# On the Performance of Group Key Agreement Protocols *

Yair Amir † Yongdae Kim ‡ Cristina Nita-Rotaru † Gene Tsudik ‡

## 1 Introduction

Group key agreement (GKA) is a fundamental building block for securing peer group communication systems (GCS). Several group key agreement protocols were proposed in the past, all assuming an underlying group communication infrastructure.

This paper presents a performance evaluation of 5 notable GKA protocols integrated with a reliable group communication system (Spread). They are: Centralized Group Key Distribution (CKD), Burmester-Desmedt (BD), Steer et al. (STR), Group Diffie-Hellman (GDH) and Tree-Based Group Diffie-Hellman (TGDH).

We present concrete results obtained in experiments on local- and wide-area networks. Our analysis of these results offers insights into their relative scalability and practicality. An in-depth conceptual evaluation accompanied by details and analysis of both protocols and experiments can be found in [1].

## 2 Experimental Results

We measured the total time necessary to establish a secure group membership following a group membership change. This time includes the communication and computation costs of the GKA protocol and the cost of the membership service provided by the GCS. Our results reflect the two most common events: join and leave.

A longer version of this paper [1] includes details of the group communication system's performance and cryptographic operations on the experimental platform we used as well as the detailed description of the test scenarios.

### 2.1 Experimental Results in LAN

The experimental testbed was a cluster of thirteen 667 MHz Pentium III dual-processor PCs running Linux.

In Figure 1, the first row shows the average time necessary for a group to establish a secure membership when a new member joins the group. For the 512-bit modulus (left), overall, STR outperforms the others except for very small groups where BD is the most efficient. However, as the group size grows, BD deteriorates rapidly becoming the worst performer after the group size exceeds 30.

For the 1024-bit modulus, GDH is the slowest due to the sharp increase in modular exponentiation, whereas, BD does not show the same deterioration as in the 512-bit case, remaining the best for very small groups up to 14 members. In both graphs, TGDH and STR are fairly close with the latter performing slightly better.

In Figure 1, the second row shows the average time needed for a group to establish a secure membership after a member leaves. TGDH outperforms the rest, as it requires the fewest ($O(log\ n)$) modular exponentiations (vs. GDH, CKD, STR) and signature verifications (vs. BD). This sub-linear behavior becomes particularly evident past the group size of 30. BD is the worst in 512-bit leave. STR, CKD and GDH all exhibit linear increase in cost. CKD and GDH are quite close while STR's linear factor is $2n$ which makes its slope steeper.

In case of the 1024-bit modulus, STR is the most expensive protocol, since it involves (more expensive in 1024- than in 512-bit case) modular exponentiations.

### 2.2 Experimental Results in High-Delay WAN

For the WAN environment we used the same number of machines as for the LAN environment, to ensure the same computation distribution. We used an experimental testbed of thirteen PCs running Linux: ten 667 MHz Pentium III dual-processor PCs, one 1.1 MHz Athlon and one 930 MHz Pentium III PCs, located as follows: eleven machines at Johns Hopkins University, Maryland, one machine at University of California at Irvine and one at the Information and Communications University, Korea.

Figure 2 (left) presents our results for join. We note that the GDH protocol performs significantly worse than the others due to the number of communication rounds ( 4 rounds while the others require only 2 rounds). The rest of the protocols are in the same range, with BD becoming more expensive for a group size bigger than 30, while STR and TGDH show similar performance. Though CKD has

*This work was supported by grant F30602-00-2-0526 from DARPA.

†CS Dept., Johns Hopkins University, Baltimore, MD 21218, USA. {yairamir,crisn}@cs.jhu.edu

‡ICS Dept., University of California, Irvine, Irvine, CA 92697-3425, USA. {kyongdae,gts}@ics.uci.edu

