LIGHTWEIGHT AND SURVIVABLE KEY MANAGEMENT FOR ARMY BATTLEFIELD NETWORKS

Brian J. Matt, *Network Associates Laboratories*[1] [2]

Introduction. Wireless digital battlefield networks are essential for the Objective Force Warrior to achieve greatly enhanced lethality, situational awareness, fire control, logistics capability, mobility, survivability, and the capability to operate at much faster operational tempos. They will provide the backbone for the Objective Force by providing sensor data and C4ISR information to all elements of the operation. They will link the elements of the Force together and provide access to non-organic assets. These links must be achieved using wireless ad hoc mobile networks subject to noisy, bandwidth-constrained channels (hundreds of bits per second in some cases), intermittent connectivity between nodes, and partitioning of the network. Furthermore, many nodes may be significantly energy constrained.

Cryptography is essential to the survivability of battlefield networks. Cryptography protects the confidentiality, and establishes the integrity and provides authentication of sensor data, network control and configuration information, and critical command and control information flowing through the network. In order to use cryptography, secure key management services must be available. Existing key management solutions include those that assume pre-distributed secret keys (e.g., global keys or pair-wise keys shared by all pairs of network nodes) and solutions that require interactive highly trusted third parties (I-TTP) (e.g. symmetric key servers). These global keys and I-TTPs are not survivable, they are too easily compromised, and pair-wise keying does not scale to the size of an Object Force. Solutions that rely on public key cryptography (PKC) would suffer from the latency and energy cost of distributing public key certificates, as well as the overhead of using public key sized messages for key establishment over low bandwidth channels.[3]

Non-interactive, identity-based PKC. Recently, the use of identity-based PKC [5] has been advocated for battlefield network key management [3] — in particular, the use of non-interactive identity-based PKC (NIB-PKC) [4]. In a NIB-PKC system, a System Authority (SA) derives a set of secret system parameters and the corresponding public system parameters. The system's public parameters, like the signature verification key for a certificate authority, are widely known and are known to be authentic. Anyone can convert a user's or a nodes's public identification into a public key consistent with SA's public system parameters. The SA can take the public identification and its secret system parameters and generate the corresponding private key, which it then securely distributes to the user or node. In a non-interactive system, a member A of the system can combine the public system parameters, its private key, and the public identification of another member B to create a secret key K; similarly member B can use members A's public identification to also create K. Only these members and the SA can construct K *and the system does not use certificates.*

Following is a discussion of the impact of applying NIB-PKC to a number of challenges in battlefield network key management, focusing on the reduced communication costs, the increased flexibility and the survivability of NIB-PKC. The challenges are rapid keying of local groups, multicast group key initialization, keying for air ground support missions, and key management for reactive network routing.

Local Group-to-Group Keying. An important example of the use of group keying in battlefield networks is the formation of local group key situations where two groups, Groups J and K of Objective Force Warriors, encounter each other unexpectedly while under fire and need to quickly establish a common group key for authentication and to confidentially exchange tactical information. The groups already have their own secret group keys and have also pre-arranged additional group keys KG_{com} that they will share with other groups to speed up the process of establishing common group keys.[4] Even with the use of the pre-arranged keys this protocol takes a minimum of 5 seconds using RSA on a 1 Kbps data rate channel.

[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.

[2]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.

[3]In addition, the use of public key certificate directories or interactive trusted third parties in battlefield networks is not practical, since they are an attractive target for denial of service attacks, especially when placed in the network where they can be used most effectively, and will require considerable communication support from the network to be highly available.

[4]For example, one member of Group J, M_j, may engage in a public key protocol using RSA with a member of Group K, M_k, to establish that KG_{com} is the common group key. M_k sends a 2K bit certificate to M_j, who responds with a 2K bit certificate and an encrypted and signed message of over 1K bits to M_k. M_k then broadcasts securely to its group a message of over 200 bits containing KG_{com}, while M_j broadcasts securely to its group a message of over 100 bits indicating that KG_{com} has been shared with Group K. Total cost is over 5400 bits.

