Protocolos de Autenticação de Dispositivos Móveis em Grupos para a Internet de Objetos (IoT)

Ana Paula Golembiouski Lopes[1], Lucas de Oliveira Hilgert[2], Luis Fernando Arias Roman[3], Paulo Roberto de Lira Gondim[4]

Departamento de Engenharia Elétrica – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – 70910-900 – Brasília – Brazil

{anagolembiouski, lucas.hilgert, lfroman}@aluno.unb.br, pgondim@unb.br

Abstract. *The full establishment of Internet of Things (IoT) consists in connecting billions of devices securely and efficiently. The authentication of these devices will generate a large increase of signaling traffic, overloading the wireless access networks. To avoid this, a good solution is to authenticate groups of devices. The currently proposed protocols by the 3rd Generation Partnership Project (3GPP) are not suitable to large groups of devices. Consequently, group authentication protocols emerged, aiming for efficiency and the security required to the process. This paper presents a comparison involving recent authentication protocols, considering a set of criteria and metrics, allowing the evaluation of their characteristics.*

Resumo. *O pleno estabelecimento da Internet de Objetos (ou das Coisas) – IoT (do inglês, Internet of Things), requer a conexão de bilhões de dispositivos de maneira segura e eficiente. A autenticação destes dispositivos gerará grande aumento no tráfego de sinalização, sobrecarregando as redes de acesso sem fio. Para evitar isso, uma solução é autenticar grupos de dispositivos. Os protocolos propostos pelo 3rd Generation Partnership Project (3GPP) não são adequados para grandes grupos de dispositivos. Consequentemente, surgiram protocolos de autenticação em grupos, buscando eficiência e a segurança necessária para o processo. Este artigo compara protocolos de autenticação recentes, considerando um conjunto de critérios e métricas, permitindo avaliar suas características.*

1. Introdução

A IoT (*Internet of Things*) representa uma forte tendência atual, e seu emprego pode ser vinculado a diversas áreas de aplicação, tais como redes inteligentes (*Smart Grid),* cidades inteligentes e *m-health (Mobile Health)*. Uma das maiores preocupações para o pleno estabelecimento da IoT consiste em conectar bilhões de dispositivos de maneira segura e eficiente, sendo a rede LTE (*Long Term Evolution*) uma candidata natural para a integração desses dispositivos (comumente à base de grupos) à Internet. O protocolo 3GPP EPS-AKA (*Evolved Packet System – Authentication and Key Agreement*) é o protocolo de autenticação e acordo de chaves padrão para ser utilizado na E-UTRAN (*Evolved Universal Terrestrial Access Network*), que autentica cada um dos dispositivos individualmente. No âmbito da IoT, e também para a rede LTE, isso gera problemas, como o aumento do tráfego de sinalização, dos custos computacionais e de comunicação, além de vulnerabilidades de segurança que poderiam comprometer a comunicação e o funcionamento integrado desses dispositivos.

Este artigo apresenta, na seção 2, a descrição e a comparação de alguns protocolos de autenticação em grupo. Na seção 3 é feita uma análise de segurança e, na seção 4, tem-se a conclusão, trabalhos em andamento e futuros.

2. Descrição e Comparação dos Protocolos

Vários protocolos para autenticação de dispositivos em grupos têm sido propostos na literatura. Foram selecionados cinco protocolos para análise comparativa (incluindo um, EPS-AKA, representante dos padrões 3GPP atuais), com base em requisitos de segurança, resistência a ataques, custos de comunicação e computacionais, uso ou não de protocolo Diffie Hellman sobre curvas elípticas(ECDH) e de emparelhamento bilinear, dentre outros. As arquiteturas das redes LTE e 5G podem ser encontradas em [Firmin 2016] e [Cao 2016], respectivamente, incluindo entidades como MME (*Mobillity Management Entity*) e HSS (*Home Subscriber Server*).

SE-AKA [Lai 2013] utiliza criptografia assimétrica ECDH. Faz uso de identidades temporárias de MTCD (*Mobile Terminal Communication Device*) e de grupo para preservar suas identidades permanentes. Possui uma fase de inicialização, em que são definidos parâmetros para a autenticação. É usada chave de grupo e uma tabela de gerenciamento. Ao invés de definir um líder, trata de forma diferenciada o primeiro MTCD a se autenticar. Utiliza LAI (*Location Area Identification)* para que o HSS verifique se a *Base Station* indicada pelo MME é a mesma associada ao MTCD. O uso de ECDH permite que MTCD e SN (*Server Network*) gerem uma mesma chave, não compartilhada no canal de transmissão.

