Uma Análise de Protocolos para o Estabelecimento de Chave de Grupo em Redes Ad Hoc *

Eric Ricardo Anton , Otto Carlos Muniz Bandeira Duarte

[1] Grupo de Teleinformática e Automação
COPPE/EE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro
`http://www.gta.ufrj.br/`

`eric@gta.ufrj.br, otto@gta.ufrj.br`

Abstract. *This work focuses on the establishment of a secret cryptographic key among a group of devices that are part of an ad hoc network. The main group key establishment protocols are analyzed. Two protocols that present best performance are simulated in a wireless ad hoc environment in order to evaluate their behavior under the effects of lack of connectivity, on-demand routing and mobility. Simulations are executed for two kinds of scenarios: individual and group mobility. Results indicate that device connectivity is this environment's greatest problem, requiring high densities of mobile devices to assure group key establishment. Scenarios with group mobility demand fewer messages, although they demand higher device densities in order to guarantee device connectivity.*

Resumo. *Este trabalho foca a questão do estabelecimento de uma chave criptográfica secreta entre um grupo de dispositivos que fazem parte de uma rede ad hoc. Os principais protocolos para o estabelecimento de chave de grupo são comparados. Os dois que apresentam melhor desempenho são simulados em ambiente ad hoc para avaliar seus comportamentos sob os efeitos de falta de conectividade, roteamento sob demanda e mobilidade. As simulações são efetuadas para dois tipos de cenários: movimentação individual e em grupo. Os resultados indicam que a conectividade entre os dispositivos é o maior problema deste ambiente onde é requerida uma alta densidade dos dispositivos móveis para se obter sucesso no estabelecimento da chave de grupo. Cenários com movimentação em grupo exigem bem menos mensagens apesar de exigirem maiores densidades de dispositivos para garantir a conectividade entre eles.*

1. Introdução

Os aspectos de segurança em redes sem fio ad hoc são de grande importância devido às vulnerabilidades intrínsecas ao processo de comunicação sem fio, como escuta passiva e facilidade de ataques ativos. Além disso, os mecanismos desenvolvidos para redes convencionais não são convenientes para utilização no ambiente sem fio, devido às hipóteses geralmente assumidas como disponibilidade de servidores de autenticação e repositórios

*Este trabalho foi realizado com recursos do CAPES, CNPq, FAPERJ, COFECUB e FUJB.

de chaves públicas. Em ambientes ad hoc estas hipóteses geralmente não são verdadeiras, cabendo aos próprios dispositivos que compõem a rede o estabelecimento de uma relação de segurança entre si.

A maioria dos estudos sobre segurança em redes ad hoc concentra-se na área de roteamento seguro [Hu et al., 2002, Papadimitratos and Haas, 2002]. Estes estudos assumem, no entanto, o compartilhamento de uma chave criptográfica entre os dispositivos móveis, ou seja, que o estabelecimento de uma chave de grupo já ocorreu. O estabelecimento de uma chave de grupo em redes ad hoc é abordado por Asokan e Ginzboorg [Asokan and Ginzboorg, 2000], que propõem uma versão do protocolo para estabelecimento de chave de grupo Hipercubo [Becker and Wille, 1998] tolerante a falhas e mecanismos de autenticação entre os membros de um grupo. Haas e Zhou [Haas and Zhou, 1999] abordam a questão de serviços de certificação utilizando criptografia assimétrica e apresentam um esquema de distribuição da responsabilidade de uma autoridade certificadora de chave pública entre um conjunto de dispositivos que fazem parte de uma rede ad hoc. Khalili *et al.* [Khalili et al., 2003] baseiam-se nesta proposta, substituindo a autoridade certificadora por um serviço distribuído de geração de chaves privadas. A questão da autenticação é abordada por Stajano e Anderson [Stajano and Anderson, 1999], que apresentam um modelo de política de segurança baseado na autenticação de dispositivos ad hoc por meio do contato físico destes dispositivos com outros. Balfanz *et al.* [Balfanz et al., 2002] abordam a questão da segurança e da autenticação em redes ad hoc propondo a utilização de um canal privado de alcance restrito para autenticação, como o contato físico entre os dispositivos ou a utilização de raios infravermelhos ou de som.

