیکی (V_4)، دست‌کاری غیرمجاز (V_1,V_4)

۳-۱-۳- نبود برچسب زمانی (V_3)

در T104 هیچ‌گونه مکانیزمی برای اعمال برچسب زمانی دیده نشده است؛ ازاین‌رو بسته‌های ارسالی ازلحاظ زمانی اعتبار زمانی معتبری ندارند. حملات پیرو این آسیب‌پذیری در جدول (۱) آورده شده است. در ادامه با یک مثال یک نمونه حمله ارسال مجدد پیام حاصل از فقدان برچسب زمانی را خواهیم دید.

در شکل (۲) شاهد یک سناریوی پیاده‌سازی از ایستگاه‌های مختلف هستیم؛ در این سناریو RTU B وظیفه کنترل و متمرکز کردن داده‌های مختلف را دارد. در لایهٔ پایینی این RTU دو RTU بانام‌های D و C را مشاهده می‌کنیم که ایستگاه‌های کنترل‌شونده هستند. RTU D قصد تولید و ارسال یک ASDU کنترلی به RTU C را دارد. این ASDU توسط RTU B بر اساس فیلد CA مسیریابی می‌شود.

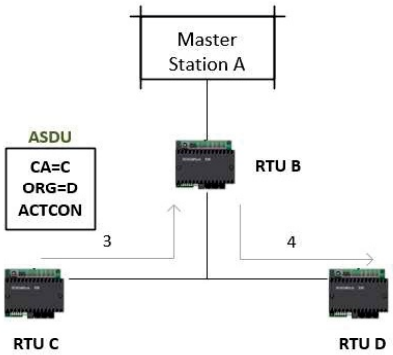


(شکل-۲): ارسال دستور کنترلی از RTU حالت دوگانه

در شکل (۳) مشاهده می‌کنیم که پیام‌های ASDU تأیید عمل توسط ایستگاه RTU C در جهت نظارت تولیدشده و فیلد ORG آن به مقدار D تنظیم می‌شود. RTU B فیلد ORG را در این بسته که برابر D است تشخیص داده و بر این اساس مسیریابی می‌کند. حال مهاجم در این سناریو می‌تواند در صورت قراردادن خود در شبکه (اگرچه کار دشواری است)

[1] نوعی حمله ممانعت از خدمات یا Denial Of Service است.
[2] Denial of Quality of Service
[3] Passive Wirctapping
[4] Data-Only Attack
[5] Replay Attack

ASDU کنترلی ارسالی از سمت RTU D را ضبط کرده و بارها و بارها همین پیام را ارسال کند، این رفتار مخرب ضمن اشغال رسانه ارتباطی منجر می‌شود که RTU C به شکل مکرر ASDU تأیید عمل ارسال کند و پهنای باند شبکه به شکل حجیمی اشغال‌شده و تجهیزات دو طرف درگیر این ارتباطات بدخواهانه باشند.



(شکل-۳): ارسال ASDU تائید عمل به RTU

سناریوی دیگر حمله این است که مهاجم در صورت دسترسی به RTU B که به‌عنوان کنترل‌کننده RTUهای سطح پایین‌تر از خود در معماری در نظر گرفته شده است و با دست‌کاری این تجهیز می‌تواند بسته‌های ارسالی در شکل (۳) که از RTU B عبور می‌کنند و وی نقش مسیریابی آن‌ها را دارد، ضبط کرده و برای هر یک از طرفین به شکل پیوسته ارسال کند و منجر به اختلال در فرآیند کنترلی موردنظر شود.

۳-۱-۴- نبود سازوکار تضمین صحت داده و فیلد چکسام (V_4)

در طراحی T104 هیچ فیلدی به‌منظور محاسبه و ذخیره‌سازی چکسام[1] در نظر گرفته نشده است؛ این در حالی است که در T101 یک بایت فضا برای ذخیره‌سازی چکسام در نظر گرفته شده بود. نبود این چکسام در T104 این پروتکل را در برابر حملات تغییر یا دست‌کاری داده بسیار آسیب‌پذیرتر می‌کند در نگاه نخست بر اساس آنچه بیان شد و بر اساس منابعی که به آن‌ها استناد شد، این‌گونه به ذهن متبادر می‌شود که امکان تغییر بسته‌های عبوری در پروتکل T104 به‌راحتی توسط هر مهاجمی با کمینه سطح حمله یک قابل انجام است؛ اما باید اذعان کرد که این‌گونه نیست.

یکی از دلایلی که طراحان T104 فیلد چکسام را از این پروتکل حذف کرده‌اند، این است که این پروتکل در لایه انتقال و شبکه از پروتکل TCP/IP استفاده می‌کند و فیلد چکسام داده درون پروتکل TCP در لایه انتقال وجود دارد؛ بنابراین برخلاف وجود نداشتن چکسام در T104 مهاجم فاقد دانش کافی قادر به پیاده‌سازی یک حمله سطح یک برای دست‌کاری داده ارسالی توسط پروتکل T104 نخواهد بود و باید از دانش بالایی برای پیاده‌سازی یک حمله سطح بالاتر برای محاسبه مجدد چکسام TCP در صورت تغییر داده T104 باشد. حملات پیرو این آسیب‌پذیری در جدول (۲) آورده شده است.

۳-۱-۵- نبود سازوکارهای امنیتی توکار در لایه کاربرد و پیوند داده (V_5)

در T104 مکانیزم‌های امنیتی توکار در لایه کاربرد و پیوند داده وجود ندارد و این مسأله در لایه کاربرد به‌نوعی می‌تواند درگیر با هر یک از آسیب‌پذیری‌های استخراج‌شده قبلی باشد (در برخی منابع نظیر [۱۷] به‌عنوان آسیب‌پذیری جداگانه‌ای مطرح شده است).

۳-۱-۶- محدودیت پهنای باند ارتباطی (V_6)

پهنای باند محدود در T104 منجر به محدودیت طول بسته ارسالی در این استاندارد می‌شود، به‌نحوی‌که حجم ارسالی قابل انتقال توسط T104 و T101 تنها ۲۵۵ اکتت در واحد زمان خواهد بود. این مسأله باعث خواهد شد که حتی برخلاف داشتن ایده‌هایی برای تقویت T104 در مقابل برخی آسیب‌پذیری‌های شناخته‌شده نتوان از به‌کارگیری بیت یا بیت‌هایی اضافه برای اعمال سازوکارهای امنیتی در طول انتقال داده بهره برد [۱۸].

۳-۲- آسیب‌پذیری‌های پیاده‌سازی و عملیاتی

در این بخش قصد داریم به بررسی آسیب‌پذیری‌های امنیتی مرحلهٔ پیاده‌سازی و عملیات T104 و تجهیزات مرتبط با آن بپردازیم. به‌دلیل محدودیت در منابع منتشرشده در این حوزه و محدودیت در برآورد تجهیزاتی که از پروتکل T104 استفاده می‌کنند با تعدادی معدود از آسیب‌پذیری‌های شناخته‌شده در این مورد، در زمان تدوین این مقاله، روبه‌رو بودیم. حل این نوع از آسیب‌پذیری‌ها با تغییر در پیاده‌سازی و پیکربندی محصولات مورد استفاده از طریق وصله‌های ارائه‌شده توسط سازندگان محصولات ممکن خواهد شد.

۳-۲-۱- آسیب‌پذیری CVE-2008-2474

سرریز بافر در واحد پردازنده ارتباطی ABB PCU 400 به مهاجمان امکان اجرای کد دلخواه را از طریق بسته‌های

[1] checksum

دست‌کاری‌شده می‌دهد. میزان تأثیر این آسیب‌پذیری روی سازمان‌های مختلف به پارامترهای مختلفی بستگی دارد که برای هر سازمان متفاوت هستند. مهاجم می‌تواند با ارسال بسته‌هایی که به‌طور خاص دست‌کاری شده‌اند، به‌واسطه وب x87 و با استفاده از پروتکل‌های ارتباطی T101 یا T104 کدهای دلخواهی را اجرا کند. نمره پایه CVSS نسخه دو این آسیب‌پذیری برابر با ۱۰ است.

