XX SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

Versão 1.0
GTL xx
22 a 25 Novembro de 2009
Recife - PE

GRUPO -XV
GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÕES PARA SISTEMAS ELÉTRICOS - GTL

IMPACTO DE MECANISMOS DE SEGURANÇA EM PROTOCOLOS SCADA

Daniel Antunes Maciel Villela(*) **Ayru Leal Oliveira Filho**

CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA - CEPEL

RESUMO

Requisitos de segurança na comunicação de dados em sistemas SCADA no setor elétrico deram origem a um conjunto de padrões no IEC pela série IEC62351 (2). Para protocolos baseados na pilha TCP/IP, a norma IEC 62351-3 (3) estabelece TLS (*Transport Layer Security*) como uma subcamada a oferecer recursos de segurança como criptografia de dados. Tais recursos permitem transmissão de dados sem violação da informação transmitida por parte de terceiros. Uma segunda alternativa neste sentido é encapsular dados transmitidos em uma sessão do tipo *Secure Shell* (SSH), procedimento também conhecido como túnel SSH. Em ambas as opções, são necessárias informações adicionais por conta de tais recursos, o que de fato gera maior demanda por banda de comunicação. Este trabalho compara o consumo de banda de comunicação pela utilização de subcamada TLS e pelo emprego de túnel SSH. Também foi analisado o recurso de compressão de dados, uma opção que é possibilitada pela inserção de TLS e SSH. O estudo foi desenvolvido através de simulações e dados oriundos de centro de controle utilizando o SAGE em ambiente fechado de testes.

Os resultados indicam que TLS e SSH realmente geram incremento na demanda em banda de comunicação. No entanto, o recurso de compressão de dados permite reduzir a banda de comunicação utilizada a um nível menor do que o nível observado para a comunicação SCADA simples, isto é, sem utilizar TLS ou SSH. Este resultado permite concluir que a adoção de TLS (ou até mesmo SSH) é viável nos sistemas SCADA de empresas do setor elétrico.

PALAVRAS-CHAVE

SCADA, TLS, SSH, Compressão

1.0 - INTRODUÇÃO

A questão da segurança em sistemas EMS/SCADA tem recebido crescente atenção do setor elétrico em todo o mundo (1). Neste sentido, o IEC publicou em 2007 o conjunto de normas IEC 62351, partes 1-4 e parte 6 (2) destinadas a cobrir vulnerabilidades de segurança em protocolos SCADA. A parte 3 deste conjunto especifica recursos do padrão TLS (*Transport Layer Security*) para protocolos SCADA que utilizam transporte de dados TCP/IP.

Protocolos seguros como TLS e SSH (*Secure Shell*) permitem garantias à comunicação de dados em rede tais como autenticação das entidades envolvidas nesta comunicação e a criptografia de mensagens. Em um ambiente de sistema de supervisão e controle, tais garantias são recomendáveis para segurança do funcionamento do sistema.

(*) Av. Horácio Macedo, n° 354 – sala D-13 – CEP 21941-911 Rio de Janeiro, RJ, – Brasil
Tel: (+55 21) 2598-6000 r. 6587 – Fax: (+55 21) 2260-6211 – Email: dvillela@cepel.br

A utilização de recursos adicionais (criptografia e autenticação) para a proteção contra ações maliciosas externas tem o custo de uma implementação com requisitos adicionais de processamento e compressão de dados, além de um custo associado de consumo de banda de comunicação. Este trabalho apresenta um estudo sobre o consumo de banda por protocolos seguros como SSH e TLS em comunicações de dados de sistemas de supervisão e controle (SCADA). Considera-se no estudo protocolos SCADA com presença crescente em sistemas de supervisão e controle, em particular no setor elétrico brasileiro. O primeiro protocolo é o protocolo ICCP que é comumente utilizado para troca de informações entre centros de controle do sistema elétrico. Um segundo protocolo é o protocolo IEC 61850 que é utilizado para troca de informações entre equipamentos (IEDs) de proteção, supervisão e controle em sistemas locais de supervisão, como em uma subestação ou uma usina. Os estudos foram conduzidos utilizando-se as implementações de ICCP e de IEC 61850 nativas do SAGE (Sistema Aberto de Gerenciamento de Energia), desenvolvido pelo CEPEL como um sistema EMS/SCADA.

Este trabalho consistiu inicialmente em uma adaptação do SAGE para suportar mecanismos do TLS nas implementações de protocolos ICCP e IEC 61850. A comunicação em túnel SSH pode ser configurada utilizando-se comandos SSH e com alterações na configuração local das máquinas do sistema SCADA. Em um segundo momento, foram coletados *logs* de sistemas reais mantidos que utilizam o SAGE no Brasil com o objetivo de emular as variações ocorridas em um sistema SCADA. Foram realizadas medidas de consumo de banda de transmissão, utilizando-se o SAGE com a implementação em TLS e SSH e com as possibilidades permitidas pelos dois protocolos de ter compressão de dados.