O estabelecimento de chave de grupo foi estudado por [Ingemarsson et al., 1982, Becker and Wille, 1998, Burmester and Desmedt, 1994, Ateniese et al., 2000, Steiner et al., 2000]. Os autores apresentaram estes protocolos em [Anton and Duarte, 2002a], e em [Anton and Duarte, 2002b] apresentam algumas comparações de desempenho destes protocolos, resumidas neste artigo na Seção 2. Os resultados analíticos obtidos nestes trabalhos não levam em consideração diversas características importantes presentes em uma rede ad hoc.

Este artigo avalia, por simulação, a execução dos protocolos de estabelecimento de chave de grupo IKA.1 e IKA.2 em ambiente ad hoc com o objetivo de avaliar o comportamento destes protocolos sob os efeitos de falta de conectividade, roteamento sob demanda e mobilidade. São utilizados dois modelos de movimentação dos dispositivos. O primeiro se baseia no modelo geralmente utilizado onde os dispositivos se movem de forma totalmente aleatória. No segundo modelo, os dispositivos são aglomerados em subgrupos e estes subgrupos se movem de forma aleatória.

O restante do artigo está organizado da seguinte forma. A Seção 2 compara os principais protocolos de estabelecimento de chave de grupo. A Seção 3 avalia os dois protocolos com melhor desempenho a partir dos resultados obtidos por simulação. O artigo é finalizado na Seção 4 com a apresentação das conclusões.

2. Estabelecimento de chave de grupo em redes ad hoc

O protocolo proposto por Ingemarsson *et al.* [Ingemarsson et al., 1982], referido neste trabalho como ING, se baseia na disposição dos dispositivos na forma de um anel lógico e necessita de um grande número de mensagens. O protocolo Hipercubo, proposto por Becker e Wille [Becker and Wille, 1998] procura contornar o elevado número de mensagens do protocolo ING por meio da disposição lógica dos dispositivos na forma de um hipercubo. O protocolo proposto por Burmester e Desmedt [Burmester and Desmedt, 1994], referido neste trabalho como BD, se baseia em cada dispositivo realizar duas operações de difusão de informações a todos os demais. Os protocolos IKA.1 e IKA.2 apresentados por Steiner *et al.* [Ateniese et al., 2000, Steiner et al., 2000] baseiam-se na coleta de contribuições pelos membros do grupo, e na posterior divulgação destas contribuições a todos os membros do grupo. Estes protocolos são apresentados em [Anton and Duarte, 2002a, Anton and Duarte, 2002b].

A Tabela 1 apresenta uma comparação entre os protocolos para estabelecimento de chave de grupo apresentados. São expostos, para cada protocolo, o número de mensagens enviadas ponto-a-ponto, a quantidade total de dados transmitidos, em função do tamanho da chave, o número total de operações de exponenciação efetuadas e se há necessidade de sincronismo entre os participantes no momento de envio de uma mensagem a outro participante.

	Mensagens	Dados transmitidos	Operações de exponenciação	Sincronismo
ING	$n^2 - n$	$n^2 - n$	n^2	Sim
BD	$2n^2 - 2n$	$2n^2 - 2n$	$n^2 - n$	Sim
Hipercubo	$n \cdot \log_2 n$	$n \cdot \log_2 n$	$2n \cdot \log_2 n$	Sim
IKA.1	$2n - 2$	$0.5n^2 + 1.5n - 3$	$0.5n^2 + 1.5n - 1$	Não
IKA.2	$4n - 5$	$4n - 5$	$5n - 6$	Não

Tabela 1: Comparação entre os protocolos apresentados para estabelecimento de chave de grupo.

Os protocolos ING e BD são os mais custosos com relação às três métricas utilizadas, o que os torna pouco atraentes para utilização quando comparados aos demais protocolos.

O protocolo Hipercubo necessita de sincronismo entre os participantes, o que implica em uma sobrecarga a nível de número de mensagens que varia em função do complexidade do mecanismo sincronizador utilizado.

Os protocolos, IKA.1 e IKA.2 apresentam algumas vantagens, como o estabelecimento da seqüência em que ocorrem as contribuições durante a execução do protocolo e a possibilidade de adição e exclusão de membros do grupo sem a necessidade de execução de todo o protocolo de estabelecimento da chave.

A comparação entre os protocolos Hipercubo e IKA.2, com relação às três métricas apresentadas, permite perceber que o protocolo IKA.2 apresenta sempre o menor custo de execução. A inclusão de um mecanismo sincronizador, conforme mencionado, prejudicaria ainda mais a performance do protocolo Hipercubo.

