Evaluation of Key Management in ad hoc Networks for Emergency and Rescue Operations (Extended Abstract)

A. M. Hegland * E. Winjum* Ø. Kure† S.F.Mjølsnes† C. Rong§ P. Spilling*
*UniK – University Graduate Center at Kjeller, †NTNU,Trondheim, §UiS, Stavanger

Abstract— *This paper surveys state of the art within key management for mobile ad hoc networks (MANETs), and evaluate the applicability for network layer security in MANETs for emergency and rescue operations.*

I Introduction

Reliable communication is mission critical to Emergency and Rescue operations. MANET technology allowing communication where fixed infrastructure is not available is very attractive for this setting. Emergency and Rescue operations may take place in both hostile as well as benign environment. The communication system must handle both situations. Security attacks can be launched towards any layer of the protocol stack. What is new with wireless ad hoc networks is the *network layer* routing information as a more probable target for security attacks. A reliable network service cannot be provided without embracing routing information security. The primary challenge is to decide which routing information can be trusted. The answer so far is cryptographically signed routing messages. The possession of cryptographic keys serves as proof of trustworthiness. A proper key management service is thus a critical factor for the success of wireless ad hoc networks.

II Emergency and Rescue Operations

Emergency and Rescue Operations are governed by international conventions and national laws and regulations. Organization, involved parties and roles are to a large extent predefined. No civilian volunteers are welcomed (unless they belong to an organization that takes part in the operation).

Two main operational scenarios that have implication for key management are: operations with participants from a *single security domain* and operations that involve participants from *multiple security domains.* In single security domain operations, all parties share a common, predefined point of trust. Examples of such operations include local, regional or national rescue operation with only predefined actors. That is, operations where pre-configuring of security credentials are possible. Multiple security domain operations involve parties that have had no prior contact, e.g., cross-border operations, operations involving “ad hoc” organizations as industrial companies, and similar. In other words, operations where no cross-domain pre-configured security parameters can be assumed.

III Key Management Schemes

Fig. 1 shows a classification of generic types of key management schemes.

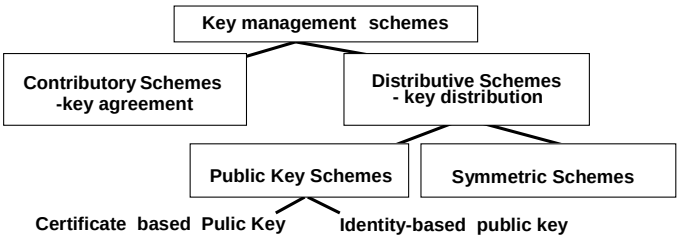

Fig. 1 Classification of Key Management schemes

IV Contributory Schemes

The main implications and limitations of contributory schemes are demonstrated by the following schemes:

--**D-H:** *Diffie-Hellman* [9]
--**ING:** *Ingemarsson, Tang and Wong CKDS* [12]
--**B-D:** *Burmester and Desmedt [6]*
--**H&O:** *Hypercube and Octopus* [4]
--**CLIQ:** *CLIQUES* [16]
--**A-G:** *Password authenticated key agreement* [2]

The contributory approach of no trusted third parties and previously exchanged security credentials fits well for both single security domain and multiple security domain scenarios. However, none of the contributory schemes are good candidates for key management in wireless ad hoc networks. The main deficiencies of D-H, ING and H&O are missing authentication. B-D and CLIQ have an inherent survivability problem as they require reliable multicasting. A-G is the best alternative, but exhibits limited robustness and scalability in dynamic networks.

V Distributive Schemes

a. Public Key Schemes

Z-H: *Zhou and Haas partially distributed Threshold CA Scheme [19]*- a framework to provide an available, fault-tolerant and non-vulnerable CA functionality in the ad hoc networking environment – assuming a traditional PKI system

MOCA *[17][18]:* an extension to Z-H [19] specifying how to select CA servers (MOCAs), and moving the combiner function of Z-H from the CA servers to the requesting end-nodes. The MP protocol proposed to provide efficient and effective communication between clients and MOCAs.

UBIQ: *Ubiquitous Security Support* [14] - fully distributed Threshold CA scheme. CA =Coalition of 1-hop neighbors.

PGP-A*: Self-organized Key Management* [7]- PGP adapted to ad hoc networks.

IBC-K: *Identity-based public key [13] [15]* - removing the need for certificates.

Summary of the public key schemes: Z-H, MOCA and PGP-A assumes an already running routing protocol. The need for an on-line CA to sign certificates is questionable. UBIQ allows ad hoc establishment of trust, but demands certificate exchanges. IBC-K performs better than the certificate based systems as bandwidth is limited. IBC-K, making certificate exchanges superfluous, is an interesting candidate for wireless ad hoc networks. The reliance of a PKG makes it best suited for single security domain operations. Depending on whether the security policy demands centralized trust management or not, IBC-K or UBIQ fits better in case of multiple security domains operations.

b. Symmetric Schemes

KDC: *Pre-distributed group key:* -The old and well-proven manual key management scheme with a Key Distribution Centre distributing symmetric keys.
PEBL: *Secure Pebblenets [3]* - aims at a network-wide traffic encryption key for protection of application data. At the network layer a pre-installed group key guarantees the authenticity of a pebble as a member of a group.
PRE: *Probabilistic Key pre-distribution [8], [10]:* nodes are outfitted with a pre-installed key ring, i.e. a set of keys drawn randomly from a large pool of keys.
INF: *Key Infection (INF) [1]* -symmetric keys "whispered" in the clear to neighbors.
Summary of the public key schemes: KDC is the only one acceptable for emergency and rescue operations.