Os resultados indicam, como esperado, aumento de consumo de banda quando se utiliza TLS e SSH. Este aumento é conseqüência do acréscimo de informação necessário em mensagens por conta do TLS e SSH. No caso de ICCP com utilização de TLS, observou-se aumento na taxa de transmissão em até 26% da taxa de transmissão obtida com ICCP sem utilização de TLS. No entanto, como tanto SSH como TLS permitem fazer compressão de dados, nos testes realizados com esta facilidade, o consumo de banda torna-se ainda menor que o resultado obtido com protocolo sem TLS ou SSH. Isto indica que além de introduzir mais segurança a comunicação, tais protocolos oferecem, na verdade, a possibilidade de ganho de banda ao utilizar o recurso da compressão de dados. A taxa de compressão em cada caso depende do grau de redundância da informação transmitida. Nos experimentos com ICCP e utilização de TLS com compressão de dados, houve uma redução da ordem de 16% em relação à taxa de transmissão observada com ICCP sem TLS. O custo inerente à compressão de dados é um processamento maior nas estações computacionais do sistema SCADA. Entretanto, a taxa de processamento é ainda perfeitamente tolerável. Por exemplo, nos testes realizados, o emprego de TLS com compressão de dados ocasionou uma taxa de utilização de 0,15% do processamento de CPU (Pentium 4, 3 GHz). Portanto, no caso de máquinas com configuração de padrão médio atual, isto é, com a taxa de processamento e disponibilidade de memória nos padrões atuais, este custo adicional por processamento pode ser considerado pequeno.

2.0 - PROTOCOLOS PARA SISTEMAS SCADA

2.1 Ligações entre centros de controle: protocolo ICCP

O protocolo ICCP (5) é utilizado para comunicação de dados entre centros de controle. Em termos de arquitetura de redes, se situa acima de protocolo MMS através de um mapeamento de serviços entre ICCP e o protocolo MMS. No modelo OSI, o MMS é caracterizado como um protocolo de aplicação, acima das camadas de apresentação e Sessão. É utilizado transporte classe 0 e mapeamento T-SAP (7) para mapear esta pilha de níveis superiores na pilha TCP/IP.

Dentre os variados serviços definidos na especificação do protocolo ICCP, ao ter estabelecida uma associação entre dois centros de controle, os serviços mais comumente utilizados que causam tráfego na comunicação de dados são os serviços *Identify* e *Information Report*. As mensagens referentes ao serviço *Identify* são enviadas periodicamente para verificação do canal de comunicação e, apesar de serem periódicas, em termos de tamanho são pequenas. *Information Reports* são gerados na medida em que há variações de dados a serem distribuídos entre os centros de controle. Este tipo de mensagem é normalmente maior devido à taxa de variação de dados. Portanto, normalmente *Information Reports* compõem a principal parcela da taxa de transmissão de dados quando a taxa de variação de pontos na base de dados é alta.

A norma do protocolo ICCP define blocos de conformidade, que são níveis de recursos que um determinado sistema ICCP pode suportar. Existe o nível básico, denominado bloco 1, que define recursos para aquisição de dados (integridade). Há também outros recursos como reporte por exceção, que é definido para bloco 2 de conformidade. Para a comunicação entre centros de controle é necessário como parte da negociação em protocolo ICCP a divulgação dos blocos de conformidade que são atendidos pelos sistemas em questão.

O bloco 3 de conformidade, em particular, permite uma demanda por banda de transmissão menor pois ao utilizar seus recursos um sistema transmite uma seqüência de pontos contendo um identificador numérico do ponto em vez de transmitir o identificador alfanumérico, além de simplificar o formato de dados pois deixa de utilizar codificação completa em ASN.1. Isto reduz a quantidade de informação a ser transmitida e normalmente permite redução significativa da demanda em banda de transmissão. No entanto, mesmo estes dados a serem transmitidos em bloco 3 potencialmente apresentam redundância. Portanto, ao utilizar um algoritmo de compressão de dados (não especificado na norma do protocolo ICCP) a quantidade de dados a ser transmitida se torna ainda menor.

