DISTRIBUTED CERTIFICATION AUTHORITY GENERATION TO ENHANCE AUTONOMOUS KEY MANAGEMENT FOR GROUP COMMUNICATIONS IN MANETS[1][2]

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

A MANET is a collection of wireless mobile nodes dynamically forming a temporary network, without the use of fixed infrastructure or centralized entities, and this is exactly the environment envisioned for military operations by the Objective Force. Military command and control rely on secure (multicast) communications, and thus key management (KM) schemes that ensure secure communications under MANET constraints are required. However, without fixed infrastructure, e.g. trusted third parties (TTPs), Certification Authorities (CAs), the design of KM becomes particularly 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, under MANET constraints. In this work, we develop distributed, scalable, robust and efficient mechanisms for dynamically generating CAs in MANETs, **by distributing the tasks of a CA among legitimate members of existing (preferably hierarchical) KM groups**. We will show how the features of our scheme render it superior in performance and resilience and how properties of KM groups are exploited to avoid impractical heavy bandwidth-delay solutions of other proposals in the literature.

Web-of-trust based models where users alone issue and revoke certificates are susceptible to attacks and do not scale well. Most of the existing proposals rely on the cryptographic primitives of *threshold cryptography* to generate CAs dynamically from a set of designated nodes. Some schemes assume the existence of "powerful, trusted" nodes and select nodes from this set, but this assumption may not hold for most MANET 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. 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.

We create 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 that have been selected initially to participate to the CA generation and k is a security threshold, selected on the fly, depending on certain KM and network parameters. The dynamic CA construction reduces to the generation of 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.

[1] 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.
[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 of the U.S Government

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 trusted dealer* assumption totally avoids this problem but is very inefficient to apply to MANETs. 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 so efficiently, that the **resulting** scheme is far more **lightweight**.

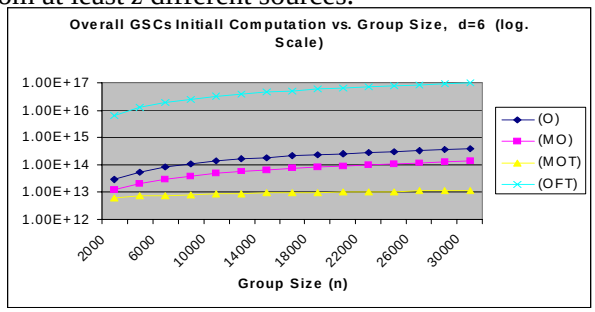
Our scheme **efficiently** operates on a resource-constrained network, because it introduces very low bandwidth and computation overhead. It uses subgroup KM information to periodically evaluate the network overhead incurred from the current CA operation under membership and dynamic changes, and decides whether a new CA should be constructed for the particular subgroup instead. This scheme is also very **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 – *k* out of *n* members suffice to sign a certificate. 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) in the first place. 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.

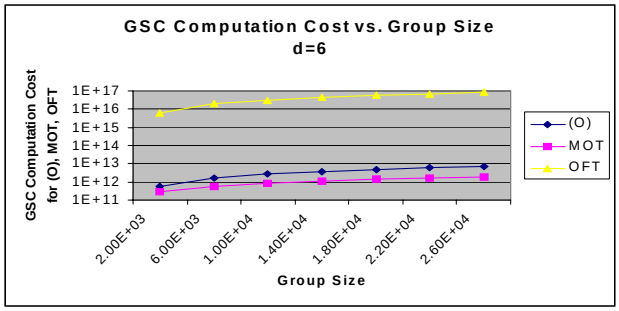
We distinguish and briefly describe the following phases that highlight sequentially the basic features of our algorithm for dynamic construction, operation and maintenance of CAs in MANETs:

P1: Select DMs to participate to the CA generation: This selection is customized to the individual key generation 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 (e.g. certificate status, voting results, accusation lists), connectivity strength (number of active links to group members), 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, and add to the robustness of the scheme.

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 key generation 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", the subgroup leader if available, and collect their neighbor and KM subgroup information, before casting their votes and committing to them via the Merkle Tree scheme. They propagate their decision to the rest of the subgroup members. The subgroup members "accept" if they receive the same decision outcome from at least *z* different sources.





These two 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 OH issued from these algorithms is very low.

[1].T.P.Pedersen, "A Threshold Cryptosystem without a Trusted Party", in Proc. of Eurocrypt'91, Lecture Notes in Computer Science, LNCS 547, Springer Verlag, pp.522-526, 1991