ENERGY-EFFICIENT AND LOW-LATENCY KEY MANAGEMENT FOR SENSOR NETWORKS

D. W. Carman* and B. J. Matt
Network Associates Laboratories
Rockville, MD 20850

G. H. Cirincione
Army Research Laboratory
Adelphi, MD 20783

ABSTRACT[1]

Army sensor networks require low energy, low latency key management techniques that enable strong security with high key granularity and tolerance of node compromise. Approaches using public key certificate-based key management techniques are not communications efficient, expend considerable battery energy, and are very time-consuming. We show how techniques based on identity-based cryptography meet the security requirements of Army sensor networks while reducing energy and latency costs by up to an order of magnitude.

1. REQUIREMENTS AND CONSTRAINTS

An underlying energy-efficient and secure communications infrastructure is a key enabler for conducting sensor network missions. Very energy-efficient, scaleable, and strong security services including confidentiality, integrity, and group-level authentication of sensor data and routing control traffic are needed.

Military sensor networks will often be forward deployed in hostile territory that presents a significant risk of node capture and eavesdropping. Predeployment of a network-wide key can be easily compromised, thus more granular keys are required to reduce this compromise potential. Since the multi-hop routing protocols most commonly utilized in sensor networks send both unicast and broadcast messages, pairwise and group keys must be established and maintained on a hop-by-hop basis (e.g., link layer).[2] Required keying protocol security properties include: *key authentication*, assuring that only intended nodes can access a key; and *forward secrecy*, where compromise of a node's current keys does not compromise keys from past cryptoperiods. Additionally, group keying protocols must provide *key independence*, whereby a new member cannot access old group keys, and removed members cannot access current and future group keys. Removal can happen due to movement, node death, or notification of a compromise.

These networks must operate over constrained and noisy wireless channels with near-earth propagation effects and intermittent connectivity. Particularly challenging for our work are severe limitations on bandwidth (as low as 1 Kbps), computational, and energy resources. An added complication is that Army sensor networks must support greater ranges and exhibit low probability of intercept/detection and anti-jam properties that significantly increase the energy cost per communicated bit than commercial networks.

Our previous research[3] showed that many conventional key management approaches, and especially group keying approaches, are not suitable for sensor networks in this environment. For representative sensor node platforms, communication energy accounts for at least 95% of all group key management energy consumed.

2. IDENTITY-BASED CRYPTOGRAPHY

A method of reducing key management communications is identity-based public key cryptography [Shamir, 1984], where a node's public key can be derived from its identity. A trusted authority generates private keys for all sensor nodes based on their identity, such as a unique node ID. These private keys, as well as public parameters of the system, are securely loaded into nodes prior to battlefield deployment. Recently a series of group key transport protocols have been developed that provide requisite security properties using identity-based public key cryptography including ID-STAR-1 and ID-STAR-3.[4] In each, the leader generates key material that is distributed to other group members using pairwise transport and message authentication code (MAC) keys generated using identity-based cryptography rather than from certificates.

[1] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. The U. S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U. S. Government.

[2] Balenson, D., et al, "Communications Security Architecture for Army Sensor Networks", NAI Labs T.R. #00-016, September 30, 2000.

[3] Carman, D., et al,, "Constraints and Approaches for Distributed Sensor Network Security", NAI Labs T.R. #00-010, June 2000.

[4] Matt, B., "A Preliminary Study of Identity-based, Group Key Establishment Protocols for Resource Constrained Battlefield Networks", TR# 02-034, Network Associates Laboratories, Sept. 2002.

These protocols can employ the Maurer-Yacobi scheme [Maurer and Yacobi, 1996] where the public and private keys are Diffie-Hellman keys over a composite modulus. In this scheme, nodes compute the Diffie-Hellman public keys of other nodes by simple computations on their identities.

In basic ID-STAR.1, the leader randomly generates the group key material, encrypts and transmits the group key material to each node using unique pairwise transport keys, and authenticates the transmissions using pairwise-keyed MACs. We provide forward secrecy by assigning multiple related identities to an individual or device and using each identity for a limited period of time.[5, 6] Nodes delete their private keys at the end of the cryptoperiod, preventing compromise of past keys.

