Simulação Aplicada à Infraestrutura da Rede Elétrica com *Smart Grid* Empregando Comunicação Sem Fio

Alcides Ortega, Ailton Akira Shinoda, Christiane Marie Schweitzer
UNESP – Avenida Brasil, 56 – Centro15385-000 Ilha Solteira, SP

***Resumo* — Este artigo apresenta um estudo sobre a utilização de redes WLAN IEEE 802.11 no sistema de comunicação em redes elétricas inteligentes (*Smart Grid*) através de simulações. O simulador utilizado foi o *Network Simulator* (NS-2), a proposta do artigo é planejar e executar simulações do protocolo de comunicação IEEE 1815 DNP3 encapsulado sobre TCP/IP em redes WLAN, a fim de avaliar o desempenho do sistema de monitoramento em infraestrutura crítica como a distribuição de energia elétrica.**

***Palavras-Chave* — NS-2, *Smart Grid*, WLAN.**

I. INTRODUÇÃO

O sistema da rede elétrica convencional tem o fluxo de energia de forma unidirecional, onde a geração da energia é feita em grandes plantas, transmitida até a central de distribuição (subestações) e finalmente distribuída aos consumidores finais e industriais. Já as redes elétricas inteligentes (*Smart Grids)* referem-se à modernização da rede de energia através do uso intensivo de técnicas modernas de tecnologia da informação e comunicação (TIC), para oferecer qualidade, eficiência e garantir maior confiabilidade ao sistema de energia elétrica.

No *Smart Grid* os fluxos de energia e de comunicação são bidirecionais, o consumidor poderá gerar energia também através de fontes alternativas como painéis solares. As redes elétricas inteligentes englobam uma tecnologia atualizada em áreas como a eletrônica de potência, geração distribuída através da incorporação de recursos de fonte de energias renováveis (micro redes), maior participação dos consumidores. O objetivo é estabelecer uma rede mais segura e confiável, econômica, limpa e ecológica [1].

Em virtude da diversidade de sistemas e topologias de comunicação existentes na área de automação da rede de transmissão de energia, há uma grande quantidade de circuitos e interfaces eletrônicas gerando uma dificuldade na montagem de cenários, além disso, a construção de *setup* com equipamentos reais torna-se muito onerosa [2]. A simulação é uma ferramenta conveniente nesses casos e comumente empregada em análises ou desempenhos de cenários.

A monitoração e controle do *Smart Grid* são realizados através do protocolo de comunicação. Existem vários protocolos de comunicação utilizados no *Smart Grid* com padrão proprietário ou aberto. Entre os padrões abertos comumente utilizados nos *utilities* na América do Norte e na América do Sul está o IEEE 1815 *Distributed Network Protocol version 3.0* (DNP3.0), que utiliza arquitetura em camadas [3].

O DNP3 adere a um protocolo simplificado de três camadas proposto pela IEC (*International Electrotechnical Commission*) para implementações mais simples, chamado de EPA (*Enhanced Performance Architecture*).

Essa proposta foi apresentada para utilização do DNP3 em aplicações de pequeno e grande porte, comunicação segura, com moderada velocidade e baixa/média transmissão de dados. A vantagem deste protocolo é a flexibilidade que permite o uso em qualquer plataforma de *hardware,* além da grande variedade de comandos para ser utilizados dependendo da aplicação escolhida [4].

Idealmente, uma rede de comunicação em aplicações críticas, como o *Smart Grid,* deve ser altamente confiável, extremamente segura e resiliente a falhas. Uma ferramenta que pode auxiliar, na análise ou desempenho da rede de comunicação a ser implantado, é um simulador de redes a evento discreto como o NS-2 (*Network Simulator V.2*). O NS-2 incorpora o protocolo DNP3 através do encapsulamento para simulações em redes *ethernet* LAN (*Local Area Network)*, WLAN (*Wireless Local Area Network*), MAN (*Metropolitan Area Network)* e WAN (*World Area Network*) sobre TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Isso permite a montagem de vários cenários e resultados que só poderiam ser obtidos em testes restritos de laboratório (em pequena escala) ou testes subdimensionados de campo, economizando tempo, custo e equipamentos.

