



MICROCOPY RESOLUTION TEST CHART NATIONAL BUREAU OF STANDARDS 1903 A

u ti TO. AD-A143 424 C 1  $\mathbf{O}$ DTIC JUL 27 84 DTC FILE E 84 07 20 004

Image: Approximate and a section of the sectin of the section of the section of the section of the section of	T'S CATALOG NUMBER
MIT/LCS/TR-315 TITLE (and Submite) Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement AuthoR(a) Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement AuthoR(a) PERFORMING ORGANIZATION NAME AND ADDRESS MIT Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139 CONTROLING OFFICE NAME AND ADDRESS DARPA/DOD 1400 Wilson Boulevard Arlington, VA 22209 To MONITORING AGENCY NAME & ADDRESS(I) MIT/Department of the Navy Information Systems Program Arlington, VA 22217 CONTRIBUTION STATEMENT (of the Report) Approved for public release, distribution is unli 7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report) Unlimited Supplement and reverse side If necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. Abinary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be Produce America agreement algorithm can be Produce America agreement algorithm can be Produce America	
Aution True (and Schemation)       First (and Schemation)         Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement       Inter First (and Schemation)         Extending Binary Byzantine Agreement       Inter First (and Schemation)         AuthoR(a)       Brian A Coan         Russell Turpin & Brian A Coan       DARPA N00001         PERFORMING ORGANIZATION NAME AND ADDRESS       DARPA N00001         DEFERFORMING ORGANIZATION NAME AND ADDRESS       IO. PROCE MIT Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139         1. CONTROLLING OFFICE NAME AND ADDRESS DARPA/DOD       II. REPOR April 1400 Wilson Boulevard Arlington, VA 22209       II. REPOR 7         I MONIFORMA GAENCY NAME & ADDRESS(II different from Controlling Office)       II. SECURI 000000000000000000000000000000000000	
Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement Author() Author() Author() Author() PERFORMING ORGANIZATION NAME AND ADDRESS MIT Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139 1 Controlling office NAME AND ADDRESS DARPA/DOD 1400 Wilson Boulevard Arlington, VA 22209 13. NUMBER Arlington, VA 22209 14. REPOR MITORME AGENCY NAME AND ADDRESS DARPA/DOD 15. SECURI ONR/Department of the Navy Information Systems Program Arlington, VA 22217 15. OSTAIBUTION STATEMENT (of the abstract misred in Block 20, if different from Report) Unlimited 2. SUPPLEMENTARY NOTES A DESTRACT (Continue on reverse side If necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. A Distribution and reverse side If necessary and identify by block number) Byzantine generals, Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce domain is significant.	REPORT & PERIOD COVERED
Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement       Inter Inter Inter Inter Inter Pression         Multivalued Byzantine Agreement       Inter In	im Bogonrah
Multivalued Byzantine Agreement  Author(a)  Author(a)  Performing organization name and adoress  Mit Laboratory for Computer Science S45 Technology Square Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Mit Laboratory for Computer Science Cambridge, MA 02139  Controlung office name and adoress  Arigon, VA 22209  7  14. Secure NUncla  Arigon, VA 22217  55. Secure Controlung office of the Navy Information Systems Program Arington, VA 22217  Approved for public release, distribution is unli  7. Distribution statement (of the abstract entered in Block 20, 11 different from Report)  Unlimited  Supplementary notes  Abinary Byzantine agreement, fault to distributed systems.  Abinary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b prod	Im Research
MIT/1 AuthoR(s) Russell Turpin & Brian A Coan DARPA MIT Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139 1 CONTROLING OFFICE NAME AND ADDRESS MIT Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139 1 CONTROLING OFFICE NAME AND ADDRESS DARPA/DOD 1400 Wilson Boulevard Arlington, VA 22209 15. SECURI ONR/Department of the Navy Information Systems Program Arlington, VA 22217 15. SECURI ONSTRIBUTION STATEMENT (of the Report) Approved for public release, distribution is unli 7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, 11 different from Report) Unlimited 8. SUPPLEMENTARY NOTES 9. KEY WORDS (Continue on reverse side 11 necessary and Identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. 9. ABSTRACT (Continue on reverse side 11 necessary and Identify by block number) A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	ING ORG. REPORT NUMBER