این آسیب‌پذیری داری منشأ تهدید غیرطبیعی، محل تهدید خارجی، عامل تهدید غیرانسانی است و ویژگی امنیتی دسترس‌پذیری را نقض می‌کند. این آسیب‌پذیری لایه‌های صنعتی سامانه کنترل مرکزی و سامانه کنترل محلی را تهدید می‌کند و زمینه‌ساز حملات فنی سرریز بافر در پشت، ممانعت از خدمات، اجرای کد دلخواه و تخریب حافظه می‌شود.

۳-۲-۲- آسیب‌پذیری CVE-2015-3939

مهاجم می‌تواند با استفاده از این آسیب‌پذیری به گواهی‌نامه‌هایی دست یابد که برای ارتقای سطوح دسترسی مورد نیاز است. نمره پایهٔ CVSS نسخه دوم این آسیب‌پذیری برابر با ۸/۵ است. با استفاده از این آسیب‌پذیری، مهاجم می‌تواند به بعضی از فایل‌ها از طریق واسط سرویس داخلی ماژول ارتباطی دسترسی پیدا کند.

این آسیب‌پذیری دارای منشأ تهدید غیرطبیعی، محل تهدید خارجی، عامل تهدید غیرانسانی است و ویژگی امنیتی محرمانگی را نقض و این آسیب‌پذیری لایه‌های صنعتی سامانه کنترل مرکزی و سامانه کنترل محلی را تهدید می‌کند و زمینه‌ساز حملات فنی نقض کنترل دسترسی، مرور سامانه، پیمایش مسیر، ارتقای مجوزها می‌شود.

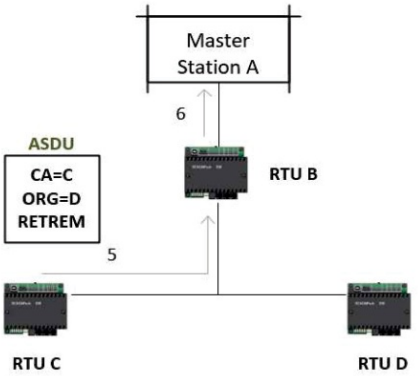
۳-۲-۳- آسیب‌پذیری‌های ارتباطی در به‌کارگیری رسانه غیرقابل اطمینان

درصورتی‌که رسانه‌های ارتباطی به‌کارگرفته‌شده برای انتقال داده‌های در T104 امواج رادیویی یا کابل‌های زوج سیم به هم تأییده باشد و این رسانه‌های در برابر تداخل امواج و فرکانس‌ها ایمن نشده باشند چالش‌های امنیتی در این حوزه به‌وجود می‌آید و می‌بایست امکان تداخل فرکانس توسط عوامل عمدی و غیرعمدی در آن‌ها بررسی شود.

۳-۲-۴- آسیب‌پذیری‌های پیکربندی تجهیزات

راه‌اندازی و پیکربندی تجهیزات مختلف صنعتی فارغ از نوع پروتکل مورد استفاده نیازمند درنظرگرفتن اصول و ملاحظاتی است که شاید در اصل استانداردهای مربوط به پروتکل‌ها به‌صراحت در مورد عدم استفاده و به‌کارگیری نادرست آن‌ها و پیامدهای ممکن در مورد آن‌ها صحبتی نشده باشد. به‌عنوان‌مثال پروتکل T104 دارای فیلدهای متعددی نظیر شناسه، نوع، SQ، NumIX و غیره بوده که چنانچه مانند مثالی که در ادامه بیان می‌شود هرکدام به شکل صحیح مورد استفاده قرار نگیرند، می‌تواند امکان سوءاستفاده برای مهاجم را فراهم سازد.

به‌عنوان مثال در شکل (۲) و شکل (۳) شاهد یک سناریوی پیاده‌سازی از ایستگاه‌های مختلف بودیم. همان‌طور که در شکل (۴) مشاهده می‌کنیم، تغییرات در حالت برگشت در اثر یک دستور منجر به بازگردانی ASDU اطلاعاتی به ایستگاه فرمانده می‌شود؛ این بسته ارسالی دارای نشانی ORG برابر صفر و نوع RETREM در جهت نظارت بوده همین باعث می‌شود که RTU B آن را به ایستگاه فرمانده بفرستد که در صورت عدم دقت در استفاده صحیح از این مقادیر امکان سوءاستفاده برای مهاجم می‌تواند فراهم شود.



(شکل-۴): نظارت بر اطلاعات برگشت یافته به ایستگاه کنترل‌کننده

اگرچه آسیب‌پذیری‌های پیکربندی یا عملیاتی یک دسته مجزا از آسیب‌پذیری‌های امنیتی هستند که به‌علت پیکربندی و گسترش نادرست یک سامانه در محیطی خاص به‌وجود می‌آیند؛ اما با توجه به اینکه استخراج این آسیب‌پذیری‌های در هر فرایند کنترل صنعتی و زیرساخت پیاده‌سازی‌شده آن (با توجه به تنوع تجهیزات و تولیدکنندگان تجهیزات) متفاوت و نیازمند استخراج و ارزیابی دارایی‌های واحد صنعتی هدف است، شناسایی و احصای آسیب‌پذیری‌های این نوع است؛ ازاین‌رو این نوع آسیب‌پذیری‌های باید در محیط عملیاتی و توسط گروه امنیت سامانه‌های سایبر-فیزیکی انجام پذیرد.

قابل‌توجه است که چنانچه شرکت‌های تولیدکننده تجهیزات هدف و شرکت‌های پیاده‌سازی این تجهیزات و

زیرساخت‌های لازم الزامات امنیتی نصب و بهره‌برداری را تهیه‌کرده باشند رعایت این الزامات در این مرحله می‌توان آسیب‌پذیری‌های این مرحله را تا حد مناسبی مرتفع سازد؛ چنانچه این امر توسط این شرکت‌ها در نظر گرفته نشده باشد، توصیه می‌کنیم که با درنظرگرفتن مصالحه‌های اقتصادی و در نظر گرفته نقشه راه امنیت سایبری واحد هدف از شرکت‌های متولی درخواست ارائه الزامات نصب و بهره‌برداری تجهیزات درگیر با T104 صورت گیرد.

۴- راه‌کارهای امن‌سازی در مرحله طراحی

در این بخش قصد داریم تا بر اساس اسناد مرجع، برخی راه‌کارهای امن‌سازی مرحله طراحی T104 را بررسی کنیم؛ قاعدتاً شناخت مسائل درگیر در این بخش به ما کمک می‌کند تا برخی راه‌حل‌های امن سازی T104 و پروتکل‌های مشابه را در مرحله طراحی بهتر بیاموزیم و چنانچه قصد داشته باشیم در آینده در زمینهٔ امن‌سازی پروتکل‌های کنترل صنعتی، بومی‌سازی امن آن‌ها و ارائه پروتکل کنترل صنعتی جدید امن فعالیت کنیم، بتوانیم الگوهای مناسبی برای این حوزه پژوهشی و صنعتی داشته باشیم.

با توجه به اسناد انتشاریافتهٔ کنونی در این حوزه راه‌حل‌هایی برای پیش‌گیری از حملات فنی جعل هویت، دست‌کاری غیرمجاز، ارسال مجدد پیام، شنود (فقط در مورد مبادله کلیدهای رمزنگاری) و ممانعت از خدمات ارائه‌شده است که در ادامه به‌اختصار به آن‌ها می‌پردازیم. در حوزه استانداردها و الزامات امنیتی مرتبط با پروتکل‌های مبتنی بر استانداردهای IEC 60870 یکی از مراکز فعال، کمیسیون IEC است. کارگروه ۱۵ IEC مجموعه‌ای از استانداردهای امنیتی را به‌منظور ارتقای اطمینان‌پذیری و امنیت زیرساخت‌های اطلاعاتی منتشر کرده است [۱۹]. عمده الزامات و ملاحظات امن‌سازی این بخش که با درنظرگرفتن پارامترهای عملکردی و پایداری گردآوری و تهیه شده مبتنی بر استاندارد IEC/TS 62351 است که یک سند مشخصات فنی است و از سوی کمیته فنی ۵۷ تهیه‌شده است.