VI Conclusions

Our evaluation has focused on *network layer* security. Key management for application layer security is a topic for further analysis. No single technique was found superior to all others. The simplest solution is the old and well-proven: pre-configured symmetric group keys (KDC). But it offers no intrusion tolerance. Furthermore, multiple security domain operations call for some means of transferring the group key from one node to another. The alternative is an on-scene Key Distribution Centre where new members of the rescue team are required to sign in.

For single security domain operations demanding a more intrusion tolerant scheme the scheme relying on identity-based public key cryptography (IBC-K) appears as the best candidate. With limited bandwidth, the elimination of certificates makes it a better option than the other public key schemes. Its reliance on a trusted entity (PKG) to provide private keys calls for an on-scene PKG service in case of multiple security domain operations. If the security policy opens for distributed trust management UBIQ fits better for the multiple security domain operations setting. However, UBIQ still requires bandwidth consuming certificate-exchanges and off-line authentication when new members join. Secure and efficient key revocation is an open challenge for all schemes.

REFERENCES

[1] Anderson, R., Chan, H. and Perrig, A., *Key infection: Smart trust for smart dust*, 12th IEEE International Conference on Network Protocols, ICNP'04, 2004, p.206-215.

[2] Asokan, N., and Ginzboorg, P., *Key agreement in ad-hoc networks*, in *Computer Communications*, vol. 23, 2000, p. 1627 – 1637.

[3] Basagni, S., Herrin, K., Bruschi, D. and Rosti, E., *Secure pebblenets*, 2nd ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), 2001, p. 156-163.
[4] Becker, K., and Wille, U., *Communication complexity of group key distribution*, 5th ACM conference on Computer and Communication Security, 1998, p.1-6.
[5] Boneh, D. and Franklin, M., *Identity-based encryption from the weil pairing*, Crypto 2001, Springer, 2001,p. 213-229.
[6] Burmester, M., and Desmedt, Y., *A secure and efficient conference key distribution system*, Advances in Cryptology - EUROCRYPT'94, Springer-Verlag, 1994, p. 275-286.
[7] Capkun, S., Buttyán, L. and Hubaux, J. P., *Self-Organized Public-Key Management for Mobile Ad Hoc Networks.* IEEE Transactions on mobile computing, 2003. 2(1): p. 1-13.
[8] Chan, H., Perrig, A., and Song, D., *Random key predistribution schemes for sensor networks*, IEEE Symposium on Security and Privacy, IEEE Computer Society, 2003, p. 197-213.
[9] Diffie, W., and Hellman, M.E., *New Directions in Cryptography*. IEEE TRANSACTIONS ON INFORMATION THEORY, 1976. IT-22: p. 644-654.
[10] Eschenauer, L., and Gligor, V.D., *A key-management scheme for distributed sensor networks*, The 9th Conference on Computer Communication Security (CCS2002), ACM Press, 2002, p. 41-47.
[11] Hegland, A.M., Winjum, E., Kure, Ø., Mjølsnes, S.F., Spilling, P., *Key Management in ad hoc Networks, Survey and Evaluation*, UniK report, 2005.
[12] Ingemarsson, I., Tang, D., and Wong, C., "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. 28, 1982, p. 714-720.
[13] Khalili, A., Katz, J., and Arbaugh, W.A., *Towards secure key distribution in truly ad-hoc networks*, IEEE Workshop on Security and Assurance in Ad hoc Networks - in conjunction wiht the 2003 International Symposium on Applications and the Internet, 2003.
[14] Kong, J., Zerfos, P., Luo, H., Lu, S., and Zhang, L., *Providing robust and ubiquitous security support for mobile ad-hoc networks*, The Ninth International Conference on Network Protocols (ICNP'01), IEEE Computer Society Washington, DC, USA, 2001, p. 251-260.
[15] Shamir, A., *Identity-based cryptosystems and signature schemes*, CRYPTO '84, Springer, 1984.
[16] Steiner, M., Tsudik, G., and Waidner, M., *CLIQUES: A new approach to Group Key Agreement*. in *ICDCS'98*. 1998.
[17] Yi, S., and Kravets, R., *Key Management for Heterogeneous Ad Hoc Wireless Networks*, University of Illinois at Urbana-Champaign, Urbana, 2002.
[18] Yi, S., and Kravets, R., *MOCA: MObile Cerificate Authority for Wireless Ad Hoc Networks*, Report No. UIUCDCS-R-2004-2502,UILU-ENG-2004-1805, University of Illinois at Urbana-Champaign, Urbana, 2002
[19] Zhou, L., and Haas, Z.J., "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, 1999, p. 24-30.