Optou-se pela utilização do NS-2 nesse trabalho pelo fato de ser uma ferramenta de simulação de rede de comunicação amplamente empregada no universo acadêmico. O *software* possui código fonte *open source* com linguagem de programação em C/C++ e Otcl. E permite desenvolver novos *patch* com novas funções ou até mesmo adaptar *patch* já existente a fim de utilizar com novas tecnologias de comunicação [5].

Este artigo está dividido da seguinte forma: a seção II apresenta o protocolo DNP3. A seção III apresenta o modelo NS-2/DNP3 que opera a simulação do protocolo de comunicação dentro do NS-2, as simulações do protocolo DNP3 sobre TCP/IP em rede WLAN. A seção IV apresenta alguns resultados preliminares obtidos do simulador. Por fim,

Este trabalho foi parcialmente financiado pela Padtec S/A. e pela CAPES.
Alcides Ortega, ortega.tex@gmail.com, Ailton Akira Shinoda, shinoda@dee.feis.unesp.br, C. M. Schweitzer, chris@mat.feis.unesp.br.

a seção V apresenta as conclusões.

II. PROTOCOLO DNP3

O DNP3 é um protocolo de comunicação aberto, com duas classes de dispositivos definidos. Estação central (*Master),* dispositivos com algum poder de processamento e armazenamento de dados. São interligadas aos dispositivos localizados em campo (linhas de transmissão, sub-estações, transformadores) através das estações remotas (*OutStation*) , encarregados de coletar dados dos sensores e enviar a estação central [6].

O padrão DNP3 oferece quatro tipos de topologias: Ponto-a-ponto, Multiponto, Hierárquica e Concentrador de dados [7]-[8].

A. Camadas do Protocolo DNP3

Camada do usuário (*User Layer)*: a estação central interage com a base de dados e solicita os dados da estação remota. Na estação remota, o *software* extrai as informações coletadas para enviar para a estação central através das funções da camada de aplicação as mensagens.

Camada de Aplicação DNP3: a estação central (*Master)* organiza e envia mensagens para a estação remota (*Outstation)* para requerer informações, realizar função especial ou executar um comando. A estação remota gera a mensagem apropriada dependendo do requerimento e envia a mensagem para a estação central. O tamanho do fragmento (pacote) depende do tamanho do *buffer* do dispositivo na qual se tem um intervalo entre 2048 e 4096 *bytes*.

Função Transporte do DNP3: é uma função incorporada na camada de aplicação, limita a dividir uma mensagem da camada de aplicação em pacotes menores para serem enviados pela camada de enlace. Na recepção, a função transporte monta os vários segmentos em um fragmento e notifica a camada de aplicação que apresenta um fragmento recebido já pronta disponível.

Camada de Enlace do DNP3: é a camada encarregada de assegurar que a transmissão de dados pela camada física seja confiável realizando detecção de erros CRC *(Cyclic Redundancy Check).* O CRC é um esquema amplamente utilizado na verificação da integridade dos dados, no protocolo DNP3 ele ocupa um espaço de dois octetos (2 *bytes* = 16 *bits*) são anexados após cada quadro (16 octetos) de dados enviados, incluindo os campos do cabeçalho.

A verificação de redundância cíclica é gerada com base no polinômio (1).

$$X^{16} + X^{13} + X^{12} + X^{10} + X^8 + X^5 + X^2 + 1 \qquad (1)$$

Considerando que o polinômio forma um número binário de 17 *bits* e cada termo presente no polinômio determina a existência de um 1 e cada ausência corresponde a zero, esse número é invertido *bit*-a-*bit* e anexado a cada quadro de até 16 octetos, inclusive aos 8 octetos do cabeçalho.

Camada física do DNP3: o DNP3 utiliza tipicamente interface física serial (RS-232 ou RS-485), utilizando vários meios de transmissão (cabo par trançado, fibra ótica, rádio, satélite), no entanto, em aplicações recentes têm sido utilizado as implementações com conexões *ethernet* DNP3 LAN.

B. DNP3 sobre TCP/IP

Inicialmente o protocolo DNP3 foi projetado para ser usado em enlace serial com comunicação ponto-a-ponto entre central e remoto, no qual o canal de comunicação possuía banda estreita.