AUTHOR(c)       E. CONTRA         Russell Turpin & Brian A Coan       DARPF N0001         C. PERFORMING ORGANIZATION NAME AND ADDRESS       D. PROFINATION NAME AND ADDRESS         MIT Laboratory for Computer Science       545 Technology Square         Cambridge, MA 02139       12. REPOR         1. CONTROLLING OFFICE NAME AND ADDRESS       12. REPOR         DARPA/DOD       April         1400 Wilson Boulevard       7.         Arlington, VA 22209       7.         14 WONTORIK AGECKY NAME 4 ADDRESS(// different from Controlling Office)       15. SECURI         ONR/Department of the Navy       Information Systems Program       15. SECURI         Arlington, VA 22217       15. SECURI       Uncla         4. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)       3. NUMBER         Approved for public release, distribution is unli       15. SECURI         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)       10.         Unlimited       8. SUPPLEMENTARY NOTES       14.         8. KEY WORDS (Continue on reverse side if necessary and identify by block number)       15.         Byzantine generals, Byzantine agreement, fault to distributed systems.       14.         0. ABSTRACT (Continue on reverse side if necessary and identify by block number)       15.     <	CS/TR-315
Russell Turpin & Brian A Coan       DARPA N0001         Dependentiation of a control of the control of control of control of the control of the control of control of control of the control of	T OR GRANT NUMBER(.)
NO001       N0001         PERFORMING ORGANIZATION NAME AND ADDRESS       10. PROOF         MIT Laboratory for Computer Science       545 Technology Square         Cambridge, MA 02139       12. REPOR         1. CONTROLLING OFFICE NAME AND ADDRESS       12. REPOR         DARPA/DOD       April         1400 Wilson Boulevard       April         Arlington, VA 22209       7         1400 Wilson Boulevard       15. SECURI         ONR/Department of the Navy       Information Systems Program         Arlington, VA 22217       15. SECURI         ONSTRIBUTION STATEMENT (of the Report)       15. SECURI         Approved for public release, distribution is unli       16. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)         Unlimited       5. SUPPLEMENTARY NOTES         5. KEY WORDS (Continue on reverse side If necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         0       ABSTRACT (Continue on reverse side If necessary and identify by block number)         ABSTRACT (Continue on reverse side If necessary and identify by block number)         Abinary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm pre algorithms when the cost of transmittin	/DOD .
D. PERFORMING ORGANIZATION NAME AND ADDRESS II. CONTROLING OFFICIENT OF COMPUTER SCIENCE 545 TECHNOLOGY Square Cambridge, MA 02139 I. CONTROLLING OFFICE NAME AND ADDRESS DARPA/DOD 14 CONTROLLING OFFICE NAME AND ADDRESS DARPA/DOD 15. REFORMATION OF ADDRESS DARPA/DOD 14. NONLING OFFICE NAME AND ADDRESS DARPA/DOD 15. REFORMATION OF ADDRESS 16. MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office) 17. MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office) 18. SUPPLEMENT OF THE ADDRESS (II different from Report) ONR/DEPARTMENT (of the abstract entered in Block 30, If different from Report) Unlimited 8. KEY WORDS (Continue on reverse side if necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. ABSTRACT (Continue on reverse side If necessary and identify by block number) A ABSTRACT (Continue on reverse side If necessary and identify by block number) A ADDRESS (Continue on reverse side If necessary and identify by block number) A ADDRESS (Continue on reverse side If necessary and identify by block number) A ADDRESS (Continue on reverse side If necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. A ADDRESS (Continue on reverse side If necessary and identify by block number) A ADDRESS (Continue on reverse side If necessary and identify by block number) ADDRESS (Continue on reverse side If necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. A ADDRESS (Continue on reverse side If necessary and identify by block number) A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm realgorithm of the produce and the cost of transmitting values f valued domain is signif	4-82-K-0154
