

February 10, 2010

## Abstract

Modelos	Ataque	Contramedidas
Dolev-Yao	Ataque ao meio de comunicação	Criptografia simétrica, <i>One Way Hashing</i>
Organização e Descoberta da Rede	Falsificação de informação de Routing	Autenticação, <i>One Way Hashing</i>
	Ataques de <i>Rushing</i>	Seleção aleatória de RREQ, autenticação, verificação bidirecional
Estabelecimento de Rotas	HELLO flooding	Autenticação com verificação bidirecional ( <i>acknowledge</i> )
	Ataques <i>Sinkhole</i>	Autenticação, Distribuição de chaves <i>pairwise</i>
	Ataques <i>Wormhole</i>	<i>Packet leaches</i> , MAC
	Ataques <i>Sybil</i>	Distribuição de chaves <i>pairwise</i> , selecção aleatória de canais de rádio
Manutenção de Rotas	Ataques de <i>Backhole</i>	Definição de temporizadores e mecanismos de confirmação (ACK) autenticados
Modelo de Intrusão	Intrusão	Encaminhamento multi-rota; <i>One Way Hashing</i>
	Replicação	Certificação central; Autenticação; Nós vizinhos como testemunhas

Table 1: Tabela de Ataques *vs* Contramedidas

Protocolos	Ataques ao Encaminhamento							Intrusão	Comunicação
	Info. Falsa	<i>Rushing</i>	HELLO flooding	<i>Sinkhole</i>	<i>Wormhole</i>	<i>Sybil</i>	<i>Blackhole</i>	Intrusão/Replicação	Dolev-Yao
SIGF								/	
INSENS								/	
Clean-Slate								/	

Table 2: Tabela de Protocolos de Encaminhamento *vs* Ataques

		Ambientes de Simulação				
Critérios		Prowler/JProwler	J-Sim	Freemote	ShoX	Nova Plataforma
Software	Portabilidade da linguagem	Java	Java	Java	Java	Java
	Código Livre Aberto	Sim	Sim	Sim	Sim	Sim
	Modularidade e extensibilidade	Sim	Sim (JTcl)	Sim	Sim	Sim
	Documentação	Apenas comentários no código	Papers e On-line	Pouca	Pouca	
Propriedades das RSSF	Escalabilidade	Aprox. 5000 nós	Documentado na ordem dos milhares	Documentado na ordem dos milhares	Foram testados 100 nós sem sucesso	Na ordem de milhares
	Colisões/Comunicação	Sim, modelo B-MAC	Sim, mas 802.11	Sim, mas muito simples	Sim, mas 802.11	Sim
	Gestão de Energia	Não	Não	Não	Sim	Sim
	Emulação	Não	Não	Sim, para plataformas Java <i>Based</i>	Não	Não
	Mobilidade	Sim, mas rudimentar	Sim	Sim	Sim	Não
	Visualização	Sim, mas só de visualização da topologia	Existem ferramentas auxiliares	Sim	Sim, mas não em tempo real. Apenas depois de executar a simulação	Sim
	Topologia	Não existe de raiz, pode ser modelado	Não existe de raiz, pode ser modelado	Não existe de raiz, pode ser modelado	Existem alguns de raiz, podendo ser estendido	Existirão de raiz alguns modelos permitindo a adição de mais

Table 3: Tabela de Critérios de Avaliação *vs* Ambientes de Simulação