Com base nestas informações, o protocolo IKA.2 apresenta-se como o mais vantajoso dentre os protocolos apresentados. Embora o protocolo IKA.1 não seja tão eficiente com relação à quantidade de dados transmitidos e ao número de operações de exponenciação realizadas, sua utilização como uma alternativa ao IKA.2 pode ser interessante, uma vez que ele é mais eficiente com relação ao número de mensagens transmitidas e ambos pertencem à mesma família de protocolos, compartilhando a forma da chave criptográfica utilizada. Assim, eventuais alterações da chave de grupo podem ocorrer ora por um protocolo ora pelo outro.

3. Análise de desempenho

As análises dos protocolos realizadas na Seção 2 não consideram importantes fatores que são encontrados em comunicações reais por redes de computadores. Um destes fatores é o encaminhamento das mensagens através de outros dispositivos da rede, realizando múltiplos saltos. Ou seja, se a transmissão de uma mensagem de um dispositivo A para um dispositivo B requerer s saltos, a quantidade total de dados transmitidos é s vezes maior que a inicialmente prevista. Um outro fator muito importante em redes ad hoc é a conectividade dos dispositivos, pois em redes ad hoc móveis alguns dispositivos podem estar momentaneamente indisponíveis, impedindo o estabelecimento da chave de grupo. Como a conectividade depende do número de dispositivos que compõem a rede, do tamanho da área sobre a qual estes dispositivos estão distribuídos e de sua mobilidade, uma das medidas de desempenho a ser obtida é a taxa de sucesso no estabelecimento da chave de grupo em função destes parâmetros. Além da conectividade, outros fatores que influenciam o desempenho do estabelecimento de chave de grupo em redes ad hoc são os protocolos de acesso ao meio e de roteamento. Visando considerar estes fatores, a análise de desempenho dos protocolos de estabelecimento de chave IKA.1 e IKA.2 foi realizada por simulação.

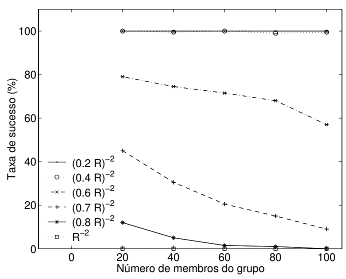
Foi utilizado o simulador de redes de computadores ns-2. Os dispositivos sem fio simulados utilizam o padrão IEEE 802.11 e possuem um raio de alcance de 250 metros. Foram calculadas margens de erro com intervalos de confiança de 95% relativos às médias das medidas.

Os cenários de movimentação dos dispositivos que compõem a rede ad hoc se baseiam em dois modelos de mobilidade: o modelo geralmente utilizado, onde todos os dispositivos móveis são posicionados aleatoriamente segundo uma distribuição uniforme em uma área especificada e o modelo onde os dispositivos são aglomerados em subgrupos.

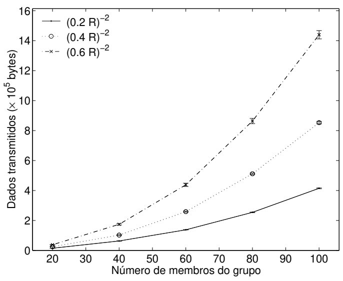
Conforme mencionado, redes ad hoc podem apresentar problemas de conectividade entre os dispositivos da rede. Um dispositivo é alcançável se está dentro do raio de ação do emissor, ou se existe um ou mais dispositivos que podem encaminhar a mensagem do emissor até o destino por múltiplos saltos. Assim, a conectividade total se consegue em áreas totalmente cobertas pelo raio de ação dos dispositivos. Quando a área onde se encontram os dispositivos é maior que o raio de ação do dispositivo móvel pode haver necessidade de se usar outros dispositivos intermediários para se alcançar o destino e, nestes casos, a probabilidade de se alcançar um dispositivo aumenta com a densidade de dispositivos.

Visando avaliar a influência do espaçamento entre os dispositivos, foram realizadas simulações com diferentes densidades de dispositivos por área. Para se obter diferentes densidades, variou-se a área quadrada de simulação em função do número de dispositivos. As densidades tipicamente utilizadas foram $(0.2\ R)^{-2}$, $(0.4\ R)^{-2}$, $(0.6\ R)^{-2}$, $(0.8\ R)^{-2}$ e R^{-2}, onde R = 250 m é o raio de alcance dos dispositivos.