از میان مجموعه استانداردهای منتشرشده در قالب IEC/TS 62351 دو استاندارد خاص از این مجموعه با شماره‌های 62351-5 [۲۰] و 62351-3 [۲۱] در ارتباط با پروتکل T104 هستند؛ البته این بدین معنا نیست که این دو استاندارد خاص فقط برای T104 ارائه شده باشند. استاندارد IEC/ST 62351 تنها بر احراز اصالت لایه کاربرد و مسائل امنیتی ناشی از این استناد تمرکز دارد. سایر دغدغه‌های امنیتی، به‌خصوص حفاظت در برابر حملات صورت‌گرفته توسط انسان با به‌کارگیری روش‌های رمزنگاری، خارج از قلمرو این استاندارد هستند.

۴-۱- مسائل درگیر در طراحی سازوکار احراز اصالت

در این استاندارد با مبنا قراردادن سازوکار احراز اصالت، مسائل درگیر در طراحی سازوکار را موارد مطرح می‌کند که در زیر به اهم آن‌ها اشاره می‌کنیم:

۴-۱-۱- ارتباطات نامتقارن[1]

در T104 یک ایستگاه کنترل‌کننده و یک ایستگاه تحت کنترل وجود دارد که هر یک نقش‌ها، مسئولیت‌ها، شیوه‌نامه‌ها و قالب‌های مختلفی برای پیام دارند. به‌ویژه، ایستگاه کنترل‌کننده در بسیاری از موارد مسئولیت کنترل جریان و دسترسی رسانه‌ای را بر عهده دارد. وجود ایستگاه‌های تحت کنترل و کنترل‌شونده دو تأثیر بر طراحی سازوکار احراز اصالت دارد:

- قالب پیام در هر مسیر متفاوت بوده، حتی درصورتی‌که کارکردها مشابه باشند.
- توزیع کلید از این بابت ساده می‌شود که آن‌ها همیشه از سوی ایستگاه‌های کنترل‌کننده صادر می‌شوند.

۴-۱-۲- مبتنی بر پیام بودن[2]

T104 یک پروتکل مبتنی بر پیام است؛ این بدان معناست که احراز اصالت باید بر اساس پیام‌ها، نه بر اساس زمان شروع جریان داده‌ها یا زمان بعد از آن صورت گیرد.

۴-۱-۳- دنبالهٔ اعداد ضعیف یا فقدان دنباله اعداد

یکی از روش‌های رایج امنیتی برای رسیدگی به تهدید ارسال مجدد پیام درج یک عدد دنباله‌ای در پیام است. این عدد شرایط حمله‌کننده را برای جا زدن خود به‌صورت کاربر قانونی به‌واسطه رونوشت‌برداری از یک پیام موجود را سخت می‌کند. T104 اگرچه دارای فیلد SQ است، اما کاربرد این فیلد با آنچه در این بخش مدنظر است متفاوت بوده و محدودیت دارد؛ بنابراین در طراحی امن پروتکل‌هایی نظیر T104 باید سازوکار دنباله عددی مناسب و دیگر داده سازوکارهای وابسته به زمان را برای حافظت در برابر حملات ارسال مجدد پیام در نظر گرفته شود.

۴-۱-۴- توان پردازش محدود

فقدان توان پردازش بالا در بسیاری از سامانه‌های کنترل صنعتی یکی از نگرانی‌های اصلی طراحی برای پروتکل‌های

[1] Asymmetric

[2] Message-Oriented

نظیر T104 است. این نیاز طراحی الزاماً بر سازوکار احراز اصالت تأثیرگذار است؛ نگرانی به این دلیل افزایش پیدا می‌کند که بسیاری از این دستگاه‌ها ماشین‌های تک‌پردازنده هستند؛ بنابراین حمله ممانعت از خدمات نه‌تنها بر قابلیت ارتباطی این دستگاه‌ها تأثیر دارد، بلکه بر کارکردهای آن‌ها به‌عنوان کنترل الکتریکی، حفاظتی و نظارت نیز تأثیر دارد؛ بنابراین استفاده از سازوکارهای امنیتی مانند رمزنگاری کلید عمومی و استفاده از کلیدهایی با اندازه بزرگ که به توان پردازش بالایی نیاز دارند تا جای ممکن اجتناب شده است.

۴-۱-۵- پهنای باند محدود

میزان محدود پهنای باند موجود در شبکه‌های کنترل صنعتی یکی دیگر از نگرانی‌های اصلی طراحی پروتکل‌هایی نظیر T104 است؛ بنابراین، سازوکار احراز اصالت نباید سربار زیادی را به پروتکل‌های تحت تأثیر اضافه کند. اندازه چالش[1] و داده‌های احراز اصالت ازاین‌رو محدودشده و تا جای ممکن در حالی انتقال داده می‌شود که سطحی مناسب از امنیت را در برمی‌گیرد.

۴-۱-۶- عدم دسترسی به سرور احراز اصالت

ماهیت شبکه‌های کنترل صنعتی که پروتکل T104 و سایر پروتکل‌های مشابه در آن‌ها منتشر می‌شوند به این‌گونه است که ایستگاه‌های کنترل‌کننده اغلب تنها دستگاهی هستند که به‌وسیله آن با ایستگاه‌های تحت کنترل قابلیت برقراری ارتباط دارند. درصورتی‌که دسترسی به دیگر شبکه‌ها وجود داشته باشد، این دسترسی اغلب از طریق ایستگاه کنترل‌کننده انجام می‌گیرد. تأثیر این مسأله بر سازوکار احراز اصالت این است که هر سامانه‌ای که به راستی‌آزمایی[2] برخط[3] اعتبار امنیتی ایستگاه کنترل‌کننده به‌واسطه سامانه شخص ثالث[4] نیاز داشته باشد، غیرعملی است.

۴-۱-۷- چکسام محدود

همان‌طور که در بخش ۳-۱-۰۴ توضیح داده شد راه‌کارهای کنترل صحت مورد انتخاب برای T104 به‌منظور حفاظت در برابر نوفه تصادفی طراحی شده است، نه حملات موردنظر؛ صحت T104 به راه‌کارهای تأمین صحت لایه‌های پایین در EPA بستگی دارد. ازآنجایی‌که T104 یک پروتکل لایه کاربرد و لایه فرآیند کاربر است و از سویی استاندارد منبع [۲۰] تنها به بحث در مورد سازوکار لایه کاربردی می‌پردازد، نمی‌تواند به اندازه‌های کافی تضمین‌کننده صحت دست‌کم در لایه کاربرد باشد.

۴-۱-۸- سایت‌های از راه دور[5]

دستگاه‌هایی را که پیاده‌سازی می‌کنند اغلب در مناطقی واقع هستند که فاصله جغرافیایی آن‌ها از یکدیگر دور بوده و دسترسی به آن‌ها هزینه بالایی دارد؛ بنابراین تا جایی که امکان داشته باشد، سازوکارهای امنیتی ازجمله احراز اصالت توصیه می‌شود شامل روش‌های به‌روزرسانی اعتبار به شکل از راه دور باشد.

۴-۱-۹- رسانه غیرقابل اطمینان[6]

T104 اغلب در رسانه‌های غیرقابل اطمینان به کار گرفته می‌شوند. در طراحی سازوکارهای امنیتی مانند احراز اصالت، توصیه می‌شود، شرایط خطا را نیز زمانی که عدم اطمینان در رسانه وجود دارد، مدنظر قرار گیرد. برای مثال، ازدست‌رفتن یک پیام امنیتی واحد الزاماً به معنای یک حمله نیست.