Foi desenvolvido levando-se em conta que o meio de comunicação está sujeito às interferências e distorções. Com o passar dos anos houve a necessidade da expansão da comunicação com redes de maior porte e capacidade. Sendo assim, utilizou-se a implementação de uma nova versão levando em consideração o protocolo TCP/IP.

A Fig. 1 apresenta a implementação do padrão DNP3 sobre o protocolo TCP/IP, de maneira que as camadas anteriormente citadas não se alteram, exceto o método de sincronização de tempo. Entretanto o envio de mensagem transparente é independente do protocolo TCP/IP.

As confirmações na camada de enlace não são utilizadas, somente a confirmação na camada de aplicação é empregada similarmente ao que ocorre no meio de transmissão serial.

A interface na camada de gerenciamento de controle e a camada de transporte do protocolo TCP/IP são implementadas através de um API (*Application Program Interface*). O protocolo TCP/IP é composto por dois protocolos na camada de transporte: TCP e UDP (*User Datagram Protocol*). Sendo assim, dispositivo que suporte DNP3 deve também ter suporte a ambos os protocolos.

Quando não há a recomendação/exigência da atribuição de endereços IP aos dispositivos que utilizam DNP3, o número da porta designado geralmente para esta aplicação é 20000.

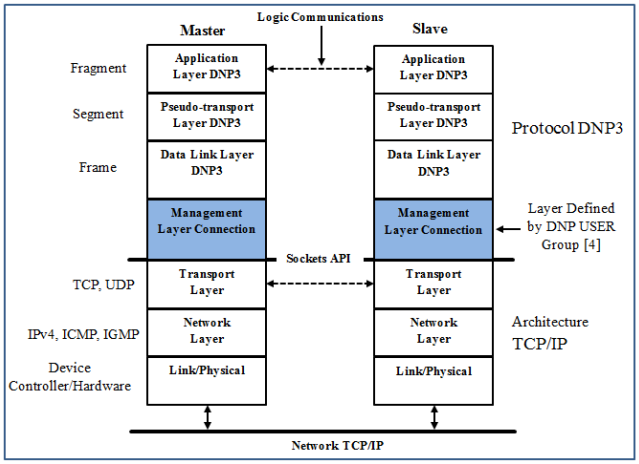

Fig. 1. DNP3 sobre TCP/IP [7]

A camada de gerenciamento do controle promove a interface entre as camadas dos protocolos DNP3 e TCP/IP. É encarregada de estabelecer e encerrar conexões TCP, transmitir, aceitar datagramas (protocolo UDP) ou segmentos

(protocolo TCP) e enviar parte dos quadros DNP3 entre a camada de enlace do protocolo DNP3.

Os níveis de implementação se dividem em três:

- Nível 1 é composto de funções básicas do protocolo DNP3, os demais são opcionais e estão orientados a estabelecer comunicação com IEDs (*Intelligent Eletronic Device).*
- Nível 2 permite mais funções, grupos e variações, os IEDs são mais sofisticados e RTUs *(Remote Terminal Unit*) com centenas de pontos (*tags*).
- Nível 3 é aquele que suporta todas as funcionalidades do protocolo.

O funcionamento do DNP3 sobre uma rede *Ethernet* e realizada mediante o encapsulamento de dados. De forma que os quadros da camada de enlace de dados DNP3 sejam encapsulados sobre os segmentos da camada de transporte TCP/IP.

O DNP3 utiliza as mensagens do TCP/IP para transportar mensagens por meio de redes *LAN/MAN/WAN*. As recomendações dos membros do grupo DNP *user group* [7] são as seguintes:

- As confirmações da camada de enlace de dados DNP3 devem ser desabilitadas, porque o TCP se encarrega de garantir uma conexão confiável do início ao fim;
- A camada física recomendada é *Ethernet*;
- Todos os equipamentos devem suportar TCP e UDP;
- TCP deve ser usado para rede *WAN* porque é um protocolo orientado a conexão e confiável;
- O modelo *Enhanced Performance Architecture* (EPA) da camada na qual se baseia o protocolo DNP3 não se altera.

A camada pseudotransporte e de enlace de dados são os elementos e serviços essenciais. Os serviços de direcionamento e detecção de erros realizados na camada de enlace de dados do DNP3 são requeridos para trabalhar junto com a arquitetura TCP/IP.