2.2 Protocolo IEC 61850.

O protocolo IEC61850 foi definido para controle e supervisão de equipamentos do sistema elétrico como IEDs (*Intelligent Electronic Devices*). Normalmente estes equipamentos encontram-se em subestações e usinas geradoras. O protocolo IEC61850 permite troca de dados entre equipamentos em uma rede local de forma bastante rápida através de pacotes de dados SMV (Sampled Values) e pacotes GOOSE, que não utilizam TCP/IP. Para comunicação com equipamentos centrais de supervisão, no entanto, a norma define uma pilha de protocolos bastante semelhante ao utilizado para ICCP, pois o IEC61850 também é mapeado no protocolo MMS (6). Por conseguinte, utiliza a mesma pilha de protocolos, constituída por protocolos de modelo OSI para níveis superiores e TCP/IP para níveis inferiores e um mapeamento ditado pela RFC 1006 para junção dos dois modelos.

Com base nisso também é possível fazer experimentos utilizando IEC61850 (descartando mensagens SMV e GOOSE) sobre túnel SSH e TLS.

2.3 TLS e SSH em SISTEMAS SCADA

TLS e SSH oferecem segurança a nível 4, isto é, nível de transporte em arquitetura de redes de computadores. Em particular oferecem segurança como uma "subcamada" acima de TCP/IP. Implementam opcionalmente autenticação utilizando, por exemplo, certificados RSA. Implementam também a codificação por criptografia e a troca de chaves periódica por mensagens autenticadas (*Message Authentication Code – MAC*). A autenticação tem por objetivo garantir que as partes envolvidas na comunicação são legítimas. A criptografia tem por objetivo garantir que mensagens não podem ser lidas em algum ponto entre transmissor e receptor. A troca de chaves por mensagens autenticadas tem por objetivo evitar um pacote legítimo ser utilizado em um contexto diferente, como por exemplo em outro intervalo de tempo.

Atualmente o IEC estabeleceu TLS como requisito da norma IEC62351-3 (5) para segurança em protocolos SCADA. Esta parte da norma visa perfis de pilha de protocolos baseadas no TCP/IP. Portanto, o esquema definido é válido para IEC60870-5-104, DNP3, ICCP e IEC61850. Há outros aspectos da norma que se referem a requisitos em nível 7 (Aplicação) que estão fora de escopo do presente documento.

2.3.1 TLS

A especificação TLS (4) origina-se da especificação *Secure Socket Layer* (SSL). É definido um formato TLS para um pacote que é encapsulado em um pacote TCP/IP. Para a implementação no SAGE foi utilizada a biblioteca OpenSSL. A adaptação para utilização de TLS foi implementada no transportador MMS[1] do SAGE o que permitiu que a camada TLS fosse adicionada em ambos os protocolos ICCP e IEC61850 (perfil que utiliza TCP/IP).

O protocolo TLS ainda possibilita utilização de algoritmo de compressão de dados (9). No entanto, não está ainda definido um mecanismo automático para que cliente e servidor se negociem sobre qual algoritmo a utilizar. Como foram realizados teste locais, o procedimento normal de testes foi ter cliente e servidor já pré-configurados com o mesmo algoritmo de compressão, no caso codificação *Lempel-Ziv* (o mesmo algoritmo utilizado pelo utilitário gzip).

2.3.2 Túnel SSH

O procedimento para implementar um túnel criptografado é essencialmente encapsular as mensagens do protocolo desejado em conexões SSH (8) estabelecidas. A implementação testada, foram criados túneis SSH para ambos os sentidos de comunicação entre os pontos envolvidos. Para colocar a comunicação de dados do SAGE via túnel SSH, foram necessárias alterações no sistema local de testes, contendo inclusive ajustes de configurações que refletem a comunicação através dos túneis e não diretamente entre as partes.

[1] Apesar do MMS ser um protocolo de aplicação, comumente nos referimos ao "transporte" MMS porque sobre ele trafegam os protocolos ICCP e IEC61850.

Da mesma forma que o TLS permite a compressão de dados, o túnel SSH também pode ser ativado com compressão; opção inserida no estabelecimento do túnel. O algoritmo default é também o *Lempel-Ziv*.

3.0 - EXPERIMENTOS

3.1 Metodologia

Foram realizados experimentos utilizando-se duas máquinas, cada uma com dois processadores Intel P4/Xeon 3,2 GHz e 2 Gbytes de memória RAM. Cada máquina executa o SAGE sobre Linux, requerendo recursos para os processos básicos do SCADA (base de dados, alarmes, aquisição e distribuição de dados), para o MMS e para o conversor de protocolo, que pode ser ICCP ou IEC61850 dependendo do estudo desejado.

A variação de pontos pode obedecer dois modelos criados para simulação. Um primeiro foi implementado em script *perl* que gera número de variações segundo distribuição gaussiana com média e variância determinadas por usuário. Este script realiza chamadas por intermédio da ferramenta de simulação do SAGE (sim-tr) que efetivamente simula as múltiplas variações de pontos. O intervalo de tempo entre variações de pontos segue distribuição exponencial. Este modelo foi utilizado com uma base criada exclusivamente para testes.