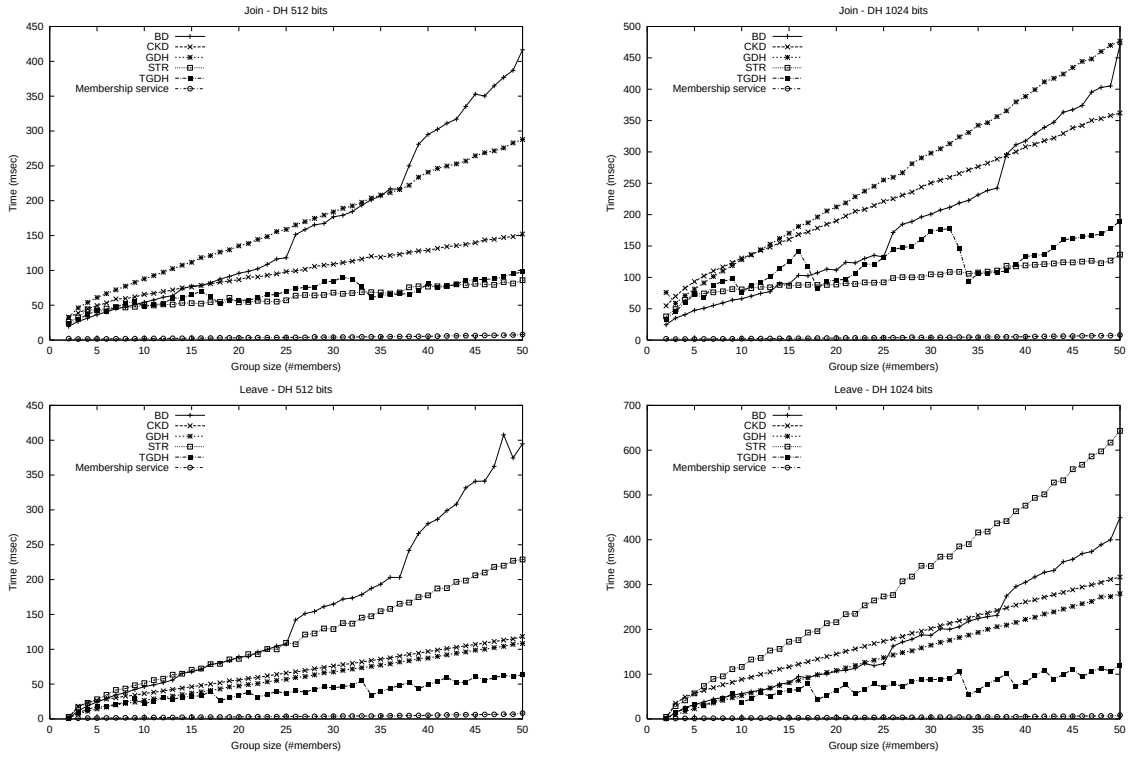


**Figure 1. LAN - Join and Leave (average time)**

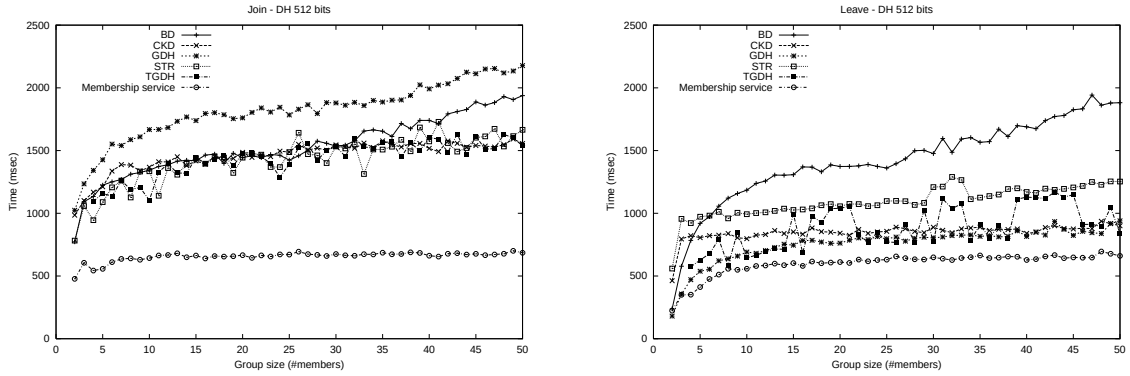


**Figure 2. WAN - Join and leave (average time)**

three rounds, two of them are unicasts which helps it to remain competitive with respect to the other protocols.

In case of leave (see Figure 2, right), BD is the most expensive protocol in our WAN setup, due to the two rounds on $n$ broadcasts and its high computational cost. GDH, CKD and TGDH require only a single broadcast, thus, they exhibit similar performance results. Although STR also requires only one broadcast, it has significantly higher computation cost with respect to the rest.

## 3 Conclusions

In this work, we investigated the performance of five group key agreement protocols in a realistic network setting. We integrated the protocols with a reliable group communication system (Spread) and measured their behavior in both LAN and WAN settings. The results indicate that TGDH exhibits the best average performance in both cases. **A much more complete and detailed version of this work can be found in [1].**

## References

[1] Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik, "On the performance of group key agreement protocols," Tech. Rep. CNDS 2001-5, Johns Hopkins University, Center of Networking and Distributed Systems, 2001. http://www.cnds.jhu.edu/publications/.