3. PERFORMANCE

We compared the performance of six protocols in establishing and maintaining a group key for a singly-hop-connected group. We studied Burmester-Desmedt conference keying [Burmester et al., 1994], IKA.2 [Steiner et al., 2000], ID-STAR.1, a certificate-based static Diffie-Hellman group key transport protocol we call DH-STAR.1, and corresponding ephemeral variants of these last two ".1" protocols that we call ID-STAR.3 and DH-STAR.3, respectively. Our comparison is performed using the communication and computational characteristics of an Army sensor network under development. We assume 1024-bit public key sizes and 256 bits of transported secret key material are needed to provide requisite security.

We examine energy consumption and latency for initial group key establishment. The energy consumption results shown in Fig. 1 represent the sum of communications and computational energy needed. To establish a single ten-node group key, the Burmester-Desmedt and IKA.2 schemes consume 162 and 139 Joules, respectively, whereas ID-STAR.1 consumes only 12 Joules.

The amount of time consumed by each protocol is shown in Fig. 2 and represents the time to communicate the key information and the time spent performing cryptographic computations. For just a single ten-node group, the Burmester-Desmedt and IKA.2 schemes take over thirty seconds to establish the group key. By using fewer communications, ID-STAR.1 establishes a ten-node-group key in less than three seconds.

Using identity-based cryptography to securely initialize protection of Army sensor networks significantly reduces energy and latency costs versus existing public key certificate-based approaches. Our ID-STAR.1-based solution offers order of magnitude reduction in energy and latency consumption over group key agreement schemes and provides better performance than certificate-based group key transport.

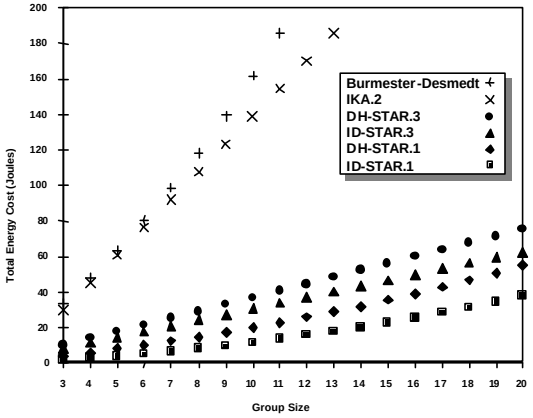

Fig. 1 – Group key formation protocol energy

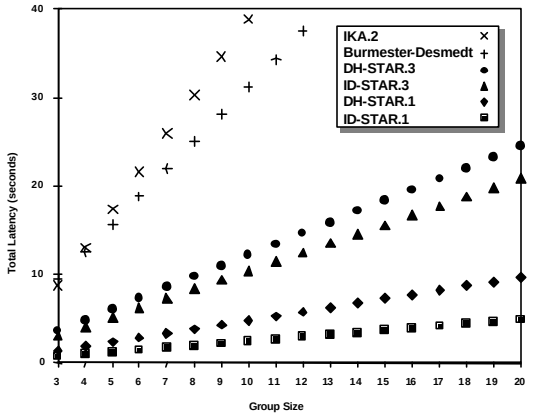

Fig. 2 – Group key formation protocol latency

REFERENCES

Burmester, M. and Desmedt, Y., "A Secure and Efficient Conference Key Distribution System", *In Proc. of Eurocrypt '94*, pp. 275-286, 1995.

Maurer, U. and Yacobi, Y., "A Non-Interactive Public-Key Distribution System", *Designs, Codes, and Cryptography*, Vol. 9, No. 3, pp. 305-316, 1996.

Shamir, A., "Identity-Based Cryptosystems and Signature Schemes", *In Proc. of Crypto '84*, pp. 47-53, 1985.

Steiner, M., Tsudik, G. and Waidner, M., "Key Agreement in Dynamic Peer Groups", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 11, No. 8, pp. 769-780, 2000.

[5] Back, A., "Non-Interactive Forward Secrecy", http://www.cypherspace.org/~adam/nifs/, Dec. 2001.

[6] Anderson, R., "Two remarks on public key cryptology". Invited Lecture, ACM-CCS '97.