Two Level Hybrid Key Scheme for Efficient Key Distribution in Mobile Ad-Hoc Networks

John S. Baras and Maria Striki *
Electrical and Computer Engineering Department
and the Institute for Systems Research
University of Maryland College Park
College Park, MD 20742

ABSTRACT

Military command and control require that information be communicated to the appropriate groups and only with the utmost security. At the same time the environment envisioned by the Objective Force is mobile ad-hoc and consists of a large number of heterogeneous nodes deployed in a hostile field of limited bandwidth and unreliable channels. The nodes of the network may present severe bandwidth, energy, capacity and processing constraints (vary from Satellites, PDAs, laptops, to GPS devices, cellphones and pagers). In this work we develop a secure, robust and scalable key management scheme for multicast communications. This service is very important in determining the security and efficiency of the network. It consists of key generation, entity authentication and key distribution. We assume that the nodes are already authenticated and focus on studying and developing key distribution techniques with the aim to achieve scalability and high performance of our key distribution framework without sacrificing the security level of the network. For that we need to reduce the total storage, communication and computation cost of the nodes, resulting from the key distribution protocol we apply to our network. The new key distribution framework we designed is a **hierarchical, two-level hybrid key management scheme**.

1. INTRODUCTION

In this work, we have derived analytical expressions for the evaluation of the communication, computation and storage costs of key distribution protocols for MANETs. To this end we have studied the Group Key Management Protocol **GKMP** (Harney et al., 1997), the Core Based Tree **CBT** (Harder et al., 1999), the One-Way function Tree **OFT** (McGrew et al., 1998), the **2^d-Octopus** and its variations (Asokan et al., 2000), the Efficient Large Key Distribution **ELK** (Perrig et al.), the Diffie-Hellman group **GDH** protocols (Steiner et al., 1996). Their performance (along with our own enhancements to some of those, and new hybrid ones) was evaluated with respect to these metrics and their applicability to the designated military environment was examined.

We incorporated the most efficient key distribution schemes in terms of performance and robustness into the two-level hybrid scheme, in various combinations and conducted an overall performance evaluation of the model for every such combination. The results demonstrate which combination presents the best overall performance given the ratio of users at each level (n_2/n_1), the relative ratio of the mobility of users (p_2/p_1) and those that determine the level of security: length of key (K), number of offspring of a tree (d) in a tree based scheme. Thus, we developed a theory and a software tool for evaluation and design so that given the parameters of the network we can decide on the most appropriate version of the two-level hybrid model for that particular case.

2. TWO-LEVEL HYBRID MODEL

We believe that the two-level hybrid scheme is the most appropriate for the requirements of the Objective Force for the following reasons: it links key distribution schemes to network topology, hierarchy, predicted or unpredicted member mobility, routing. The nodes are heterogeneous so their links are of variable qualities, their paths are uni/bi-directional, asymmetric, they have larger bandwidth resources at higher tiers (satellites) and restricted at lower (cellphones, laptops). They also have different physical/communicational mobility levels. At the low end mobility is more rapidly changing. Nodes at the low end often have only intermittent connectivity to reach nodes at the higher end. Moreover, at the low end higher degree of self-organization is observed. Our key distribution scheme takes these environmental variations into account and models them so that the first level of the scheme represents nodes at the higher end, and the second level nodes at the lower.

The scheme has the following modules: In the upper level the Group Security Controller **(GSC)** node is the leader of the upper level group built from all the nodes called Group Security Agents **(GSAs)**. Every GSA is the leader of a group of simple members of the second level, and in practice it is dynamically selected. The GSC is also leader of all the group members of the second level. In the upper level we can assume a satellite or a UAV as the GSC. It has relatively low mobility but high bandwidth

and processing capabilities. It controls the GSAs and the members, so it is responsible for the whole network. GSA controls one group of members only, so the requirements for energy, bandwidth and computation power can be lower than those of the GSC. Every multicast group will acquire its own group key. We also investigate the effect of mobility and link failure in a MANET by providing corresponding values for the probabilities p_1, p_2.