III. MODELO DE DNP3 NO NS-2

Inicialmente foi desenvolvido um *patch* para o NS-2 com um gerador de tráfico DNP3 com nível de implementação 1 por [9] para simulações em redes cabeadas. Com a necessidade de estender simulações em rede *wireless* foi necessário implementar neste *patch* a funcionalidade para ser utilizada tanto em redes *wired* como *wireless*, baseado no aplicativo já existente no NS-2 do TCP: *Application/*TcpApp com as características de transmitir dados das aplicações HTTP (*Hyper Text Transfer Protocol).*

O *Patch* desenvolvido em questão, foi somente a implementação do protocolo DNP3, baseado no funcionamento do TcpApp já existente no NS-2, não havendo a necessidade de alteração do protocolo TCP/IP existente.

O TcpApp transmite dados de forma confiável e ordenada, o <comando> será executado no destino sendo informado o comando e o tamanho do pacote para iniciar a simulação. Através deste gerador de tráfego DNP3 pode-se fazer a simulação das operações básicas como o uso de mensagens não solicitadas, leitura, escrita, função de *restart* de uma estação escrava e funções de seleção e operação.

Para realizar a validação da aplicação, foi implementado um sistema de mensagens que permite identificar a estação transmissora de mensagem, receptora de mensagem, o tamanho e quantidade de pacotes com seu valor de tempo na simulação. O sistema de mensagem implementado tem a seguinte estrutura:

<t. de sim.><*Master/Outstation*><*recv*/*sended*><cmd><pkt\#>.

O campo tempo de simulação (<t. de sim.>) é dado pelo comando de OTcl "[\$ns *now*]" com finalidade de marcar o tempo do evento que está ocorrendo. O campo *Master* refere-se ao fato de que o evento ocorreu na estação central, enquanto o *Outstation* refere-se à estação remota.

O terceiro campo "*recv"* indica que a estação recebeu uma mensagem enquanto "*sended"* que uma mensagem foi enviada. O campo "cmd" define a função a ser executada, existindo atualmente cinco funções principais: *Read, Write, Select and Operate, Restart e Event.* O último campo, "pkt\#" define o número de pacotes enviados quando é necessária uma segmentação pelo fato do tamanho da informação ser grande, ou seja, quando o tamanho da informação ultrapassar a quantidade de 292 *bytes* a mensagem será fragmentada.

Nas simulações pode-se construir o cenário de uma subestação onde o local é propício a ruídos que interferem na comunicação de dados, nesses ambientes são avaliadas as possíveis falhas e confiabilidade do sistema.

Os eventos que podem ser simulados no DNP3 são:

- Transmissão e retransmissão de uma mensagem não solicitada;
- Transmissão e retransmissão de mensagem não solicitada com função de leitura;
- Transmissão e retransmissão de mensagem não solicitada com função diferente da leitura;
- Transmissão e retransmissão de mensagem de *reset;*
- Função de Leitura *(Read)*;
- Função de escrita (*Write*);
- Funções de seleção e operação.

Através dos resultados obtidos pode-se avaliar o desempenho do DNP3 em uma rede TCP/IP em aplicações *Smart Grid*.

IV. RESULTADOS

Infraestruturas críticas, hoje em dia desempenham um papel fundamental numa sociedade moderna. O sistema de energia elétrica é uma infraestrutura critica altamente interligada e dinâmica. Constituída de várias concessionarias, são divididas em sistemas de geração, transmissão, distribuição e usuários [10].

Com a automação da rede elétrica, as *utilities* possuem diversas aplicações voltadas à monitoração, controle e operação na rede elétrica. E todas essas operações exigem meio de comunicação eficiente, confiável e alta disponibilidade, seja em regiões urbanas ou áreas rurais. A rede sem fio ad hoc viabiliza essa comunicação com um custo mais reduzido e mais rápido para ser implantada.

Com o objetivo de analisar o desempenho do protocolo de comunicação DNP3 em redes WLAN foi desenvolvido um

patch específico do protocolo DNP3 sob o IEEE 802.11b no NS-2. Os resultados foram obtidos no simulador NS-2 na versão 2.35 compilado no sistema Operacional *Linux Fedora Core* 15 64.