۴-۲- سازوکار طراحی امن

سازوکار احراز اصالت بر اساس دو مفهوم طراحی می‌شود:

- پروتکل چالش و پاسخ.
- مفهوم MAC[7] که هر دو ایستگاه کنترل‌کننده و کنترل‌شونده بر اساس ASDU یا پیام پروتکل محاسبه می‌شود، باید احراز اصالت شوند.

سازوکار احراز اصالتی که در استاندارد [۲۰] شرح داده شده است بر اساس مفهوم چالش و پاسخ طراحی شده است؛ این مفهوم به دلایل زیر اعمال شده است:

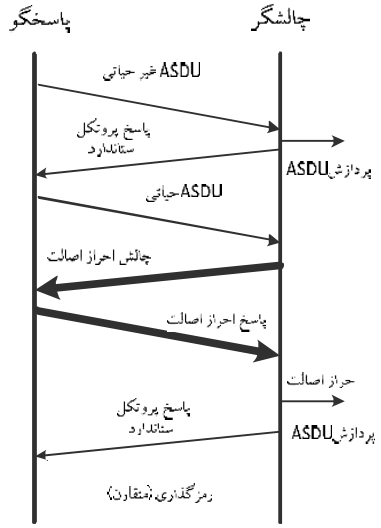
- این مفهوم مسئولیت امنیت را در دستگاهی که نیاز به احراز اصالت دارد فراهم می‌کند و شرایط کاربردی مناسبی را در شبکه‌های متنوعی مانند شبکه‌های کنترل صنعتی فراهم می‌سازد.
- این مفهوم امکان داشتن ارتباط غیر امن را در صورت لزوم ممکن می‌کند و پهنای باند و نیازهای پردازشی را در این شرایط کاهش می‌دهد.

نمودارهای شکل (۵) نشان‌گر نمونه دنباله پیام‌هایی است که سازوکار چالش و پاسخ یک ASDU حیاتی را به تصویر می‌کشد. چالش ممکن است با ایستگاه کنترل‌کننده یا تحت کنترل شروع شود. ازآنجایی‌که پروتکل‌های سری

[1] Challenge
[2] Verification
[3] Online
[4] Third Party
[5] Remote Sites
[6] Unreliable
[7] Message Authentication Code

استاندارد IEC 60870-5 به‌طورعمومی نامتقارن هستند، این بدان معناست که قالب حقیقی چالش و پیام‌های پاسخ تا حدودی در مسیرهای نظارت و کنترل متفاوت هستند.

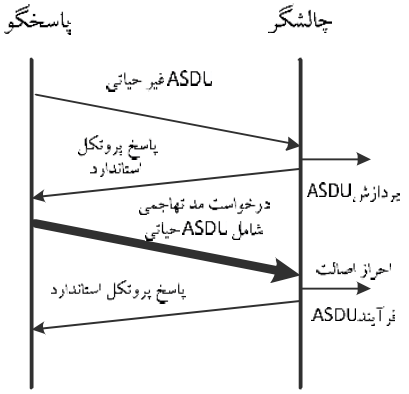
T104 ممکن است، عملیات الزامی دیگری را نیز تعریف کند. به‌منظور حفاظت در برابر حملات ارسال مجدد پیام، پیام چالش حاوی داده‌هایی است که به‌صورت تصادفی هر زمان که چالشی صادر می‌شود، تغییر می‌کند. چالش‌گر در پیام چالش مشخص می‌کند که الگوریتم MAC برای پاسخ‌گو به پاسخ به این چالش چگونه باشد. ایستگاه تحت کنترل یا کنترل‌کننده که چالش را دریافت می‌کند باید قبل از اینکه ارتباطات ادامه داشته باشد، پاسخ دهد. پاسخ‌گو الگوریتم MAC تعیین‌شده در پیام چالش را برای تولید پاسخ اجرا می‌کند. کلید نشست مشترک که برای هر دو ایستگاه شناخته‌شده است یک بخش جدانشدنی از محاسبه به‌شمار می‌رود.



(شکل-۵): نمونه چالش موفق ASDU حیاتی[۲۰]

در زمان دریافت پاسخ، چالش‌گر محاسبات مشابه را روی داده‌های مورد استفاده از سوی پاسخ‌گو اعمال می‌کند. درصورتی‌که نتیجه مطابقت داشته باشد، چالش‌گر ادامه ارتباط را اجازه می‌دهد. برای کاهش استفاده از پهنای باند یک مد تهاجمی[1] نیز می‌توان طراحی کرد؛ پاسخ‌گو یک عملیات حیاتی[2] را امتحان می‌کند و ممکن است به‌صورت اختیاری چالش را پیش‌بینی کرده و مقدار MAC را در ASDU مشابه که حفاظت شده است ارسال کند. شکل (۶) نشانگر احراز اصالت ASDU کلیدی با بهره‌گیری از مد تهاجمی موفق است.

[1] Aggressive Mode
[2] Critical



(شکل-۶): نمونه‌ای از درخواست مد تهاجمی موفق[۲۰]

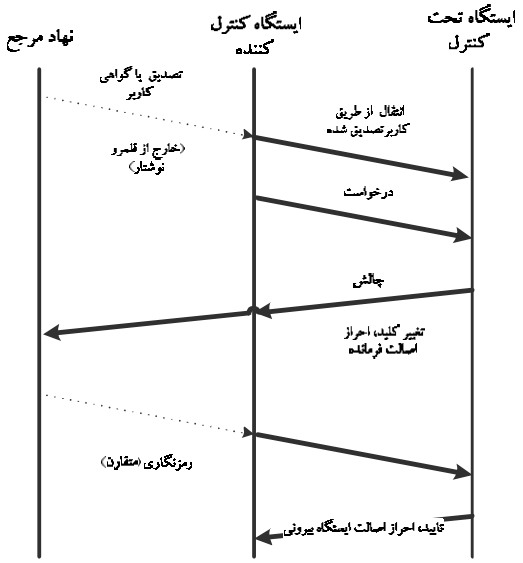
استاندارد [۲۰] استفاده از کلیدهای از پیش مشترک را به‌عنوان پیش‌فرض امکان‌پذیر می‌کند. این اصلی مشخص می‌کند که بسیاری از تجهیزات کنترل صنعتی برای مدیریت اعتبار امنیتی به شیوه‌ای پیچیده‌تر آماده نیست، ولی نیاز به کمینه سطح حفاظتی دارند. این استاندارد همچنین روش‌های اختیاری را برای تغییر کلیدهای از پیش مشترک به شکل از راه دور با بهره‌گیری از رمزنگاری کلید عمومی متقارن یا نامتقارن فراهم می‌کند.

استاندارد [۲۰] از اصول امنیتی محرمانگی پیشرو عالی[3] تبعیت می‌کند که در IEC/ST 62351-2 [۲۲] تعریف شده است. استفاده از کلیدهای رمزنگاری و نحوه به‌روزرسانی آن‌ها در سازوکار احراز اصالت اهمیت ویژه‌ای دارد، که در استانداردهای مرجع کلیدهای نشست مسیر نظارت، نشست مسیر کنترل، به‌روزرسانی، گواهی مرجع[4] (اختیاری)، خصوصی مرجع، عمومی مرجع، خصوصی کاربر، عمومی کاربر، خصوصی ایستگاه تحت کنترل، عمومی ایستگاه تحت کنترل در طراحی در نظر گرفته شده‌اند. در کمترین سطح، کلیدها به‌وسیله ایستگاه کنترل‌شده و کنترل‌کننده مدیریت می‌شوند. فرآیند مدیریت کلید به‌صورت اختیاری می‌تواند به‌کمک شخص ثالث مورد اعتماد صورت گیرد. جهت مطالعه اطلاعات تکمیلی در مورد مدیریت و متعلقات آن‌ها می‌توان به [۲۰] و IEC-62351-9 [۲۳] مراجعه کرد. به‌عنوان‌مثال در شکل (۷) نمایی سطح بالا را از تعامل بین مرجع و ایستگاه‌ها در فرآیند توزیع کلید مشاهده می‌کنیم.