MIT Laboratory for Computer Science         S45 Technology Square         Cambridge, MA 02139         1. CONTROLLING OFFICE NAME AND ADDRESS         DARPA/DOD         1400 Wilson Boulevard         Arlington, VA 22209         7         1400 Wilson Boulevard         Arlington, VA 22209         7         14 WohitoRike AGENCY NAME & ADDRESS/II different from Controlling Office)         15. SECURE         ONR/Department of the Navy         Information Systems Program         Arlington, VA 22217         6. DISTRIBUTION STATEMENT (of the Report)         Approved for public release, distribution is unli         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)         Unlimited         8. SUPPLEMENTARY NOTES         9. KEY WORDS (Continue on reverse alds If necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         0. ABSTRACT (Continue on reverse alds If necessary and identify by block number)         A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm pre algorithms when the cost of transmitt	MELEMENT DROIECT TASK
Mill Laboratory Square         Cambridge, MA 02139         1. CONTROLLING OFFICE NAME AND ADDRESS         DARPA/DOD         1400 Wilson Boulevard         Arlington, VA 22209         17 MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office)         0000 Wilson Boulevard         Arlington, VA 22209         17 MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office)         00000 Wilson Boulevard         Arlington, VA 22209         18 SECURI         ONR/Department of the Navy         Information Systems Program         Arlington, VA 22217         19 OFFIGUTION STATEMENT (of the Report)         Approved for public release, distribution is unli         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)         Unlimited         8. SUPPLEMENTARY NOTES         9. KEY WORDS (Continue on reverse side If necessary and Identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         0         0         ABSTRACT (Continue on reverse side If necessary and identify by block number)         A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significa	WORK UNIT NUMBERS
Cambridge, MA 02139         1. CONTROLLING OFFICE NAME AND ADDRESS         DARPA/DOD         1400 Wilson Boulevard         Arlington, VA 22209         7         MONN/DEPArtment of the Navy         Information Systems Program         Arlington, VA 22217         Is. DECL.         ONR/Department of the Navy         Information Systems Program         Arlington, VA 22217         Is. DECL.         Schett         6. DISTRIBUTION STATEMENT (of the Report)         Approved for public release, distribution is unli         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)         Unlimited         • SUPPLEMENTARY NOTES         P KEY WORDS (Continue on reverse side if necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         • ABSTRACT (Continue on reverse side If necessary and identify by block number)         A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	
Controlling office NAME AND ADDRESS       12. REPOR         DARPA/DOD       April         1400 Wilson Boulevard       7         Arlington, VA 22209       7         If MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office)       15. SECURI         ONR/Department of the Navy       11. MUMBE         ONR/Department of the Navy       11. SECURI         ONR/Department of the Report       11. SECURI         Approved for public release, distribution is unli       11. SECURI         * DISTRIBUTION STATEMENT (of the abstract entered in Black 20, If different from Report)         Unlimited       .         * SUPPLEMENTARY NOTES       .         * ABSTRACT (Continue on reverse side If necessary and Identify by black number)         A binary Byzantine agreement algorithm can b	
DARPA/DOD       April         1400 Wilson Boulevard       7         Arlington, VA 22209       7         'M WONTORING AGENCY NAME & ADDRESS/! different from Controlling Office)       15. SECURI         ONR/Department of the Navy       Information Systems Program         Arlington, VA 22217       'S. SECURI         ONR/Department of the Navy       Uncla         Arlington, VA 22217       'S. SECURI         6. DISTRIBUTION STATEMENT (of this Report)       Approved for public release, distribution is unli         7. DISTRIBUTION STATEMENT (of the obstract entered in Bleck 20, If different from Report)         Unlimited         8. KEY WORDS (Continue on reverse side If necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         9. ABSTRACT (Continue on reverse side If necessary and identify by block number)         A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	DATE