Outro modelo para variação de pontos utiliza a ferramenta ads, parte integrante do SAGE, e uma base de dados real. Uma das máquinas executa a ferramenta ads que permite a um sistema SAGE sincronizar a base de dados com a base de dados em outro sistema SAGE. Um sistema SAGE instanciado para ambiente de testes pode obter dados de um sistema real oriundo de outro sistema SAGE e distribuir dados dentro do ambiente de teste. Como a ferramenta ads permite apenas ler os dados, o ambiente de testes tem uma base de dados replicada de um ambiente real, sem interferir no sistema real. O ambiente de testes foi criado para replicar uma ligação do CNOS com o centro COSR-NE ambos do ONS. A comunicação entre as duas máquinas para distribuição de dados ocorre via protocolo ICCP, utilizando os recursos do bloco 3 de conformidade.

No caso do espelhamento de dados do CNOS via ads atualmente em operação no CEPEL, os dados são obtidos a cada 3 minutos. Foi elaborado um script que realiza a cada 5 segundos a troca de dados previamente obtidos via ads em intervalos de 3 minutos. O resultado é ter todas as variações em um intervalos de tempo de 3 minutos “observadas” em um intervalo de tempo mais curto, gerando mais *Information_Reports*, do que ao reproduzir os mesmos dados em 3 minutos. Portanto, tal procedimento acelera a troca de dados e gera um tráfego de dados mais intenso.

Os experimentos consistiram em capturar pacotes relativos à comunicação ICCP entre as duas máquinas utilizando-se a ferramenta *dumpcap* em n intervalos de 10 minutos cada. Para cada intervalo obtém-se estimativas para quantidade total de dados transmitida em bytes (a fim de obter-se a taxa média de transmissão), taxa máxima de transferência de dados, taxa média de pacotes transferidos e taxa máxima de pacotes transferidos. Estas medições ocorrem nos dois sentidos da comunicação. A análise dos dados é realizada *post mortem* uma vez que os pacotes já foram capturados. Para medir as taxas de transmissão de dados e de pacotes, utiliza-se a ferramenta *tethereal* e scripts desenvolvidos em *perl* especialmente para tal propósito. A razão para capturar múltiplos intervalos é computar intervalos de confiança para os valores medidos. O método estatístico foi computar intervalos de confiança com 95% em distribuição *t-student*.

O método de criptografia utilizado foi AES-256 (chaves de 256 bits) tanto nos experimentos com SSH quanto com TLS. Este método é considerado o mais forte dentre os possíveis métodos disponíveis no pacote OpenSSL. A camada TLS foi configurada por *default* com *ciphersuite* TLS1_TXT_RSA_WITH_AES_256_SHA. Esta suíte é composta pelo uso do protocolo TLS com certificados digitais em RSA, criptografia AES-256bits e mecanismo SHA para troca de mensagens de autenticação para troca de chaves. O túnel SSH foi criado utilizando-se criptografia por algoritmo com chave AES 256 bits CBC e mecanismo HMAC-MD5 para mensagens de autenticação para troca de chaves.

3.2 Resultados para simulação

A ferramenta mmf do SAGE permite a análise do tráfego de mensagens trocadas com o SAGE. Ao capturar logs do mmf entre o CNOS (ONS) e centro de controle da CEMIG, pode-se estudar a distribuição do número de *Information Reports* que corresponde ao modelo utilizado para variação de pontos, i.e., uma média de pouco mais de 70 *Information Reports*. Foram realizados testes com ferramenta de simulação do próprio SAGE, sim-tr, de forma a simular tal taxa de variação de pontos. Nos testes o número de pontos a variar a cada iteração tem distribuição gaussiana com média 70 e variância 20. O intervalo de tempo entre variação de pontos tem distribuição exponencial com média 1 segundo.

A Figura 1 apresenta a distribuição de número de variáveis observada na simulação seguindo-se procedimento descrito na seção anterior. Esta distribuição é apresentada na forma de um histograma onde se observa uma distribuição gaussiana consistente com o modelo utilizado para simulação.