به‌منظور پیاده‌سازی سازوکارهای ارائه‌شده نیاز به اضافه‌کردن مواردی به استاندارد [۲۴] هستیم. در ادامه بر اساس استاندارد [۲۵] اقدام به معرفی برخی از این موارد می‌کنیم. مقادیری که باید در فیلد علت انتقال (COT) اضافه شود و شرح مختصری از هر یک، در جدول (۳) آورده شده

[3] Perfect Forward Secrecy
[4] Authority Certification Key

است. هدف از اضافه‌کردن سه مقدار جدید ۱۴، ۱۵ و ۱۶، تجهیز پروتکل هدف به سازوکارهای احراز اصالت است؛ چون به‌دلیل اهمیت این مقوله، استفاده از کلیدهای رمزنگاری و نحوه به‌روزرسانی آن‌ها در استاندارد [۲۵] مورد توجه ویژه‌ای قرار گرفته است. مقادیر یادشده در فیلد علت انتقال به گیرنده پیام وضعیت احراز اصالت، نگه‌داری کلید نشست و نگه‌داری کلید نقش کاربر را مشخص می‌کند.



(شکل-۷): تعامل بین مرجع و ایستگاه‌ها در مدیریت کلید[۲۰]

(جدول-۳): مقادیری که باید به فیلد COT اضافه شوند

مقدار جدید	علت انتقال
۱۴	احراز اصالت
۱۵	نگه‌داری کلید نشست احراز اصالت
۱۶	نگه‌داری نقش کاربر و کلید به‌روزرسانی

مقادیری که باید در فیلد شناسه نوع اضافه شود و شرح مختصری از هر یک در جدول (۴) آورده شده است. مقادیر بیان‌شده در جدول (۴) مشخص می‌کند که با توجه به نیازمندی‌های متفاوت پیام‌ها در ارتباطات امن و بر اساس نوع تعامل بین طرفین ارتباطات، از چه نوع شناسه‌ای باید استفاده شود.

گفتنی است که استاندارد IEC62351 اگرچه سازوکارهای امنیتی مطلوبی برای ارتقای امنیت فراهم می‌کند اما این استاندارد جهت ارتقای امنیت تمرکز ویژه‌ای بر روی لایه کاربرد دارد؛ ازاین‌رو باید به این نکته توجه داشت که در صورت پیاده‌سازی کامل استاندارد IEC62351 نمی‌توان امنیت بالایی در همه لایه‌ها توقع داشت [۲۶]. باید به این نکته توجه کرد که به‌منظور تقویت سازوکارهای امنیتی مرجع [۲۰] می‌توان از سایر استانداردهای خانواده IEC62351 مانند استاندارد[۲۱] جهت افزایش سازوکارهای محرمانگی یا صحت در ASDUهای استفاده کرد.

(جدول-۴): مقادیری که باید به فیلد شناسه نوع اضافه شوند

نوع	شماره	توضیح
S_IT_TC_1	<۴۱>	برچسب زمانی برای آمار و گزارش‌های امنیتی
S_CH_NA_1	<۸۱>	چالش احراز اصالت
S_RP_NA_1	<۸۲>	پاسخ احراز اصالت
S_AR_NA_1	<۸۳>	درخواست احراز اصالت مد تهاجمی
S_KR_NA_1	<۸۴>	درخواست وضعیت کلید نشست
S_KS_NA_1	<۸۵>	وضعیت کلید نشست
S_KC_NA_1	<۸۶>	تغییر کلید نشست
S_ER_NA_1	<۸۷>	خطای احراز اصالت
S_US_NA_1	<۹۰>	تغییر وضعیت کاربر
S_UQ_NA_1	<۹۱>	درخواست تغییر کلید به‌روزرسانی
S_UR_NA_1	<۹۲>	پاسخ تغییر کلید به‌روزرسانی
S_UK_NA_1	<۹۳>	تغییر کلید به‌روزرسانی متقارن
S_UA_NA_1	<۹۴>	تغییر کلید به‌روزرسانی نامتقارن
S_UC_NA_1	<۹۵>	تائید تغییر کلید به‌روزرسانی

درعمل شاهد این هستیم که برخی شرکت‌های تولیدکننده تجهیزات صنعتی برخی سازوکارهای امنیتی را در سطح تجهیزات خود پیاده‌سازی کرده‌اند که بتوان داده‌های پروتکل‌هایی را مانند T104 که فاقد سازوکار امنیتی‌اند از درون کانال‌هایی امن ارسال کرد؛ در صورت استفاده از این‌گونه راه‌حل‌های امنیتی باید توجه داشت که مخاطرات امنیتی پروتکل T104 از بین نمی‌رود، بلکه تنها از پروتکل T104 به مخاطرات امنیتی کانال مورداستفاده و پروتکل‌های امنی که آن کانال استفاده می‌کند منتقل می‌شوند.

۵- بستر آزمایش و ارزیابی

جهت بررسی آسیب‌پذیری‌های پروتکل T104، مبتنی بر سناریوی حمله‌محور، ابتدا رویکرد مورد نظر را مورد بررسی قرار می‌دهیم. در ادامه سه‌گام تحقق حمله برای بهره‌جویی از آسیب‌پذیری‌های پروتکل T104 مورد بررسی قرار می‌گیرند.

۵-۱-شناسایی: دو روش فعال و غیرفعال برای شناسایی یا تشخیص تجهیزات بهره‌بردار از پروتکل T104 متصل به شبکه TCP/IP وجود دارد. در روش غیرفعال که به شکل منفعلانه انجام می‌گیرد، هیچ عملی بر روی شبکهٔ هدف انجام نمی‌شود؛

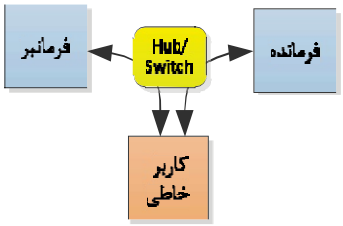
یک واسط بر روی مد بی‌قاعده[1] تنظیم می‌شود تا تمامی بسته‌های روی خط را بپذیرد. بسته‌ها می‌توانند از طریق نرم‌افزارهایی مانند TCP dump یا وایرشارک مورد بررسی قرار گیرند. زمانی که ترافیک پروتکل T104 شناسایی شد می‌تواند برای مصارف آینده از قبیل حمله ارسال مجدد یا شناسایی اهداف حمله با تحلیل ترافیک ذخیره شود.

روش شناسایی فعال، روندی است که بسته‌هایی برای برقراری ارتباط و دریافت پاسخ توسط یک دستگاه ارسال می‌شود. برای مثال در منبع [۱۴] اسکریپت پایتونی نوشته است که فهرستی از نشانی‌های IP تجهیزات بسته‌های پروتکل T104 را در صورت وجود کشف می‌کند و نشانی مشترک آن‌ها را برمی‌گرداند. به این طریق که دستگاه مورد نظر یک بسته APDU ارسال می‌کند و هدف با یک بسته تصدیق پاسخ می‌دهد؛ سپس یک بسته شروع انتقال داده (STARTDT[2]) ارسال می‌کند. بسته پاسخ برای تشخیص نشانی مشترک بررسی شده و اگر نشانی مشترک پیدا نشد از روش دیگری که در ادامه توضیح داده می‌شود استفاده می‌شود. روش دیگر برای به‌دست‌آوردن نشانی تجهیزات T104 این است که اسکریپت یک بسته C_IC_NA_1 در شبکه پخش کند. این بسته حاوی یک دستور جست‌وجوی تشخیص T104 است. روش غیرفعال ممکن است توسط یک هکر مبتدی، کسی که مطمئن نیست درون سامانه چه می‌گذرد یا برای جلوگیری از شناسایی توسط یک مهاجم ماهرتر استفاده شود. در صورت امکان حالت فعال به‌احتمال زیاد برای اطمینان از وجود دستگاه T104 و به‌دست‌آوردن اطلاعات دقیق بیشتر از حالت غیرفعال استفاده می‌شود [۱۶].

