This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

Technical Report

Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing

Brett Hemenway, William Welser IV, Dave Baiocchi

RAND Project AIR FORCE

Prepared for the United States Air Force

The research described in this report was sponsored by the United States Air Force under Contract FA7014-06-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-0-8330-8166-7

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS

BOSTON, MA • CAMBRIDGE, UK • BRUSSELS, BE

www.rand.org

Summary

Using Orbital Information to Prevent Collisions in Space

The United States has been interested in protecting its on-orbit assets ever since the first U.S. satellite was launched in 1958. Since that time, the United States has been monitoring the location of objects in orbit to maintain custody of its satellite inventory, as well as predict and prevent collisions between known objects. The Space Surveillance Network (SSN), managed by U.S. Strategic Command (USSTRATCOM) and staffed by 14th Air Force, currently tracks more than 20,000 orbital objects larger than 10 cm in diameter. The data collected by the SSN are used to maintain a master catalog of known space objects, and this catalog is then used to estimate the probability of collisions involving active satellites. When a collision is predicted, the operator is notified, and evasive action can be taken.

The SSN tracks both operational and defunct satellites as well as space debris. Although debris can only be tracked passively (i.e., using sensors to detect these objects), operators of active satellites can take advantage of on-board instrumentation to provide more accurate coordinates on where the satellite is located in orbit. This operational data has an advantage over that obtained by the SSN for two reasons. First, operational data is of higher fidelity than the positional data available via the SSN. Second, the data provided by the SSN can never predict active maneuvers made by operational satellites. Any reactive tracking system like the SSN will have inherent delays in recognizing active maneuvers, and in some cases, active maneuvers can cause the SSN to temporarily lose track of the object. Both of these issues could be mitigated if satellite operators were willing to share data with each other about their satellites' positions. However, under current practice, this does not happen across the industry because the operators want to ensure that their data will be protected as private.

Privacy Concerns

The satellite community has long recognized that data sharing among operators could be used to improve space situational awareness (SSA). Although the benefits of data sharing are known, privacy concerns prevent satellite operators from sharing the accurate orbital information they possess about their satellites. Governments view such orbital information as state secrets because it could provide adversaries with insight on future intentions, and are therefore unwilling to make the information public. Private corporations view their active tracking data as proprietary information, and they fear that revealing these data would provide an advantage to their competitors.

To date, there have been some small-scale efforts to share information between operators while also providing a level of privacy. These operators employ a trusted third

party to privately calculate collision probabilities for them. These calculations are called "conjunction analyses." In practice, this means that participating operators provide their private, highly accurate information to the trusted third party. The third party then performs the conjunction analyses, and returns the results to the operators. Data-sharing agreements of this type allow operators to reap the benefits of coordination and cooperation while still maintaining their own privacy. However, these data-sharing agreements require operators to find an outside party trusted by all participants. Finding such a trusted party can be difficult, and, in some cases, could be impossible, especially if the participants are large nation-states. Even if a mutually trusted party can be found, the limited availability of such trusted parties allows them to charge a premium for their services.

Privately Sharing Information Through Secure Multiparty Computation

Recent advances in the field of cryptology have produced tools that can be used to allow groups of participants to coordinate their actions, without the need for a trusted third party, while still maintaining the privacy of each individual's secrets.

These cryptographic tools are called secure multiparty computation (MPC). In its most general form, MPC allows a group of parties with private inputs to engage in a secure protocol that allows them to compute a joint function of their inputs while maintaining the privacy of each party's input.[1] In this context, an MPC protocol replaces the trusted third party, and each participant can be assured that their data will remain private, irrespective of the actions of the other participants. MPC therefore allows two operators—each with their own private orbital information—to engage in a protocol to securely compute a conjunction analysis, while maintaining the privacy of each operator's orbital information. In particular, the security of the protocol guarantees that operators learn no more than if a trusted third party had performed the conjunction analysis computation. In either setting, however, the result of the conjunction analysis computation reveals some information. For example, a conjunction analysis calculation that reports a high collision probability reveals the fact that another operator's satellite is close to your own. Whether conjunction analyses are performed by a trusted third party or via MPC, a malicious operator could attempt to learn positional information about other satellites by performing repeated conjunction analysis calculations inputting diverse (and possibly fabricated) orbits for its own satellites. The primary benefit of computing

[1] A secure protocol is a set of public rules that specify messages that each participant must send in order to execute the desired task (e.g., performing a conjunction analysis). A participant's initial message depends on his/her private inputs. Subsequent messages are crafted based on both private inputs and messages received from other participants. To be secure, the protocol must be designed so that the messages that are sent reveal nothing about the participants' inputs beyond the final result of the calculation (e.g., the collision probability).

conjunction analyses using MPC is that it allows cooperation without any need for mutual trust between the operators, because the operators cannot see each other's data.

MPC Is Feasible

The initial MPC algorithms were first developed in the 1980s;[2] since then, the cryptographic community has accepted these methods as providing mathematically provable security. Although these methods are secure, the general protocols have been seen as too inefficient for practical applications.

This report is therefore focused on determining the practical feasibility of using MPC to securely compute conjunction analyses. An MPC protocol that securely computes a conjunction analysis but requires a week's worth of computation time on modern computing hardware is of little value to the operational community. The feasibility of using MPC to compute conjunction analyses is primarily determined by the efficiency of the underlying MPC protocol.

Research Objective and Methodology

Currently, conjunction analysis calculations are never encrypted. They are performed "in the clear" by a trusted party. The research objective of this project was to determine how quickly modern MPC implementations could securely compute a conjunction analysis using present-day computing equipment. To address this task, we evaluated the efficiency of modern MPC algorithms. Efficiency depends on two factors: the complexity of the (unencrypted) conjunction analysis calculation and the efficiency of the general MPC protocol.