O cenário da simulação considerado nesse trabalho foi o comportamento do protocolo DNP3 sob uma topologia multiponto da rede IEEE 802.11b *Ad hoc.* O envio de mensagens não solicitadas, enviadas pela estação remota para otimizar o uso do canal de comunicação, foi a única função básica do DNP3 utilizada.

A topologia da rede é composta por duas estações escravas, uma estação central e um ponto de acesso. A comunicação entre os nós é ponto-a-ponto se estiver dentro do alcance. Caso contrário a comunicação é realizada por outros nós intermediários pela retransmissão dos pacotes até o nó destino.

A tabela 1 apresenta os principais parâmetros do modelo da rede considerada na simulação de transmissão de mensagens não solicitadas com tamanho de pacotes de 292 bytes.

TABELA I. PARÂMETROS DA REDE MODELADA

Parâmetro	Valor
Canal	WirelessChannel
Propagação	TwoRayGround
Interface de rede	Wireless Phy
Camada MAC	802_11
Tipo de fila	*DropTail*
Camada de enlace	LL
Modelo da antena	OmniAntenna
Número Máximo de pacote na fila	50
Número de nós sem fio	3
Protocolo de roteamento	DSDV
Área de cobertura (XxY)	400m x 200m
Número de estaçoes basse	1
Taxa de transmissão	11Mb
Tamanho dos pacotes	292 bytes
Tipo de aplicação	DNP3
Evento	Mensagens não solicitados

A Fig. 2 mostra um trecho da simulação pelo NAM (*Network Animator*). Nessa ilustração é possível visualizar que todos os nós estão dentro de alcance e o trafego gerado na rede é encaminhado diretamente ao nó destino.

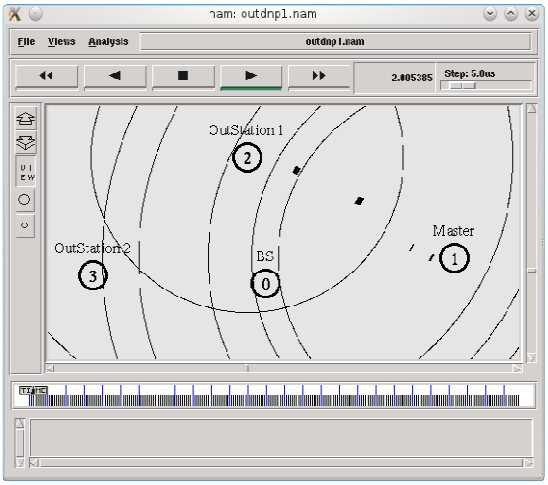

Fig. 2 Estação *OutStation1* enviando pacotes paras a estação *Master*.

O envio do pacote do DNP3 é constante com intevalos de 2.0 s em cada estaçao escrava, iniciado-se no instante 2.0 s e terminado no instante 205.0 s, a estação mestre recebe as informaçoes num intervalo de 1.0 s. A configuração é um cenário simples que conta com uma estação mestre definida no "nó1" e duas estações escravas definidas no "nó2" e no "nó3" com um ponto de acesso no "nó0". Nesta simulação o protocolo DNP3 está sendo encapsulado em uma rede TCP/IP e a comunicação de dados é no nível da camada de aplicação.

A Fig. 3 ilustra o funcionamento dos eventos. Ao receber uma mensagem de dados proveniente de uma estação *outstation*, a estação *master* deve efetuar a confirmação de recebimento ao emissor da mensagem. Se a confirmação não for recebida pelo dispositivo Remoto, o mesmo deve retransmitir a mensagem anterior. Do mesmo modo, caso haja o recebimento, a estação escrava limpa seu *buffer* de mensagens.

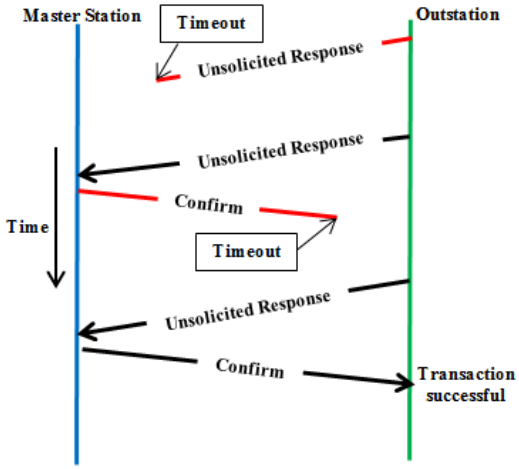

Fig. 3 Esquema de Transmissão de Mensagens não Solicitadas.