۵-۲- گردآوری: در این مرحله پس از شناسایی اهداف، اطلاعاتی را که می‌تواند برای حمله استفاده شود، جمع‌آوری می‌شود. این امکان وجود دارد که در زمان انجام حمله، اطلاعات از طریق نظارت بر داده‌ها جمع‌آوری شود. در یک سوییچ شبکه به‌طورعمومی یک رونوشت از تمام بسته‌ها به یک درگاه خاص با نام درگاه span که درگاه آینه نیز نامیده می‌شود، ارسال‌شده و جمع‌آوری می‌شود. اگر یک مهاجم قادر باشد به ماشینی دسترسی پیدا کند که متصل به یک درگاه span است یا بتواند با به‌دست‌آوردن کنترل مدیریت یک سوییچ، یک درگاه span روی آن فعال کند، قادر خواهد بود کلیه ترافیک عبوری شامل داده‌هایی را که توسط اهداف منتقل می‌شود، جمع‌آوری کند [۱۶].

راه دیگر جمع‌آوری اطلاعات ترافیکی شبکه، قرارگرفتن در بین اهداف و جمع‌آوری داده‌ها است. یکی از راه‌های انجام این کار حمله از جعل بسته‌های ARP است؛ به‌عنوان مثال در منابع [۱۰] و [۱۲] در این زمینه کار کرده شده است. شکل (۸) یک حمله جعل ARP موفق را نشان می‌دهد. حمله جعل ARP از این نکته بهره می‌برد که پروتکل T104 به‌طور ذاتی از تأیید و احراز اصالت پشتیبانی نمی‌کند. یک مهاجم می‌تواند پیام‌های ARP جعلی را با MAC نشانی خود و IP نشانی هدف مورد نظر ارسال کند؛ بنابراین هر بسته‌ای که حاوی IP نشانی هدف باشد به ماشین مهاجم ارسال خواهد شد. درنتیجه مهاجم می‌تواند تمامی بسته‌هایی را که بین اهداف در حال ارسال است، ببیند و ویرایش کند.

راه‌های جایگزین حمله جعل ARP، مسموم‌کردن DNS[3] و حمله سرریز جدول CAM[4] است که مهاجم با اقداماتی حافظه سوئیچ را سرریز و آن را به یک تکرارکننده[5] یا یک هاب تبدیل می‌کند (در بعضی موارد این حمله می‌تواند باعث ازکارافتادن سوئیچ و به‌نوعی حمله ممانعت از خدمات شود)، البته این حملات، نیاز به آسیب‌پذیری‌های دیگری دارد که خارج از ماهیت اصلی خود پروتکل T104 است [۱۶].



(شکل-۸): حمله جعل ARP موفق

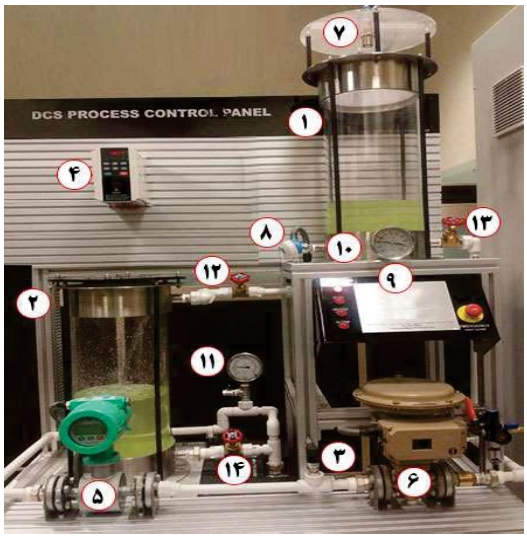
۵-۳- حمله نهایی: مرحله نهایی که تمامی مراحل دیگر به آن ختم می‌شود، در این دسته‌بندی «حمله نهایی» نام دارد. در حمله ارسال مجدد داده‌های معتبر در زمان ارسال جمع‌آوری شده و توسط مهاجم دوباره ارسال می‌شوند. بسته‌ها را می‌توان از محل منبع یا استراق‌سمع به‌وسیله روش حمله مردی در میان در قلب سناریوهای حملات چندمرحله‌ای[6] جمع‌آوری کرد. داده‌ها ممکن است، بدون هیچ تغییری یا با تغییر، دوباره ارسال شوند. اگر داده‌ها بدون تغییر ارسال شوند، به معنی خواندن و ارسال به ایستگاه نظارت به‌منظور خواندن دستورهای کنترلی است. این کار می‌تواند موجب اختلال در شبکه یا حتی خسارت شود؛ چنین حملاتی می‌تواند توسط

[1] Promiscuous
[2] Start Data Transfer
[3] DNS Poisoning
[4] Content Addressable Memory
[5] Repeater
[6] Multi-Step Attack

یک مهاجم بی‌تجربه یا فردی که سامانه را به‌درستی نمی‌شناسد (سطوح حمله ۱ و ۲)، انجام شود.

با توجه به شناسایی آسیب‌پذیری‌ها و حملات مطرح‌شده در قسمت سوم، در این قسمت یکی از حملات پیاده‌سازی‌شده در بستر آزمایش تحت عنوان حمله ارسال مجدد بر روی پروتکل T104 شرح داده می‌شود. بستر آزمایش هدف «پلنت کنترل صنعتی شبیه‌سازی‌شده مخازن انتقال مایع» نام دارد و از تجهیزات ابزار دقیق و کنترلی مختلفی که در فرآیندهای صنعتی، ازجمله مخازن انتقال مایع صنایع پتروشیمی، استفاده می‌شوند، طراحی و ساخته شده است. بر اساس شماره‌های شکل (۹) این بستر دارای تجهیزات زیر است:

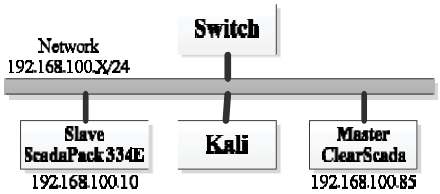
- دو مخزن مایع (۱ و ۲)
- پمپ آب و درایور (۳ و ۴)
- جریان‌سنج[1] (۵)
- شیر کنترلی به همراه فرستندهٔ فشار صفر تا شش‌صد میلی‌بار (۶)
- حس‌گر التراسونیک[2] سطح مایع (۷)
- دماسنج (۸)
- دماسنج غیر بازخوردی (۹)
- بخاری[3] (۱۰)
- فشارسنج صفر تا شش غیر بازخوردی (۱۱)
- سه دریچه کنترل مایع (۱۲-۱۴)



(شکل-۹): نمایی از بستر آزمایش

در این آزمایش حمله ارسال مجدد با بسته‌های جمع‌آوری‌شده از سامانه پایش انجام شده است. این یک شکل به‌نسبه ساده از حمله است؛ هدف از حمله، گردآوری بسته‌های T104 و ارسال مجدد آن‌ها در زمان مناسب به مقصد مورد نظر است؛ بنابراین هدف شبیه‌سازی رفتار یک مهاجم بی‌تجربه در اتصال به شبکه است.

شکل (۱۰) جزئیات شبکه آزمون را نشان می‌دهد که متشکل از یک دستگاه فرمانده و فرمان‌بر T104 و بستر حمله لینوکس کالی[4] است؛ از نرم‌افزار ClearSCADA شرکت اشنایدر جهت پایش و کنترل مقادیر و به‌عنوان دستگاه فرمانده T104 استفاده می‌شود.