Of the NIB-PKC group keying protocols presented in [2], ID-STAR.1 is particularly well suited for this situation.[5] This protocol achieves authenticated Diffie-Hellman key agreement using long-term keys by only the exchange of identities, combined with group key transport, and reduces the communication cost of the public key portion of the Objective Force's protocol by over 90% and the overall time to 3/4 second on a 1 Kbps data rate channel.[6]

Multicast Group Keying. Multicast groups play a significant role in the operation of battlefield networks. Since the network is ad-hoc and the nodes are subject to compromise, techniques such as the Core Based Trees of Ballardie et al. are inappropriate. End-to-end solutions, such as Logical Key Hierarchy (LKH), are needed. However, their use is constrained by the high cost of initializing the group keying and the cost of adding new members. Our research has applied identity-based techniques similar to those presented above to multicast group initialization and to group member additions. When initializing LKH group key trees with our approach, we achieve savings in bandwidth (with commensurate savings in time and energy) compared to using RSA ranging from 80% for a group size of 16K, up to 89% for group size of sixteen.[7]

Role / Mission Group Keying. When warriors become isolated from normal communication channels in urban environments and need air support, their ability to communicate may be restricted (reduced view, range and bandwidth). The communication cost of soldier — aircraft key management must be minimized for the survivability of the Objective Force. Group orientated NIB-PKC offers a key management option that public key cryptography does not provide. Here time-limited public identities (TLPI) that correspond to groups of aircraft, or to aircraft operating in a sector for each day, are used. Since the aircraft operate out of bases with good communication channels to the SA, they can receive private keys corresponding to these TLPIs daily. Ground units contact aircraft using TLPIs rather than the aircraft's identity. The keying latency is reduced 94% compared to RSA-based protocols.[8]

Keying for Battlefield Network Routing. Mobile ad-hoc wireless networks frequently use reactive routing protocols. The need for confidentiality, authentication and integrity in secure reactive routing requires that security associations be established between widely distributed nodes that could not have been anticipated in advance.[9] Protocols that rely on public key cryptography either must assume the public keys/certificates are already distributed, or distribute them during route establishment. The first approach is clearly impractical for battlefield networks, and the second costs significant bandwidth, latency, and energy. Using identity based PKC we can significantly reduce the key management communications cost of initializing routes and adding new nodes to routes in battlefield networks.[10]

Summary. We have identified multiple challenges to Army battlefield networks that impact the operation of the Objective Force. Meeting the challenges requires substantial reduction in the latency and energy consumption of key management protocols and the ability for the Objective Force to perform key management independently of security infrastructures that can slow its deployment and reduce its agility and survivability. NIB-PKC addresses these problems and the limitations of protocols that implicitly assume that public key certificates are readily and cheaply available. Employing this technology, we have developed protocols that frequently provide nearly an order of magnitude or better reduction in key management communications costs.

References

[1] G. Cirincione, D. Carman, and B. Matt. Energy-efficient and low-latency key management for sensor networks. In *submission to The Twenty-Third Army Science Conference.*

[2] B. Matt. A preliminary study of identity-based, group key establishment protocols for resource constrained battlefield networks. Technical Report 02-xx, Network Associates Laboratories, (in preparation).

[3] B. Matt. Identity based group keying. ARL CTA-C&N Secure Group Communications Workshop, March 2002.

[4] U. Maurer and Y. Yacobi. A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, 9(3):305–316, 1996.

[5] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc of Crypto'84*, pages 47–53, 1985.

[5] The use of these protocols for sensor network key management is explored in [1].

[6] The combined cost of the exchanges between M_j and M_K are reduced from 5K bits to under 300 bits.

[7] The number of bits exchanged between group leader and group member ranges from 10.7K bits to 6.4K bits using RSA and LKH, and ranges from 2.0K bits to 0.7K bits using NIB-PKC and LKH.

[8] The combined cost of the exchanges between soldier and aircraft are reduced from 5K bits to under 300 bits. In addition, the ground units do not need to receive a message from the aircraft first; they only need to know that the aircraft is within communication range before they can establish a secure channel.

[9] Some authors assume that the associations already exist, but this assumption is not realistic in battlefield networks; since interactive trusted third parties are not available, public key cryptography must be used for key management.

[10] For example, we can reduce the key management communication cost when initializing a route in the Secure Routing Protocol of Papadimitratos and Hass by over an order of magnitude, by removing certificate transport costs and the use of PKC to establish shared secret keys.