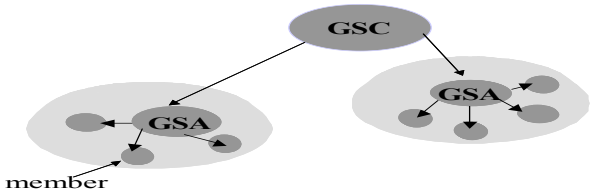

Figure 1: The two-level hybrid key management scheme

2.1 Parameters

In order to get closed analytical expressions for the cost functions, we have derived the computation cost for generating a key (C_r), for Public Key Infrastructure (PKI) encryption/decryption (C_{PE}/C_{PD}), for symmetric key encryption/decryption (C_{SE}/C_{SD}), for applying hash functions, and performing exponentiations. We show how these values and all the costs of the scheme as a consequence, depend on the key tree parameters (d, h), the frequencies of the member motion (p) and the length of keys (K). We select the RSA method for modeling the PKI, and the DES method for the symmetric encryption/decryption. (Contributory protocols provide security by performing a number of exponentiations).

2.2 Key Distribution Schemes Evaluation

We distinguish between the two different families of key distribution protocols: those based on a trusted entity to distribute the keys, and the contributory ones based on key agreement. Through our theoretical research and the performance evaluation we conclude that the contributory protocols are only appropriate for relatively small groups. For a larger number of nodes the substantial number of exponentiations that have to be done overshadow the advantage of not requiring a central controller. Apart from that, the key agreement protocols are not fault tolerant. If the connectivity of a node is lost (node out of range, no battery resources left, intentionally quit the group etc) during the establishment of the session key, the process for session key has to start all over again. This causes substantial overhead to the system. Contributory protocols could be used for the group of GSAs, which are less likely to disconnect, if the number of GSAs is not that large. Apart from that, their performance compared to protocols derived from CBTs, like OFT (seems to be prevailing) and ELK is poorer for most of the cases.

Parameter	GKMP	CBT	OFT
Initial Comm/cation	2 n K	(n + d(n-1)/(d-1)) K	3nK
Add GSC computation	$2\,C_r + C_{PE} + 2\,C_{SE}$	$(h+1)\,C_r + C_{PE} + 2\,h\,C_{SE}$	$C_r + C_{PE} + h(C_{SE}+2C_g)$
Add member computation	$C_{PD} + C_{SD}$	$C_{PD} + h\,C_{SD}$	$C_{PD} + hC_{SD} + hC_g$

Table 1: a small sampling of cost parameters for a few protocols

ACKNOWLEDGMENTS

Prepared through collaborative participation in the Collaborative Technology Alliance for Communications & Networks sponsored by the US Army Research Laboratory under Coop. Agreement DAAD19-01-2-0011.

REFERENCES

Becker, K. and Wille, U., "Communication Complexity of Group Key Distribution," Proc. 5th ACM Conf. on Computer /Communications Security, pp 1-6, 1998.

Harder, E. and Harney, H., "Logical Key Hiearchy Protocol". Internet Draft, IETF, April 1999.

Harney, H., Muckenhirn C., " Group Key Management Protocol (GKMP) Specification/Architecture", Internet Engineering Task Force, July 1997.

McGrew, D. and Sherman, A., "Key Establishment in Large Dynamic Groups Using One-Way Function Trees", May 1998.

Perrig, A., Song, D. and Tygar, J., "ELK, a new Protocol for Efficient Large-Group Key Distribution". Proc. IEEE Security and Privacy Symposium, May 2001

Steiner, M., Tsudik, G., Waidner, M., "Diffie-Hellman Key Distribution Extended to Groups", 3rd ACM Conference on Computer /Communications Security, ACM Press, 1996, pp. 31-37.

CONCLUSION

Most of the evaluated protocols reduce the communication overhead at the expense of computation cost (OFT protocol) or do the opposite. Our results indicate that these two cost values are antagonistic. Moreover, some of the operations inherent in the protocols (e.g. public encryption, exponentiations) are so costly that even smart improvements that some of the protocols achieve don't reduce the value of a given parameter (communication/computation/storage cost) as dramatically as expected (and the reduction is at the expense of another cost value). So we need to invent more efficient schemes for our PKI, or invent more radical key distribution protocols that manage to significantly reduce at least one of the desired parameters, preferably the communication cost.