Em ambientes com muita interferência com ruídos no canal de transmissão, mesmo com as conexões ponto-a-ponto podem haver quadros errôneos entre as estações. Este efeito de erros de transmissão é agravado por cenários onde existem outros serviços operantes no enlace, como HTTP, FTP, CBR, entre outros.

A probabilidade de erro no tráfego de mensagens no enlace foi modelada a partir da variável "*proberror_*". Esta variável é configurada dentro do intervalo (0,9), sendo que 0 representa um enlace imune a erros de transmissão e 9 para 90% de probabilidade de ocorrer erros em uma transmissão. O valor *default* da variável é 1, ou seja, 10% de erros de transmissão. O intervalo de tempo para a retransmissão de uma mensagem é configurado através da variável "*retrytimer_*", sendo que o valor padrão é de 1 s. A tabela 2 apresenta os requisitos do tempo de atraso para entrega de uma mensagem de acordo a cada tipo de aplicação no sistema *smart grid.*

TABELA II. REQUISITOS DO DELAY PARA ENTREGA DE MENSAGEM

Tipo	Delay entrega	Aplicações
Proteção	3 ~ 16ms	Disparo, desligamento, religamento.
Monitoramento em tempo real	16 ~ 100ms	Relatórios dos Estados
Baixa Velocidade	≥ 100ms	Transferência de arquivos

Fonte: Adaptado de [11].

A Fig.4 mostra o *Throughput* ou vazão dos pacotes transmitidos do *OutStation 1* para o *Master* (curva azul) e do *OutStation 2* ao *Master* (curva vermelho). Com os parâmetros da topologia, tráfego DNP3 gerado a cada 2 s e tamanho de 292 *bytes* mais 40 *bytes* de cabeçalho do protocolo TCP/IP totalizando 332 *bytes* por pacotes transmitidos, a vazão média esperada esta em torno de 166 *bytes*/s (0,166 *Kbytes*/s). O resultado mostra uma vazão um pouco menor do que o teórico, aceitável em função de outros processos levados em consideração no simulador.

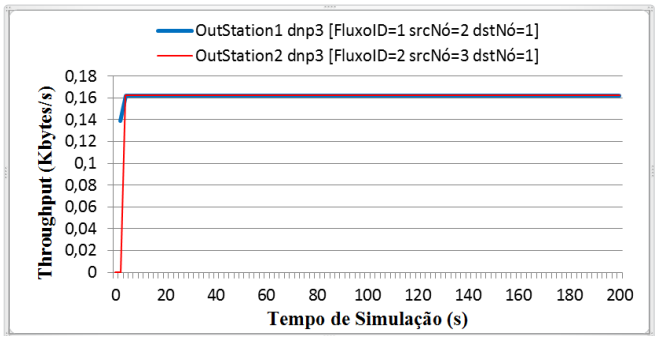

Fig. 4 *Throughput*

A Fig. 5 ilustra o atraso na entrega do tráfego DNP3 das *OutStation´s* para o *Master.* A distância entre o *OutStation 1* e o *Master* é por volta de 283 m e entre o *OutStation 2* e o *Master* está em torno de 400 m. Como o *OutStation 1* está mais próximo do *Master* do que o *OutStation 2* a tendência é que os pacotes enviados pelo *OutStation 1* tenham um atraso menor do que o *OutStation 2*. O histograma da Fig. 5 mostra claramente esse perfil, uma quantidade maior de pacotes com atrasos menores do que 1,5 ms pelo *OutStation 1* em relação ao *OutStation 2* e a inversão dessa característica no caso do atraso maior do que 1,5 ms.

A Fig.6 mostra o histograma do *Jitter* e a análise é análogo ao do atraso.