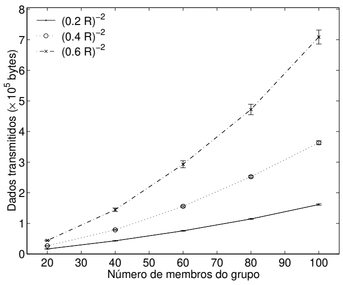
Os protocolos IKA.1 e IKA.2 foram simulados inicialmente para cenários sem movimentação. A Figura 1(a) apresenta as taxas de sucesso obtidas com a execução dos protocolos em função do número de membros que compõem o grupo, para diferentes densidades de dispositivos. A taxa de sucesso é calculada dividindo-se o número simulações que obtiveram sucesso no estabelecimento da chave de grupo pelo número total de simulações realizadas. Para altas densidades de dispositivos ($(0.2\ R)^{-2}$ e $(0.4\ R)^{-2}$) a conectividade da rede é alta de forma que o estabelecimento da chave de grupo se dá sempre com sucesso, havendo uma diminuição das taxas de sucesso à medida que a densidade de dispositivos por área diminui. Isto se deve à diminuição da conectividade da rede em função do maior espaçamento entre os dispositivos. É possível perceber que, para uma dada densidade de dispositivos, à medida que o número de dispositivos aumenta, a taxa de sucesso no estabelecimento da chave de grupo diminui. Isto ocorre pois à medida que a área aumenta, devido ao aumento do número de dispositivos, aumenta a probabilidade de, em uma área maior, haver pelo menos um dispositivo não alcançável aos demais, impedindo a finalização do protocolo.



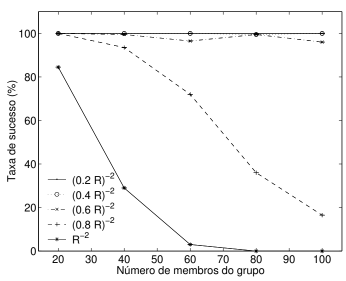
(a) Taxa de sucesso - 0 m/s - IKA.1 e IKA.2.



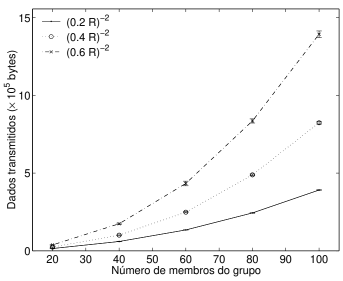
(b) Dados transmitidos - 0 m/s - IKA.1.



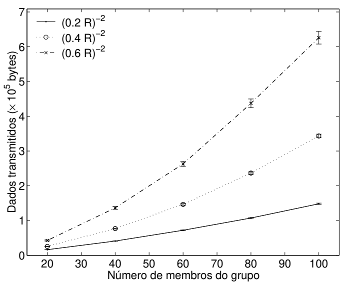
(c) Dados transmitidos - 0 m/s - IKA.2.



(d) Taxa de sucesso - 1 m/s - IKA.1.



(e) Dados transmitidos - 1 m/s - IKA.1.



(f) Dados transmitidos - 1 m/s - IKA.2.

Figura 1: Desempenho para dispositivos aleatoriamente posicionados.

As Figuras 1(b) e 1(c) expressam as quantidades de dados transmitidos durante a execução dos protocolos de estabelecimento de chave em função dos número de membros do grupo, para diferentes densidades de dispositivos. São contabilizados apenas os dados referentes às densidades de dispositivos que apresentaram taxas de sucesso acima de 60% e mensagens relativas ao protocolo de estabelecimento de chave de grupo, não sendo contabilizadas, por exemplo, mensagens de roteamento. Para uma dada densidade, à medida que o número de membros do grupo cresce, aumenta a quantidade de dados transmitidos, conforme esperado. Nota-se no entanto que para o protocolo IKA.2 este crescimento é mais acentuado que o crescimento linear previsto (Tabela 1). Isto se deve à necessidade de transmissão de dados por múltiplos saltos, de modo que a cada salto é gerada uma nova mensagem, que é encaminhada ao destino, elevando a quantidade de dados transmitidos na rede.