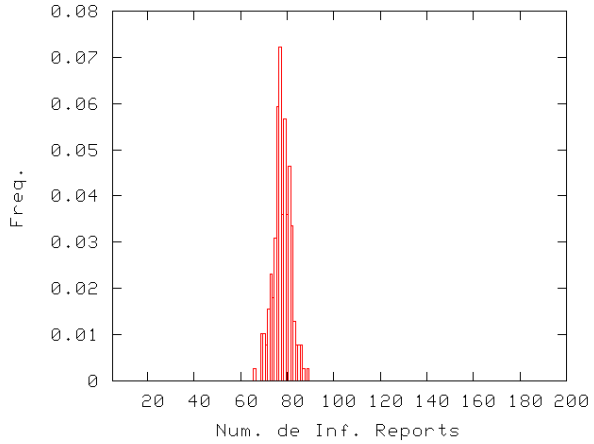


Figura 1 – Histograma de número de *Information Reports* na simulação.

A Figura 2 (a) apresenta as taxas médias de transmissão observadas nas simulações com sim-tr. O eixo vertical apresenta a taxa de transmissão (em kbit/s) e apresenta-se barras verticais correspondentes a resultados obtidos para a comunicação de dados via ICCP puro (i.e., sem TLS ou SSH), via TLS, via TLS com compressão de dados (TLS/c), via SSH e via SSH com compressão de dados (SSH/c). O aumento da taxa de transmissão com a utilização de TLS é da ordem de 26%. Já para túnel SSH, o aumento é da ordem de 14%. Para os casos de TLS e SSH, ambos com compressão de dados, a taxa de transmissão reduz-se. No caso de TLS com compressão de dados, observa-se uma queda de aproximadamente 16%. No caso de SSH com compressão de dados, a queda é de aproximadamente 31%. Deve-se observar que o decréscimo é computado em relação ao desempenho obtido pelo ICCP puro. O grau de compressão em cada um dos casos é aproximadamente equivalente.

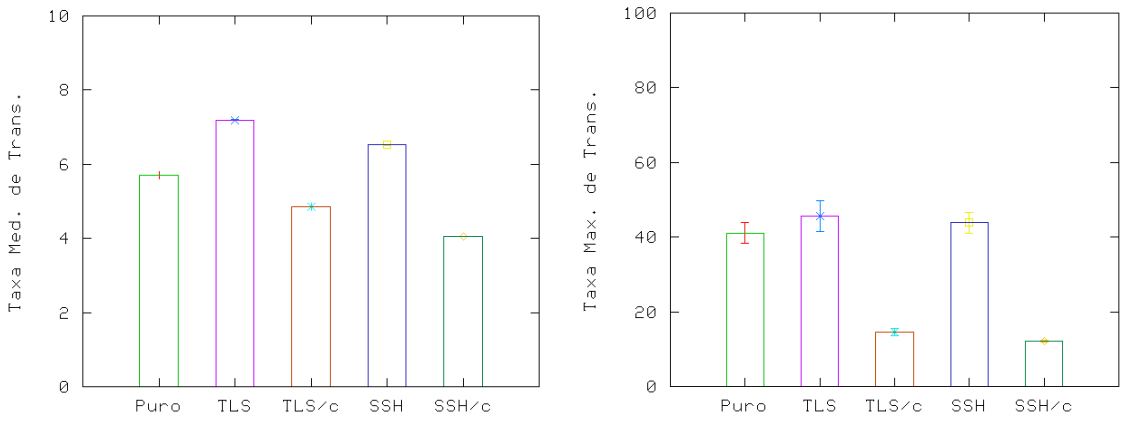
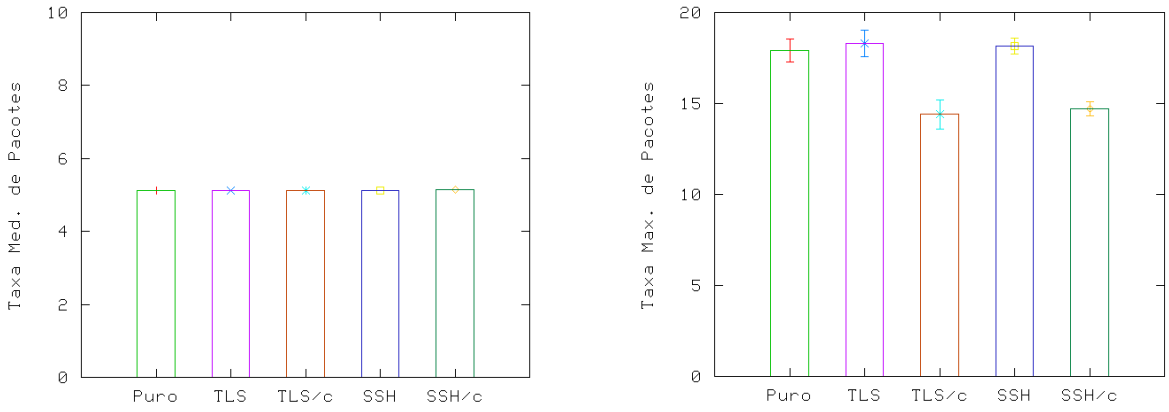


Figura 2 – Taxa média (a) e máxima (b) de transmissão observada nas simulações com o simulador sim-tr.