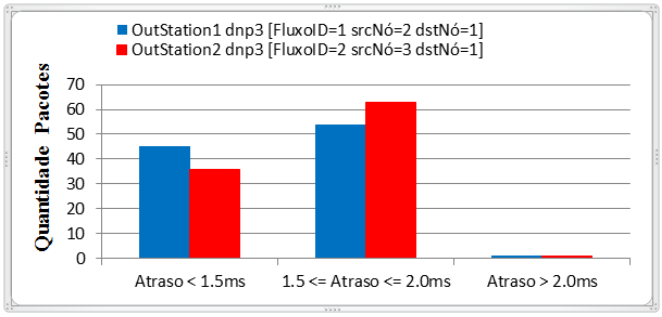

Fig. 5 Atraso

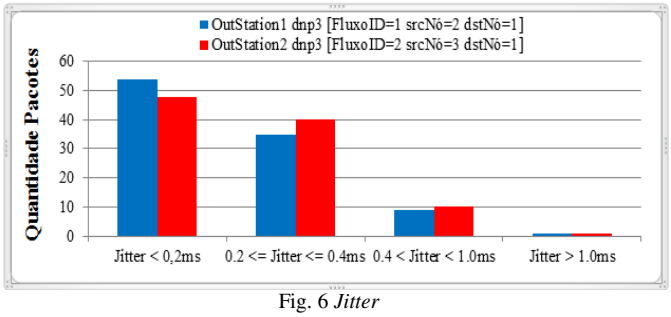

Fig. 6 *Jitter*

V. CONCLUSÕES

As ferramentas e funções que se encontram disponíveis no simulador NS-2, permitiram a realização da implementação do protocolo DNP3 operando sobre TCP/IP. A vantagem do NS-2 é o fato de ser um *software* livre *open source* que permite realizar estudos de redes similares com algumas restrições e aproximações de funcionamento de redes reais.

A simulação do comportamento de redes de dispositivos é importante para que sejam reduzidos os erros na implantação de quaisquer equipamentos para a automação no sistema de infraestruturas críticas.

Este trabalho teve o objetivo de desenvolver um *patch* para o NS-2 com a finalidade de simular o protocolo DNP3 sobre redes WLAN. Nas simulações observou-se que a integração DNP3 encapsulado sobre TCP/IP apresentou a funcionalidade esperada quando utilizado em redes sem fio 802.11 sem mobilidade e sem saltos, dos pacotes transmitido sem perdas e descarte de dados.

Nos trabalhos futuros pretendem-se realizar cenários em redes com tráfegos heterogêneos, com mobilidade, integrando redes cabeada e sem fio.

REFERÊNCIAS

[1] R. Brown, “Impact of smart grid on distribution system design,” in Proc. IEEE Power and Energy Society General Meeting, 2008, pp. 1-4.

[2] R.H. Lasseter, et al., “CERTS Microgrid laboratory test bed,” IEEE Trans. Power Delivery, vol. 26, no. 1, pp. 325-332, Jan. 2011.

[3] Arup Sinha, S. Neogi, R. N. Lahiri, S. Chowdhury, S. P. Chowdhurry and N. Chakraborty, " Smart Grid Initiative for Power Distribution Utility in India," 2011 *IEEE.*

[4] Distributed Network Protocol, http://www.dnp.org/

[5] M.Greis, Tutorial for the Network Simulator NS, http://www.isi.edu/nsnam/ns/tutorial/index.html.

[6] S. Bagaria, S. B. Prabhakar, Z. Saquib "Flexi-DNP3: Flexible Distributed Network Protocol Version 3 (DNP3) for SCADA security," 2011 *IEEE.*

[7] IEEE Distributed Network Protocol DNP3. IEEE Power and Energy Society. 2012, ISBN 978-0-7381-7292-7, STD97267

[8] M.Greis, Tutorial for the Network Simulator NS, http://www.isi.edu/nsnam/ns/tutorial/index.html.

[9] O. E. R. Jaimes, "Estudios de desempeño de escenarios SCADA que utilizan el Protocolo DNP3," Magíster. dissertation, Ing. Elet. Comp. Eng., Univ. de los Andes, College Park, 2012.

[10] Bigham, J., Gamez, D., and Ning Lu, “Safeguarding SCADA Systems with Anomaly Detection”, V.Gorodetsky et al.(Eds.):MMM-ACNS 2003, LNCS 2776, pp. 171-182, Springer-Verlag Berlin Heidelberg, 2003.

[11] Xiang Lu; Zhuo Lu; Wenye Wang; JianFeng Ma, "On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP," *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* , vol., no., pp.1,6, 5-9 Dec. 2011.