To determine the complexity of the conjunction analysis calculation, we reviewed the conjunction analysis literature to find a description of the algorithms in use today. We then dissected this algorithm, carefully counting the exact number of additions and multiplications needed to calculate a conjunction analysis to any specified degree of precision. To determine the efficiency of MPC protocols, we reviewed the cryptographic literature to find the benchmarks of efficiency for the most recent implementations of MPC protocols. Converting these benchmarks to "per-gate" measurements,[3] we arrived at

---

[2] Andrew C. Yao, "How to Generate and Exchange Secrets," *27th Annual Symposium on Foundations of Computer Science (FOCS 1986),* Toronto, October 27–29, 1986, pp. 162–167; Oded Goldreich, Sylvio Micali, and Avi Wigderson, "How to Play ANY Mental Game," *STOC 1987: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, New York: ACM, January 1987, pp. 218–229; Oded Goldreich, *Foundations of Cryptography,* Volume II, Cambridge University Press, 2004;

[3] In digital computing, every function is represented as a binary circuit, which means that functions are broken down into a series of AND and OR gates in order to be processed by the central processing unit. Similarly, functions may be rewritten as a series of ADD and MULT gates. A circuit composed of ADD and MULT gates is called an arithmetic circuit. The time required to perform a single gate operation—

an estimate of how many milliseconds are required to perform a single addition or multiplication securely using each of the different protocols. Combining these results, we argue that securely computing conjunction analyses is a practical possibility using current algorithms and hardware.

Findings

Our research found that several MPC protocols have been developed, and many of these protocols have been implemented in software to test their efficiency. Using available benchmarks from previous MPC implementations, our estimates indicate that a number of different MPC implementations exist that could securely compute a single conjunction analysis using commercial off-the-shelf hardware in under an hour. To securely compute all conjunction analyses of interest would require computing conjunction analyses in less than ten seconds, something that is easily achieved in the insecure setting.[4] Given the rapid progress of computing hardware and the improved ease of building parallel computing systems, our findings suggest that using MPC to compute conjunction analyses is certainly possible in the coming years.[5]

Implementing Secure Multiparty Computation Protocols

As noted above, MPC eliminates the need to employ a trusted third party to perform the calculations, but a minimal amount of computer and network infrastructure is needed to enable the use of an MPC protocol. In practice, this means that each participant must have a trusted computer on which to run his or her portion of the protocol, as well as communication links between participants.

The protocol itself consists of a series of messages exchanged between the participants, at the end of which each participant learns the output of the protocol. The protocol is public, allowing each participant to independently verify that the software running on his or her own machine is valid. The MPC protocol specifies the messages that each participant must send during the execution of the protocol.

Malicious participants may be tempted to deviate from the protocol, sending malformed messages in an attempt to glean extra information about other participant's inputs. To prevent such cheating, cryptographic techniques (e.g., cut-and-choose and

---

multiplied by the number of gates needed to compute the entire function—provides a general method for estimating how long it takes to calculate any function.

[4] Hall, Robert, Salvatore Alfano, and Alan Ocampo. "Advances in Satellite Conjunction Analysis," *Proceedings of the Advanced Maui Optical and Space Surveillance Technologies Conference*, 2010

[5] It is also worth noting that our efficiency estimates are obtained by extrapolating from prior cryptographic implementations. Therefore, any MPC implementation tailored specifically for the conjunction analysis calculation would almost certainly be significantly more efficient than the algorithms we used in this analysis.

zero-knowledge proofs) exist that allow users to prove to the other participants that they are following the protocol, without revealing anything that would compromise the secrecy of their inputs.

Since each user needs only a computer (trusted by him or herself alone) and a connection to other users, MPC protocols can easily be implemented over the Internet. To calculate complex functions, the number of messages exchanged between participants can be quite large, requiring thousands of times more communication than computing the function insecurely. When the protocol requires that a large number of messages be exchanged, the data transfer speed between participants can be the performance bottleneck. When this is the case, faster, more direct data links between the participants may be necessary. A series of performance tests showed that moving from a wide area network (WAN) to local area network (LAN) yielded speedups in the range of 17–64 percent.[6]

Implications for Space Situational Awareness

Our analyses indicate that the current MPC technology is sufficiently advanced to perform secure conjunction analysis calculations quickly enough to be of use to the SSA community.

Moving forward, the next step would be to create a software prototype implementing a secure conjunction analysis calculation. Such a prototype would have a two-fold benefit. First, it would provide the most accurate running-time estimates for a real-world conjunction analysis calculation. Second, it would serve as a concrete demonstration to operators that MPC is a potentially viable means of computing conjunction analyses. Both of these effects would help the space community assess the benefits of MPC as they plan future SSA data architectures.

No matter what the efficiency or security provided by cryptographic tools, these protocols will not provide any benefit if they are not accepted by the user community. As a starting point, those operators who have already entered into data-sharing agreements are natural candidates to be the first adopters of any cryptographic secure conjunction analysis tools that might be developed based on the software prototypes.[7]

The fact that these data-sharing partnerships exist indicates a strong demand by the satellite community for high-fidelity conjunction analysis calculations on private data. The cryptographic tools discussed here have the potential to allow operators to compute high-fidelity conjunction analysis without the need for mutual trust.

---

[6] Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, Tal Malkin, and Dan Rubenstein, *Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces*, IACR Cryptology ePrint Archive, Report 2011/257, 2011.

[7] For example, the operators who are part of Analytical Graphics, Inc.'s space data center, or USSTRATCOM's SSA sharing partners.