Distributed Certification Authority Generation to Enhance Autonomous Key Management for Group Communications 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

A MANET is a collection of wireless mobile nodes dynamically forming a temporary network, without the use of fixed infrastructure, and this is exactly the environment envisioned for military operations by the Objective Force. Military command and control rely on secure group communications, therefore key management (KM) schemes that ensure secure communications under MANET constraints are required. However, without fixed infrastructure, e.g. Certification Authorities (CAs), trusted third parties (TTPs), the design of KM becomes very difficult, since its' most fundamental service – entity authentication, privileges update/revocation - rely on these entities to establish trust among nodes, terminate or renew participation to secure operations in a pre-agreed, global manner. Without this guarantee, all subsequent KM operations make no sense. So, it is of paramount importance to provide a secure authentication service that detects misbehavior and defends against dishonest users in the network. Thus, the challenge lies in dynamically generating mechanisms that provide individual nodes and KM groups with functionalities similar to those of the original CAs of fixed infrastructure. In this work, we develop distributed, scalable, and efficient mechanisms for dynamically generating CAs in MANETs, by **distributing** the tasks of a CA among legitimate members of **existing KM groups** (preferably hierarchical). We show how the features of our scheme render it superior in performance and resilience, and how group KM properties are exploited to avoid heavy bandwidth-delay solutions of other proposals in the literature.

1. INTRODUCTION

Web-of-trust based models where users alone issue and revoke certificates do not scale well and are susceptible to dynamically from a given set of "powerful, trusted" nodes. This assumption may not hold for most MANET attacks. Other existing proposals rely on the cryptographic primitives of *threshold cryptography* to generate CAs frameworks. Other schemes allow any node to participate to the dynamic CA generation. Dishonest users cannot be handled this way, to name one of the drawbacks. Schemes that rely merely on blindly applying threshold algorithms issue substantial communication bandwidth and are inefficient for MANETs. One version of our scheme also relies on threshold cryptography to some extent, but instead it selects the set of its participant nodes among **members of existing KM groups** in the network**, based on additional criteria** also. It is the **first** attempt that combines the primitives of threshold schemes with the attributes of existing frameworks of **hierarchical KM groups** to dynamically construct efficient, scalable and robust "localized" CAs. Our selection is motivated by the following observations: the introduction of hierarchy through KM subgroups results in more efficient and reliable execution of operations like monitoring nodes, collecting group and network information, detecting faults etc. Also, our scheme operates on top of a pre-existing framework and combines its functions with those of KM so that redundancies are eliminated and the efficiency of the scheme is further improved. Group members are periodically authenticated, and this attribute can be exploited to further reduce the cost of our scheme.

2. DYNAMIC CA GENERATION MODEL

Constructing a dynamic CA reduces to generating a pair of CA public (PK) and secret key (SK): the SK is shared among the subset of designated members (DM), and the PK is propagated to nodes in the network. We provide three different algorithms for this operation, based on the underlying group key generation protocols and other assumptions. The third algorithm which is more generic, uses a (k, n) threshold scheme that allows a CA signing key to be split into n shares such that for a certain threshold $k<n$, any k entities could combine and recover the signing key whereas k-1 or fewer shares cannot do so. In our model, n is the number of subgroup members, selected initially to participate to the CA generation, and k is a security threshold, selected on the fly.

Trusting a member alone with the SK exposes the CA to single point of failures and to adversarial behavior, especially if this member leaves the group, and cannot be monitored any more. A *threshold* scheme *without the*

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S Army Research Laboratory under the Collaborative Technology Alliance (CTA) 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.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Distributed Certification Authority Generation to Enhance Autonomous Key Management for Group Communications in Mobile Ad-Hoc Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Electrical and Computer Engineering Department and the Institute for Systems Research University of Maryland College Park College Park, MD 20742

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

trusted dealer assumption totally avoids this problem but is very inefficient to apply to MANETs as such. However, one of our approaches utilizes a modified version of this algorithm over KM subgroups with leaders, and combines its operations with the KM functions efficiently, so that the resulting scheme becomes more lightweight.