A Figura 2(b) apresenta a taxa máxima de transmissão observada nas simulações com sim-tr. O eixo vertical apresenta a taxa máxima medida em kbit/s. O intervalo de confiança é apresentado no topo de cada barra. Observa-se no caso de TLS e SSH um aumento pequeno na taxa máxima. Para os protocolos TLS e SSH com compressão de dados, no entanto, há uma redução significativa da taxa máxima de transmissão de dados.

A Figura 3 apresenta resultados obtidos para medições de taxa média (a) de pacotes e máxima (b) de pacotes enviados no eixo vertical. Observa-se que a taxa média de pacotes praticamente não teve variação independente se o protocolo o MMS está “puro”, ou sobre TLS ou SSH, ou ainda com TLS ou SSH e compressão de dados. Como nas figuras anteriores observou-se aumento de taxa de transmissão no caso de SSH e TLS sem compressão de dados e redução de taxa de transmissão de dados com a compressão de dados, pode-se concluir que o efeito de cada um destes protocolos afeta a quantidade de dados via cabeçalhos adicionais e por redução de *payload* (no caso de compressão de dados) e não afeta o número de mensagens trocadas.



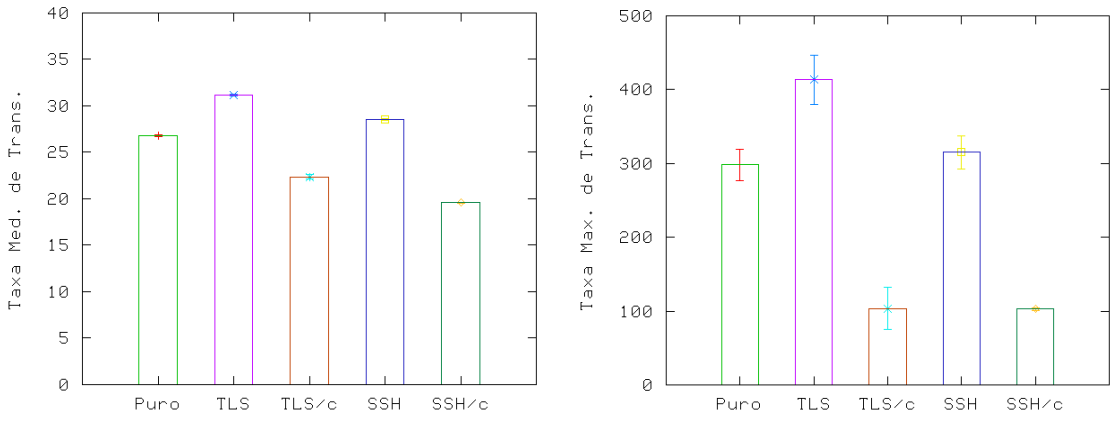
(a) (b)

Figura 3 – Taxa média de pacotes (a) e taxa máxima de pacotes (b) observados nas simulações com ferramenta sim-tr.

Foi medido o consumo de processamento de CPU nos casos em que a transmissão ocorre sem TLS e também com a utilização de TLS com compressão de dados. Aqui foi utilizada uma máquina com processador Intel Pentium 4, 3 GHz e 1,5 Gbytes de memória RAM. O resultado foi um esperado aumento na demanda por processamento. Com a transmissão sem TLS, o processo responsável por transmissão e recepção de mensagens MMS requisitou da CPU em média uma fração de 0,1 segundo para cada 100 segundos decorridos. Isto corresponde a 0,1% de consumo médio de CPU. No caso de TLS com compressão de dados, o consumo médio foi de 0,15%. Apesar de ser um aumento significativo, pois é da ordem de 50% maior, em termos absolutos a taxa de utilização de 0,15% é perfeitamente tolerável em um sistema.

3.3 Resultados em simulações com ferramenta ADS

A Figura 4(a) mostra a taxa média de utilização em um canal ICCP em kbit/s. O eixo vertical apresenta valores para taxa média de utilização. O eixo horizontal apresenta as diferentes configurações. Observa-se efeitos bastante similares aos observados nas simulações com sim-tr. O aumento de taxa de transmissão introduzido com a utilização de TLS é da ordem de 16%. O aumento de taxa de transmissão introduzido com SSH é da ordem de 6%. Quando se emprega compressão de dados, há uma redução da taxa de transmissão de dados. No caso de TLS com compressão de dados, esta redução é de aproximadamente 16%. No caso de SSH com compressão de dados, esta redução é de aproximadamente 27%. A Figura 4(b) apresenta a taxa máxima de transmissão de dados observada nas simulações com ferramenta ads. Novamente, observa-se aumento significativo para TLS e redução significativa no pico da taxa de transmissão quando se utiliza compressão de dados, sendo ou TLS ou SSH empregado em cada caso.