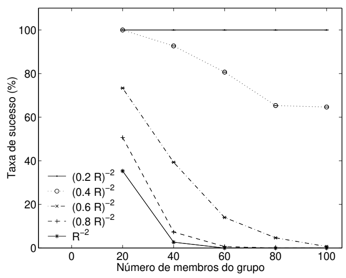
Percebe-se ainda que à medida que a densidade de dispositivos diminui há um aumento da quantidade de dados transmitidos devido ao maior espaçamento entre os dispositivos, o que tende a aumentar o número de saltos necessários ao encaminhamento das mensagens transmitidas. A comparação entre os dois protocolos permite perceber que o protocolo IKA.2 necessitou transmitir cerca da metade dos dados que o protocolo IKA.1, sendo mais vantajoso segundo esta métrica para este tipo de cenário.

Com o objetivo de avaliar a influência da mobilidade, os protocolos IKA.1 e IKA.2 foram simulados em cenários com constante movimentação dos dispositivos a velocidades em torno de 1 m/s. Percebe-se que as taxas de sucesso alcançadas com ambos os protocolos (Figura 1(d)) foram cerca de 100%, para as densidades de $(0.2\ R)^{-2}$, $(0.4\ R)^{-2}$ e $(0.6\ R)^{-2}$. Houve portanto uma melhora do desempenho com relação às taxas de sucesso obtidas com os dispositivos parados. A movimentação dos dispositivos favorece os casos de sucesso no estabelecimento da chave de grupo, pois a freqüente modificação da topologia, por meio da quebra e criação de enlaces, aumenta a probabilidade de que um dado dispositivo seja eventualmente capaz de se comunicar com os demais. Com relação às quantidades de dados transmitidos (Figuras 1(e) e 1(f)), os resultados obtidos foram semelhantes aos obtidos nos cenários com dispositivos parados.

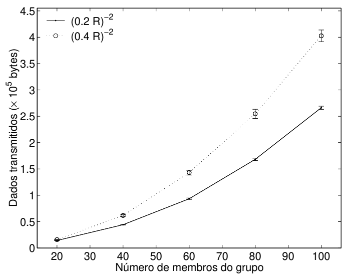
Os protocolos IKA.1 e IKA.2 foram também simulados em cenários com aglomeração em subgrupos, estando os dispositivos parados. As taxas de sucesso obtidas, apresentadas pela Figura 2(a), são mais baixas que aquelas obtidas nos cenários sem subgrupos. Este pior desempenho se deve à concentração dos dispositivos, o que gera um maior espaçamento entre os subgrupos, prejudicando a conectividade entre eles.

A comparação das quantidades de dados transmitidos em cenários com aglomeração em subgrupos (Figuras 2(b) e 2(c)) com os valores obtidos em cenários com dispositivos posicionados independentemente (Figuras 1(b) e 1(c)) permite perceber uma redução das quantidades de dados transmitidos, para ambos os protocolos IKA.1 e IKA.2. Esta redução se deve à proximidade entre os membros de um mesmo subgrupo, pois todos os dispositivos que participam de um mesmo subgrupo são adjacentes com relação à seqüência em que ocorrem as contribuições para a chave de grupo. Assim, as mensagens transmitidas durante a execução dos protocolos ficam inicialmente restritas a cada subgrupo, sem problemas de conectividade e sendo enviadas sempre por um salto, antes de serem enviadas ao próximo subgrupo.

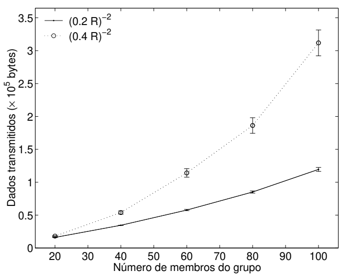
Visando analisar o efeito da mobilidade sobre os comportamentos dos protocolos IKA.1 e IKA.2, estes protocolos foram simulados sobre cenários com aglomerações dos



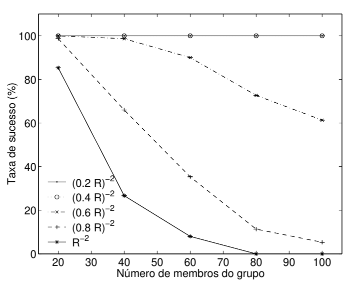
(a) Taxa de sucesso - 0 m/s - IKA.1 e IKA.2.



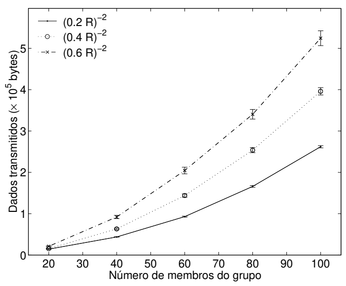
(b) Dados transmitidos - 0 m/s - IKA.1.