Our scheme efficiently operates on a resource-constrained network, as it introduces low bandwidth and computation overhead. It uses group KM information to periodically evaluate the network overhead incurred from the current CA operation under membership and dynamic changes, and decides whether a new CA should be constructed for the particular subgroup instead. This scheme is also robust and can successfully accommodate the dynamics of the network (mobility, failures), relying on the hierarchy of the framework to handle changes locally, and exploiting the redundancy of the threshold scheme. The DMs are selected so that the CA can be maintained for the longest possible period (optimally as long as the KM subgroup is alive). It is a highly distributed scheme, since it only relies on individual member operations to control nodes, collect information and decide on renewal/revocation of a certificate.

2.1 Highlight of the Dynamic CAs Algorithm

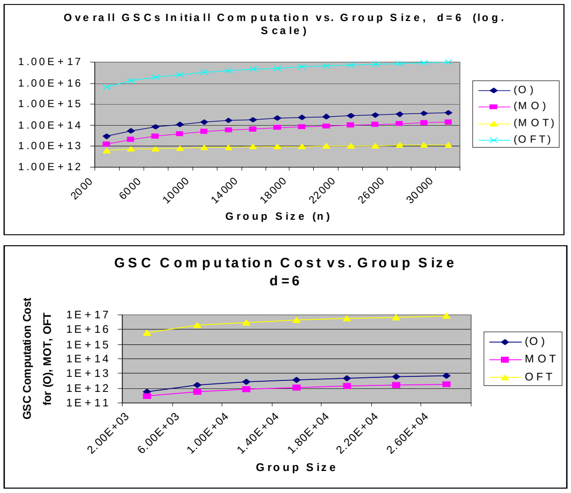
We briefly describe the phases that highlight the basic features of our algorithm for construction, operation and maintenance of dynamic CAs in MANETs:

P1: Select DMs to participate to the CA generation: This selection is customized to the individual key generation (KG) protocol of each subgroup. If a subgroup leader exists, it will participate actively to the selection process. Members combine their already acquired knowledge about other subgroup members along with local "Hello" messages to collect information about their 1-hop or 2-hop neighbors on metrics that will be used for the selection of the "best local candidate": e.g. level of trust (certificate status, voting results, accusation lists), connectivity strength, average velocity deviation, etc. After this phase, the IDs of the DMs become known to all group members. A subgroup leader, if available, operates on top of this algorithm, interacting with local decisions, to facilitate both the selection and the propagation phase.

P2: DMs generate CA <SK, PK>: DMs may use any of the three algorithms we have designed to derive the desired keys, depending on what our security and efficiency requirements are, and on the underlying subgroup KG protocol: 1.Modified **Merkle** Trees (MMT), 2. **Schnorr** based, 3.Modified **Pedersen** (threshold w/o dealer). Each approach is superior to the rest w.r.t. different metrics, but all handle the demands of MANETs quite well, as shown in our analytical and simulation results. In all cases, the tradeoff between robustness and security vs. bandwidth and delay is obvious.

P3: Distributed CA issue, renew/revoke certificates in steady state: A number of DMs consult their "accusation lists", or subgroup leader if available, and collect their neighbor and KM subgroup information, before casting their votes and committing to them with the aid of Merkle Trees. They propagate their decision to the rest of the subgroup members, which "accept" if they receive the same decision outcome from at least *z* different sources.

2.2 Evaluation of Dynamic CA Algorithms Versions



Figures 1, 2: Computation Costs of KM protocols w/o or w/ the consideration for the dynamic CA operation capabilities

These graphs show the computation costs of a few hierarchical KM protocols. Only the protocols of the second graph have been provided with two CA construction algorithms: the MMT & Schnorr-based approaches. It can be seen that the additional overhead issued from these algorithms is very low.

CONCLUSION

We have developed three distributed algorithms for the dynamic generation of CAs in MANETs, by distributing the tasks of a CA among legitimate members of existing KM groups. Our scheme utilizes the pre-existing framework and functions the best possible way, and benefits from the hierarchical structure of KM groups, so that the KM framework remains relatively lightweight despite its extra features. We are currently simulating our schemes with certain mobility scenarios to estimate their robustness in MANETs in practice.

REFERENCES

Pedersen T.P., "A Threshold Cryptosystem w/o a Trusted Party", Eurocrypt'91 Procs., Lecture Notes in Computer Science, LNCS 547, Springer Verlag, pp.522-526, 1991.

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 of the U.S Government