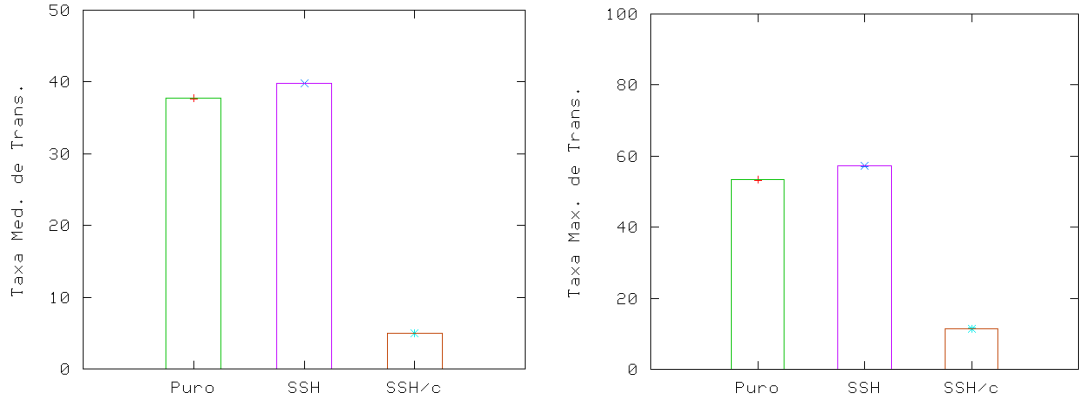
(a) (b)

Figura 4 – Taxa média (a) e máxima (b) nas simulações com ferramenta ads

3.4 Experimentos com IEC61850

Para experimentos com IEC61850 foi utilizado o simulador de testes para IEC61850 da *Tamarack Consulting, Inc.*, que simula um IED com geração periódica de variações em pontos definidos. Foi configurado o simulador com intervalo de simulação 1000 ms. A cada intervalo de 1 segundo o simulador gera *Information Reports* de acordo com modelo próprio definido.

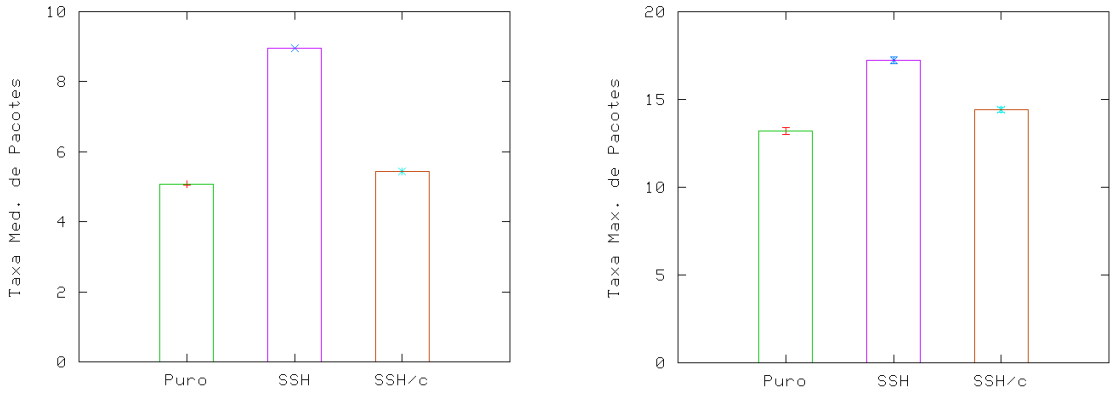
O simulador não tem suporte para TLS. Portanto não é possível fazer testes da implementação do SAGE utilizando TLS com o simulador. No entanto, é possível fazer testes configurando túnel SSH. Isto decorre do fato de que para o simulador as mensagens de protocolo aparecem vindo da máquina local em canal sem criptografia, uma vez que ao chegar à ponta do túnel as mensagens são redirecionadas para a outra porta na máquina local em canal *loopback*.