CHOI [Choi 2014] utiliza criptografia simétrica. Na fase de inicialização faz agrupamento dos MTCDs, sendo o gerenciamento do grupo feito usando árvore binária, com cada nó da árvore associado a um valor secreto derivado de seus nós pais, por funções hash. Após eleição do líder do grupo são definidos parâmetros como a chave de grupo, números aleatórios e funções hash. Os dispositivos do grupo são autenticados simultaneamente com o líder. Estabelece uma chave de sessão, obtida com a função hash dos valores secretos da árvore binária que os nós envolvidos possuem em comum.

GBAAM [Cao 2015] adota criptografia assimétrica ECDH. Na fase de registro ocorre formação de grupos e a eleição de líderes. Os MTCDs quando se registram pela primeira vez, devem ser provados autênticos para o KGC (*Key Generation Center*), recebendo chaves privadas. Um KGC define e publica os parâmetros do sistema e mantém uma chave mestre em segredo. O líder realiza a agregação das assinaturas de todos os MTCDs em uma única assinatura, que é enviada ao MME, e a autenticidade e aferida por emparelhamento bilinear. Se falhar na verificação, o MME divide o grupo de assinaturas em subgrupos e realiza emparelhamento em cada um deles, até detectar o subgrupo que apresenta assinatura inválida e, em seguida, por divisões sucessivas, encontrar a assinatura inválida.

GLARM [Lai 2016] utiliza criptografia simétrica; na fase de inicialização, forma grupos e cada MTCD calcula uma identidade temporária. Há a eleição de um líder. O processo de autenticação se baseia em desafio-resposta. Assim como o SE-AKA, utiliza identificador de localização para verificação de eNB e tabela de gerenciamento de grupo. Durante esta fase são derivadas chaves de cifragem, de integridade e a chave temporária de grupo. Ao final de uma autenticação com sucesso, cada MTCD compartilha com o MME uma chave K_{ASME} (*Key Access Security Management Entity*), essencial para

derivações de chaves futuras. Renova a chave de grupo a cada vez que um MTCD entra ou sai do grupo. Há ainda uma proposta para autenticação em grupo em redes não-3GPP. A Tabela 1 resume as características mais relevantes de cada um dos protocolos.

O custo computacional de [Cao 2015] é o mais alto dentre as propostas por utilizar emparelhamento bilinear, que exige muita capacidade de processamento. Seu custo de comunicação e o de [Lai 2016] são os mais baixos em relação aos demais protocolos.

Tabela 1. Principais características dos protocolos.

	EPS-AKA	SE-AKA	CHOI	GBAAM	GLARM
Autenticação em Grupo	Não	Sim	Sim	Sim	Sim
Tipo de Criptografia	Simétrica	Assimétrica ECDH	Simétrica	Assimétrica ECDH	Simétrica
MTC *Server*	Não possui	Dentro da EPC	Fora da EPC	Ambos	Fora da EPC
Eleição de Líder	Não	Não	Sim	Sim	Sim
Gerenciamento de Grupo	Não possui	Tabela	Árvore Binária	Dinâmico	Tabela
Emparelhamento Bilinear	Não	Não	Não	Sim	Não
Verificação de Localização (uso de LAI)	Não	Sim	Não	Não	Sim
Custo de Comunicação	Muito Alto	Alto	Baixo	Baixo	Baixo
Custo Computacional	Muito Alto	Baixo	Baixo	Alto	Baixo

3. Análise de Segurança

Algumas características estão presentes em todos os protocolos considerados: realizam autenticação mútua e acordo de chaves; usam chaves de sessão; ataques de repetição são evitados usando marcadores temporais (*Timestamps)* e números aleatórios durante autenticação; ataques *Man-in-the-Middle* são evitados, pois os parâmetros publicados no canal de comunicação não são suficientes para que um atacante gere mensagens e chaves de sessão válidas; segurança no futuro (*Forward Secrecy*) e segurança no passado (*Backward Secrecy*) são preservadas em relação a chaves de grupo, na entrada e saída de membros; todos conseguem se contrapor a ataques de personificação.

Tabela 2. Análise de segurança dos protocolos.