(شکل-۱۰): معماری شبکه بستر آزمایش

همچنین از RTU شرکت اشنایدر مدل ScadaPack 334E به‌عنوان دستگاه فرمان‌بر استفاده شده است. از این دستگاه جهت اندازه‌گیری، کنترل مقادیر دما و سطح مخزن، دبی و فشار لوله‌ها، پاسخ به دستورها و درنهایت ارسال آن‌ها تحت شبکه با پروتکل T104 به سامانه فرمانده استفاده شده است.

این ویژگی‌ها برای تأیید و توسعهٔ یک حمله جزو نیازهای اولیه است. شکل (۱۱) نمایی را از نرم‌افزار در حال اجرای ClearScada نشان می‌دهد. نوار منو در بالای صفحه طراحی‌شده سه حالت کنترل سطح، دبی، فشار و دما را به ما می‌دهد. در ستون سمت چپ امکان شروع و توقف فرآیند به همراه وضعیت و مقادیر متغیرها نشان داده می‌شود. در قسمت وسط، نمودار لحظه‌ای متغیر در حال کنترل به همراه مقدار حد مطلوب و مقدار خروجی نمایش داده شده است.

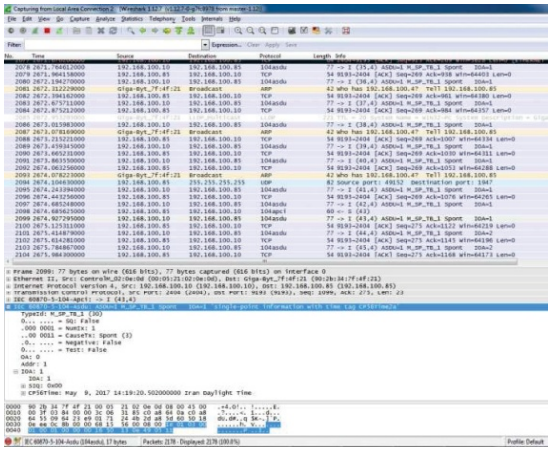
(شکل-۱۱): نمای اجرایی نرم‌افزار ClearScada

[1] Flow meter
[2] Ultrasonic
[3] Heater
[4] Kali

در این آزمایش از RTU اشنایدر استفاده شده است تا بتوان یک بستر واقعی جهت انجام حمله ارسال مجدد پیاده‌سازی کرد. مقادیر فرکانس ارسالی بسته‌ها و فیلد شناسه نوع در RTU تنظیم می‌شود. در این نمونه این فیلد دارای شماره ۳۰ از نوع اطلاعات single-point با برچسب زمانی است. برچسب زمانی می‌تواند کمتر از نصف دیالوگ تنظیم شود. فیلد علت انتقال (COT) می‌تواند همانند فرمانده تنظیم شود. در این نمونه نشانی‌های مشترک صفر است. درنهایت وضعیت اطلاعات و توصیف‌کننده‌ها می‌تواند تنظیم شود.

شکل (۱۲) ترافیک T104 بین فرمان‌بر و فرمانده را نشان می‌دهد؛ بسته‌های استفاده‌نشده برای حمله ارسال مجدد، از درگاه span سوئیچ جمع‌آوری شده‌اند. بعد از جمع‌آوری مجموعه‌ای از بسته‌ها در بازه زمانی مشخص، جهت جداسازی بسته‌های غیر T104 از بسته‌های T104 از نرم‌افزار وایرشارک استفاده می‌شود. بنابراین فقط بسته‌های مورد نیاز از ماشین هدف جمع‌آوری می‌شود که شامل بسته‌های اولیه T104، بسته‌های STARTDT، شکل خواندنی بسته M_SP_TB_1 از فرمانبر و تعدادی بسته‌های TESTFR از فرمانده که برای بررسی‌کردن فعالیت پیوند و ارتباط به کار گرفته می‌شود.

بستر حمله کالی، محلی است که بسته‌ها دوباره از آن ارسال می‌شوند. نرم‌افزار TCP Replay برای ارسال مجدد بسته‌های جمع‌آوری‌شده مناسب است. بسته‌های مجدد ارسال‌شده اگر به شکل هوشمندانه‌ای تغییر داده نشوند در لایهٔ کاربرد قابل قبول نیستند؛ زیرا بسته‌ها توسط پشته کرنل TCP/IP دور ریخته می‌شوند؛ این بسته‌ها به‌دلیل اینکه در TCP Replay مقادیر فیلدهای ACK، SYN و دنباله اعداد (#Seq) را قبل از ارسال مجدد تغییر نمی‌دهد، دور ریخته می‌شوند.



(شکل-۱۲): ترافیک مابین فرمانده و فرمان‌بر در وایرشارک

این امکان وجود دارد که بررسی رفتار مخرب حمله ارسال مجدد با استفاده از قوانین یک سامانه تشخیص نفوذ صنعتی مانند Snort و تحلیل آماری ترافیک شبکه و گزارش‌ها تشخیص داده شود؛ علاوه‌براین ازآنجایی‌که بسته‌های مجدد ارسال‌شده در لایه کاربرد بیشتر سامانه‌ها پذیرفته نخواهند شد، این سطح از حمله نباید به‌طور مستقیم عملیات فرآیند سامانه کنترل را تحت تأثیر قرار دهد. این حمله به‌دلیل این‌که به‌عنوان ترافیک مجاز به نظر می‌رسد، توسط دیواره آتش شبکه تشخیص داده نمی‌شود؛ مگر اینکه یک دیوار آتش/سامانه تشخیص نفوذ حالتمند برای ردیابی جریان‌های TCP استفاده شود. در یک شبکه با پهنای باند کم یا یک شبکه با حساسیت پایین، این دسته از حملات می‌تواند موجب اختلال در عملکرد شبکه و افزایش احتمالی زمان Time out تجهیزات شود.

با تلاش بیشتر می‌توان این امکان را به‌وجود آورد که بسته‌های جمع‌آوری‌شده دوباره ارسال شوند؛ بنابراین آن‌ها توسط کرنل دور ریخته نمی‌شوند و در لایه کاربرد پذیرفته می‌شوند. این عمل می‌تواند با یک اسکریپت پایتون انجام شود که شرایط اولیه TCP Hand shake را انجام داده و #seq را به‌درستی مدیریت می‌کند؛ برنامه‌هایی نظیر WirePlay و tcplivereplay که بخشی از پروژه TCP Replay است برای این منظور طراحی شده‌اند. قابل‌توجه است که در نوع حمله با سطح باتجربه یا پیشرفته، مهاجم با سطح اطلاعات بالا و بر اساس شناختی که از فرایند کنترل صنعتی هدف و پروتکل ارتباطی دارد، می‌تواند بسته‌های ضبط‌شده را به شکل حرفه‌ای و هدفمند تغییر دهد؛ این تغییر می‌تواند بر روی مقادیر حد مطلوب به شکل حمله تخریب غیر فیزیکی صورت گیرد که منجر به سرریز مایع مخزن شود و در فرایند کنترلی ایجاد خلل کند.

۶- آیندهٔ کاری

در ادامه قصد داریم ضمن پیاده‌سازی عملی راه‌کارهای مقاله کنونی، بر روی شناسایی چالش‌های امنیتی پروتکل‌های پرکاربرد کنترل صنعتی نظیر DNP3 وIEC 61850 فعالیت‌هایی را انجام دهیم و تلاش کنیم بر روی تجهیزات موجود صنعتی، مخاطرات امنیتی این پروتکل‌های را کاهش دهیم.