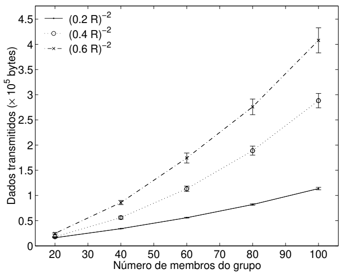
(c) Dados transmitidos - 0 m/s - IKA.2.



(d) Taxa de sucesso - 1 m/s - IKA.1.



(e) Dados transmitidos - 1 m/s - IKA.1.



(f) Dados transmitidos - 1 m/s - IKA.2.

Figura 2: Desempenho para dispositivos aglomerados em subgrupos.

dispositivos em subgrupos de 10 dispositivos e constante movimentação a velocidades em torno de 1 m/s. Houve melhora das taxas de sucesso obtidas (Figura 2(d)) com relação ao comportamento sem mobilidade. Com relação à quantidade de dados transmitidos (Figuras 2(e) e 2(f)), os desempenhos foram equivalentes àqueles obtidos com dispositivos parados aglomerados em subgrupos, sendo este resultado consistente com o obtido comparando-se dispositivos aleatoriamente posicionados parados e em movimentação.

4. Conclusões

Este trabalho comparou os principais protocolos de estabelecimento de chave de grupo e analisou, com o uso de simulações, os dois protocolos que apresentam melhor desempenho. Foram realizadas avaliações por simulação baseadas no modelo de mobilidade de dispositivos aleatoriamente distribuídos pela área de simulação e de movimentação em grupos.

Os resultados demonstram que o grande problema do estabelecimento de chave de grupo em redes ad hoc é a falta de conectividade entre os membros deste grupo, o que ocorre com o maior espalhamento dos dispositivos pela área de simulação quando se diminui a densidade de dispositivos.

Foi observado que nos cenários com aglomeração dos dispositivos em subgrupos pode-se tirar proveito da proximidade entre os dispositivos de um mesmo subgrupo para se transmitir um menor número de mensagens. Em contra-partida, este cenário, quando comparado ao cenário de posicionamento aleatório, tem um maior problema de falta de conectividade devido à maior distância entre os dispositivos, para uma mesma densidade de dispositivos móveis.

Os resultados indicam um baixo custo de execução do protocolo IKA.2 nos cenários utilizados.

Referências

Anton, E. R. and Duarte, O. C. M. B. (2002a). Estabelecimento de chave de grupo em redes ad hoc. In *Workshop em Segurança de Sistemas Computacionais (WSeg 2002)*, pages 89–96, Búzios, RJ.

Anton, E. R. and Duarte, O. C. M. B. (2002b). Segurança em redes sem fio ad hoc: Gerenciamento de chave de grupo. In *XIV Congresso Brasileiro de Automática*, Natal, RN.

Asokan, N. and Ginzboorg, P. (2000). Key agreement in ad hoc networks. *Computer Communications*, 23(17):1627–1637.

Ateniese, G., Steiner, M., and Tsudik, G. (2000). New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications*, 18(4).

Balfanz, D., Smetters, D. K., Stewart, P., and Wong, H. C. (2002). Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium (NDSS '02)*.

Becker, K. and Wille, U. (1998). Communication complexity of group key distribution. In *5th ACM conference on Computer and Communication Security*.

Burmester, M. and Desmedt, Y. (1994). A secure and efficient conference key distribution system. In *Advances in Cryptology (EUROCRYPT '94)*, pages 275–286.

Haas, Z. J. and Zhou, L. (1999). Securing ad hoc networks. *IEEE Network Magazine*, 13(6):24–30.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks. In *The Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*.

Ingemarsson, I., Tang, D. T., and Wong, C. K. (1982). A conference key distribution system. *IEEE Transactions on Information Theory*, IT-28(5):714–720.

Khalili, A., Katz, J., and Arbaugh, W. A. (2003). Toward secure key distribution in truly ad-hoc networks. In *IEEE Workshop on Security and Assurance in Ad hoc Networks*.

Papadimitratos, P. and Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*.

Stajano, F. and Anderson, R. (1999). The resurrecting duckling: Security issues for ad-hoc wireless networks. In *3rd AT&T Software Symposium*.

Steiner, M., Tsudik, G., and Waidner, M. (2000). Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 11(8):769–780.