	EPS-AKA	SE-AKA	CHOI	GBAAM	GLARM
Autenticação Mútua e Acordo de Chaves	Sim	Sim	Sim	Sim	Sim
Confidencialidade	Não	Sim	Sim	Sim	Sim
Integridade	Não	Sim	Sim	Sim	Sim
Privacidade	Não	Sim	Não	Não	Não
Segurança no Futuro / no Passado	Não	Sim	Sim	Sim	Sim
Resistência ao Ataque de Repetição	Não	Sim	Sim	Sim	Sim
Resistência ao Ataque DoS	Não	Sim	Não	Não	Sim
Resistência ao Ataque *Man-in-the-Middle*	Não	Sim	Sim	Sim	Sim
Resistência ao Ataque de Redirecionamento	Não	Sim	Não	Não	Sim
Resistência ao Ataque de Personificação	Não	Sim	Sim	Sim	Sim

Para tais ataques, GBAAM [Cao 2015] busca impedir o adversário de forjar assinaturas válidas; CHOI-2014 atribui chaves de sessão únicas para cada MTCD; [Lai 2013] e [Lai 2016] usam números aleatórios diferentes em cada autenticação.

A privacidade é garantida no protocolo SE-AKA por proteger a identidade permanente dos MTCDs através de infraestrutura de chaves públicas. Os protocolos SE-AKA e GLARM evitam o ataque de negação de serviço (DoS) pelo uso de marcadores temporais e de LAI, permitindo detectar mensagens forjadas. O uso de LAI também evita os ataques de redirecionamento. A Tabela 2 sintetiza uma análise de segurança dos protocolos.

4. Conclusão e Trabalhos Futuros

É enorme a importância da autenticação de grupos de dispositivos, especialmente para o sucesso das implementações da IoT em áreas como *smart grid* e *m-health*. Após a análise, constatou-se que, em relação ao EPS-AKA [3GPP 2009], os demais protocolos avaliados realmente apresentam custos computacionais e de comunicação bastante reduzidos, atendendo requisitos de segurança e resistindo a diversos ataques. Outros protocolos foram também avaliados (tais como [Chen 2012], [Fu 2016], [LI 2016] e [Cao 2014]), mas não inclusos neste artigo por falta de espaço.

Trabalhos em andamento incluem o projeto de protocolo de autenticação para dispositivos móveis em grupo, com ênfase na utilização de protocolo Diffie Hellman sobre curvas elípticas e de emparelhamento bilinear. Trabalhos futuros incluem a simulação a eventos discretos e a validação formal, bem como avaliação dos custos de comunicação e computação.

Referências

3GPP (2009) 3GPP TS 33.401 V8.2.1, 3GPP System Architecture Evolution (SAE). Security Architecture.

Cao, J., Ma, M. and Li, H., (2014) “ABAAM: Access Authentication of Mass Device Connections for MTC in LTE Networks”, Smart Computing Review, vol. 4, no. 4, DOI: 10.6029/smartcr.2014.04.003

Cao, J., Ma, M. and Li, H. (2015) “GBAAM: Group-based Access Authentication for MTC in LTE Networks”, Security and Communication Networks, 8(17), 3282-3299. DOI: 10.1001/sec.1252.

Chen, Y., Wang, J., Chi, K. and Tseng, C., (2012) “Group-Based Authentication and Key Agreement”, Wireless Personal Communications. 62:965-979. DOI: 10.1007/s11277-010-0104-7.

Choi, D., Choi, H. and Lee, S. (2014) “A group-based security protocol for machine-type communications in LTE-advanced”, Wireless Networks 21:405. DOI: 10.1007/s112276-014-0788-9.

Firmin, F. (2016) “The Evolved Packet Core”. Acesso em Setembro 2016. http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

Fu, A., Song, J., Li, S., Zhang, G. and Zhang. Y. (2016) “A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks”, Security and Communication Networks, 9:2002-2014 DOI: 10.1002/sec.1455.

Lai, C., Lu, R., Zheng, D., Li, H. and Shen, X. (2016) “GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications”, Computer Networks 99(2016) 66-81. DOI: 10.1016/j.comnet.2016.02.007.

Lai, C., Li, H., Lu, R. and Shen, X. (2013). “SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks.” Computer Networks 57 (2013) 3492-3510. DOI: 10.1016/j.comnet.2013.08.003.

Li, J., Wen, M., and Zhang, T., (2016) "Group-Based Authentication and Key Agreement With Dynamic Policy Updating for MTC in LTE-A Networks”, *IEEE Internet of Things Journal*, vol.3, no.3, 408-417. DOI:10.1109/JIOT.2015.2495321.