۷- نتیجه‌گیری

در این مقاله تلاش شد تا ضمن معرفی مختصری از T104 فرآیند شناخت جوانب امنیتی مختلف در رابطه با این پروتکل حاصل شود. بر اساس ساختار استاندارد T104 مرجع و برخی محصولات پیاده‌سازی‌شده، آسیب‌پذیری‌ها (مراحل طراحی، پیکربندی و پیاده‌سازی) و تهدیدهای این پروتکل استخراج و معرفی شد؛ اهم حملات شناسایی‌شده تخریب غیر فیزیکی، استراق‌سمع منفعل، ممانعت از کیفیت خدمات، دست‌کاری غیرمجاز، حملات داده‌ای، تزریق بسته، ربایش جریان کنترلی، مردی در میان غیرفعال، مردی در میان فعال و جعل هویت است. فرایند شناسایی آسیب‌پذیری‌ها و تهدیدها با بهره‌گیری از محیط آزمایشی مناسبی انجام‌گرفته است.

در این مقاله برخی راه‌کارهای امن‌سازی مرحله طراحی T104 و چالش‌های درگیر در آن بررسی شد تا دست‌کم بتوان با شناخت این مسائل امنیتی در اتخاذ راه‌کارهای امنیتی در سامانه‌های کنترل صنعتی که از این پروتکل استفاده می‌کنند، دقت بیشتری کرد و از سویی در طراحی پروتکل‌های مشابه بومی چالش‌های امنیتی بیان‌شده را موردتوجه قرارداد.

گفتنی است، پروتکل‌های دیگری نظیر IEC 61850 در صنایع، در محدوده‌های مشابه با T104، به کار می‌روند که مقالات متعددی نظیر[۲۷] به تحلیل چالش‌های امنیتی آن پرداخته و استانداردهایی نظیر IEC 62351-6 به بررسی موارد امنیتی آن پرداخته‌اند.

۸- مراجع

[1] T. Roshan K, A. Cardenas, and R. B. Bobba, "First Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC): Challenges and Research Directions," *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM*, 2015.

[2] E. Chikuni, M. Dondo, "Investing the Security of Power System SCADA," *Conference proceedings*, AFRICON, Sept. 2007.

[3] C. Gordon R, D. Reynders, and E. Wright, "Practical modern SCADA protocols: DNP3, 60870.5 and related systems," Newnes, 2004.

[4] Z. Cheah, "Testing and Exploring Vulnerabilities of the Applications Implementing IEC 60870-5-104 Protocol," M.S, KTH University, Stockholm, Sweden, 2008.

[5] F. Cleveland, W. Convenor, "IEC TC57 WG15: IEC 62351 Security Standards for the Power-System Information Infrastructure," Xanthus Consulting International.2012.

[6] M. Robinson, "The SCADA threat landscape," In: *First International Symposium for ICs & SCADA Cyber Security Research 2013. Leicester*, U.K., 2013, pp. 30–41.

[7] T. H. Morris, and W. Gao, "Industrial control system cyber attacks," In: *First International Symposium for ICs & SCADA Cyber Security Research 2013*, Leicester, U.K., 2013, pp. 22–29.

[8] T.Morris, R.Vaughn, and Y. S. Dandass, "A testbed for SCADA control system cybersecurity research and pedagogy," In: *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW '11*. New York, NY, USA, 27:127:1.

[9] P.Cambaceedes, L.Tritschler, and G. N. Ericsson, "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs," *IEEE Trans*Power Del, 2013, vol. 26 (1). pp.161–172.

[10] N. R. Saminemi, F. A. Barbhuiya, and S. Nandi, "Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks," In: *2012 2nd IEEE International Conference onParallel Distributed and Grid Computing (PDGC)*, 2012, 364–367.

[11] D.Bruschi, A. Ornaghi, and E.Rosti, "S-ARP: A secure address resolution protocol," In: *Computer Security Applications Conference*. Proceedings. 19th Annual, 2003, pp.66–74.

[12] Y.Yang, et al, "Man-in-the- middle attack testbedinvestigating cyber-security vulnerabilities in smart grid SCADA systems," In: *International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012)*, 2012, pp. 1–8.

[13] W.Gao, et al, "On SCADA control system command and response injection and intrusion detection," In: *eCrime Researchers Summit (eCrime)*, 2012, pp. 1–9.

[14] A.Timorin, (2013) atimorin/PoC2013 Available from https://github.com/atimorin/PoC2013

[15] G.Dondossola, et al, " ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds," In: *IEEE/IFIP International Conference on Dependable Systems Networks*, 2009. DSN '09, pp. 554–559.

[16] P.Maynard, K.McLaughlin, B. Haberler, "Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks," In *Proceedings of the 2nd International Symposium*

on ICS & SCADA Cyber Security Research 2014, 2014 Sep 11, pp. 30-42.

[17] Clarke, R. Gordo, D. Reynders, and E. Wright. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, 2004.

[18] Clarke, R. Gordo, D. Reynders, and E. Wright. Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, 2004.

[19] Clevland, "Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System," Frances Clevelan, d IEEE Member, PES-PSCC, 2007.

[20] IEC/TS 62351-5, Part 5: Security for any profiles including IEC 60870-5, International Electrotechnical Commission, technical specification, Edition 2.0 2013.

[21] IEC/TS 62351-3, Power systems management and associated information exchange – Data and communications security– Part 3: Communication network and system security – Profiles including TCP/IP, technical specification.

[22] IEC/ST 62351-2, Part 2: Glossary, International Electrotechnical Commission, technical specification, 2008.

[23] IEC/ST 62351-9, Part 9: Key Managment, International Electrotechnical Commission, technical specification, 2012.

[24] IEC 60870-5-104, Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, International Electrotechnical Commission, 2006.

[25] IEC/TS 60870-5-7, Part 5: Communication profile for basic telecontrol messages -Section 7: Seurity extenstion to IEC 60870-5-101 and IEC 60870-5-104 protocols (Applying IEC 62351), International Electrotechnical Commission, technical specification, Edition 1.0,2013.

[26] Pidikiti, D. Samanth, et al, "SCADA communication protocols: vulnerabilities. attacks and possible mitigations," *CSI transactions on ICT1*. Vol.2 , 2013, pp. 135-141.

[27] R.Czechowski, and B. Wiecha, "Cyber security in communication of SCADA systems using IEC 61850," 2015 Modern Electric Power Systems (MEPS). IEEE, 2015.

محمدمهدی احمدیان، تحصیلات کارشناسی خود را در رشته مهندسی کامپیوتر (گرایش نرم‌افزار) و سپس کارشناسی ارشد خود را در رشته فناوری اطلاعات (گرایش امنیت اطلاعات) پشت سر گذاشته است و در حال حاضر نامزد دکترای تخصصی رشته فناوری اطلاعات (گرایش امنیت اطلاعات) دانشگاه صنعتی امیرکبیر تهران است. نامبرده تجارب شاخصی در حوزه امنیت سامانه‌های کنترل و اتوماسیون صنعتی و پروژه‌های مرتبط مختلف (در سطوح مشاوره، طراحی، اجرا، نظارت و تدریس) با این حوزه را در کارنامک خود دارد. زمینهٔ پژوهشی مورد علاقه وی امنیت سامانه‌های کنترل و اتوماسیون صنعتی، امنیت سامانه‌های سایبر-فیزیکی، مدیریت امنیت اطلاعات، تحلیل و تشخیص بدافزارها است.

مهدی شجری، عضو هیأت علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر تهران است. ایشان مدرک کارشناسی ارشد خود را در سال ۱۹۹۳ و مدرک دکترای تخصصی خود را در سال ۲۰۰۵ در رشته علوم کامپیوتر دریافت کردند. ایشان همکاری با سازمان تحقیقات ملی کانادا و دانشگاه ترنت را به‌عنوان پژوهش‌گر و عضو هیأت علمی طی سال‌های ۲۰۰۰ تا ۲۰۰۶ در پرونده خود دارند. ایشان تجارب بسیار موفقی در حوزه صنایع فناوری اطلاعات و پروژه‌های مرتبط با این حوزه را در کارنامک خود دارند. حوزه‌های پژوهشی مورد علاقه کنونی ایشان امنیت اطلاعات، امنیت تجارت الکترونیک و امنیت سامانه‌های سایبر-فیزیکی است.