(a) (b)

Figura 5 – Taxa média (a) e máxima(b) de transmissão para IEC61850

A Figura 5(a) apresenta a taxa média de transmissão para IEC61850 ao utilizar um transportador MMS “puro”, ou seja sem TLS ou SSH, e a taxa média de transmissão nas simulações com IEC 61850 utilizando-se SSH (com e sem compressão de dados). No caso de SSH observa-se um aumento pequeno (da ordem de 6%) de taxa de transmissão de dados em comparação com a configuração “pura”. No caso de SSH com compressão de dados, houve uma redução significativa na taxa de transmissão de dados. Esta redução foi de aproximadamente 86%, provavelmente resultado de alto grau de redundância nos dados gerados pela simulação. A Figura 5(b) apresenta a taxa máxima de transmissão nas simulações para IEC61860 com simulador *Tamarack.* Os resultados foram qualitativamente similares aos obtidos para a taxa média de transmissão. Há aumento pequeno na taxa máxima de transmissão na configuração com túnel SSH, mas também há uma redução drástica no pico da taxa de transmissão ao empregar compressão de dados.



(a) (b)

Figura 6 – Taxa média (a) e máxima(b) de pacotes em comunicação via IEC 61850.

A Figura 6 apresenta as taxas de transmissão de pacotes nas simulações para IEC61850. A Figura 6(a) apresenta a taxa média de transmissão de pacotes nas simulações para IEC61850. A Figura 6(b) apresenta a taxa máxima de transmissão de pacotes nas simulações para IEC61850. Nesta simulação observou-se aumento significativo do número de pacotes ao utilizar SSH sem compressão de dados.

4.0 - CONCLUSÃO

Foi realizado um estudo sobre o uso de protocolos de transporte seguros para sistemas SCADA, em particular, usando os protocolos ICCP e IEC61850. A utilização de métodos de criptografia normalmente aumenta a taxa de transmissão de dados por causa de cabeçalhos de protocolo adicionais, bits de enchimento etc. Mas a opção de utilização de compressão de dados reduz a taxa de transmissão de dados a um nível inferior ao observado sem utilizar TLS ou SSH. Foi observado normalmente um maior *overhead* em taxa de transmissão ao utilizar TLS do que comparando-se ao observado para túnel SSH. No entanto, como há uma redução de taxa de transmissão ao empregar-se um mecanismo de compressão de dados (no caso, o mesmo utilizado no utilitário gzip), a utilização de qualquer um dos dois pode ser recomendada. Como TLS está sendo especificado em norma IEC (IEC62351), a opção TLS assumiria um caráter normativo. A opção de compressão impõe maior peso no processamento das máquinas envolvidas na comunicação de dados. Os dados de aumento de demanda de processamento levantados neste estudo indicam que este requisito não afetaria o desempenho dos sistemas de comunicação dada a atual capacidade de processamento das máquinas tipicamente utilizadas para a função.

REFERÊNCIAS BIBLIOGRÁFICAS

(1) CLEVELAND, F., “IEC TC57 Security Standards for the Power System’s Information Infrastructure Beyond Simple Encryption”, Anais da conferência Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES**,** maio de 2006, pp. 1079—1087.

(2) IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION , “Power systems management and associated information exchange - Data and communications security”, IEC 62351, junho de 2007.

(3) IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION , “Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP”, IEC 62351-3, junho de 2007.

(4) Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, Abril de 2006.

(5) IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION, “Telecontrol equipment and systems - Part 6-505: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 User guide”, IEC/TR 60870-6-505, edição 1.1, dezembro de 2006.

(6) IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION, “Communication Networks and Systems in Substations, Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3”, IEC 61850-8-1, maio de 2004.

(7) Pouffary, Y., e Young, A., “ISO Transport Service on top of TCP (ITOT)”, março de 1997.

(8) Ylonen, T., e Lonvick, C., “The Secure Shell (SSH) Protocol Architecture”, RFC 4251, janeiro de 2006.

(9) Rescorla, E., “SSL and TLS: Designing and Building Secure Systems”, Addison-Wesley Professional, outubro de 2000.

DADOS BIOGRÁFICOS

Daniel Antunes Maciel Villela
Nascido no Rio de Janeiro, RJ, em 30 de maio de 1974.
Doutor em Engenharia Elétrica (2005) pela Columbia University (NY-EUA), Mestre em Engenharia Elétrica (1998) pela COPPE/UFRJ e Engenheiro Eletricista com ênfase Eletrônica (1997) pela UFRJ.
Empresa: Centro de Pesquisas de Energia Elétrica – CEPEL, Departamento de Automação de Sistemas, desde 2006.

Ayru Leal de Oliveira Filho
Nascido em Juiz de Fora, MG, em 21 de novembro de 1964.
Doutor em Sistemas e Computação pela COPPE/UFRJ (2000), Mestre em Sistemas e Computação pelo IME/RJ (1990) e Engenheiro Eletricista pela Universidade Federal de Juiz de Fora (1987).
Empresa: Centro de Pesquisas de Energia Elétrica – CEPEL, Departamento de Automação de Sistemas, desde 1988.