1400 Wilson Boulevard       13. NUMBE         Arlington, VA 22209       7         13. MONTORING AGENCY HAME & ADDRESS(II dilferent from Controlling Office)       15. SECURI         0NR/Department of the Navy       11. Information Systems Program         Arlington, VA 22217       15. SECURI         0NR/Department of the Navy       11. Information Systems Program         Arlington, VA 22217       15. SECURI         6. DISTRIBUTION STATEMENT (of the Report)       15. SECURI         7. DISTRIBUTION STATEMENT (of the obstract entered in Block 20, If different from Report)         Unlimited         6. SUPPLEMENTARY NOTES         9. KEY WORDS (Continue on reverse side If necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to distributed systems.         0       ABSTRACT (Continue on reverse side If necessary and identify by block number)         A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values fi valued domain is significant.	1984
Arlington, VA 22209       7         IN MONITORING AGENCY NAME & ADDRESS(II different from Controlling Office)       15. SECURE         ONR/Department of the Navy       Uncla         Information Systems Program       15. SECURE         Arlington, VA 22217       15. SECURE         6. DISTRIBUTION STATEMENT (of the Report)       15. SECURE         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)       17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)         7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)       17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report)         9. KEY WORDS (Continue on reverse elde If necessary and Identify by block number)       18. SUPPLEMENTARY NOTES         9. KEY WORDS (Continue on reverse elde If necessary and Identify by block number)       19. Supplementary notes         9. KEY WORDS (Continue on reverse elde If necessary and Identify by block number)       19. Abstract (Continue on reverse elde If necessary and Identify by block number)         0. ABSTRACT (Continue on reverse elde If necessary and Identify by block number)       19. A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values for valued domain is significant.	OF PAGES
<ul> <li>MONITORING AGENCY NAME &amp; ADDRESS(II different from Controlling Office)</li> <li>IS. SECURE</li> <li>ONR/Department of the Navy</li> <li>Information Systems Program</li> <li>Arlington, VA 22217</li> <li>IS. DECLY</li> <li>OISTRIBUTION STATEMENT (of the Report)</li> <li>Approved for public release, distribution is unli</li> <li>DISTRIBUTION STATEMENT (of the abstract entered in Black 20, II different from Report)</li> <li>Unlimited</li> <li>SUPPLEMENTARY NOTES</li> <li>ABSTRACT (Continue on reverse side II necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm can b produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.</li> </ul>	
ONR/Department of the Navy Information Systems Program Arlington, VA 22217 6. DISTRIBUTION STATEMENT (of this Report) Approved for public release, distribution is unli 7. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, 11 different from Report) Unlimited 9. KEY WORDS (Continue on reverse side 11 necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. 9. ABSTRACT (Continue on reverse side 11 necessary and identify by block number) A binary Byzantine agreement algorithm can be produce a multivalued Byzantine Byza	Y CLASS. (of this report)
Information Systems Program Arlington, VA 22217 <sup>15e.</sup> DECL. SCHEE Approved for public release, distribution is unli 7. DISTRIBUTION STATEMENT (of the obstract entered in Block 20, 11 different from Report) Unlimited 9. KEY WORDS (Continue on reverse side if necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. 9. ABSTRACT (Continue on reverse side if necessary and identify by block number) Abinary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorithm can be produce a multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values for valued domain is significant.	
Arlington, VA 22217 Scher Scher Scher Scher Approved for public release, distribution is unli Approved for public release, distribution is unli T. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, If different from Report) Unlimited S. SUPPLEMENTARY NOTES Ster WORDS (Continue on reverse side if necessary and identify by block number) Byzantine generals, Byzantine agreement, fault to distributed systems. Abinary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorit Sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values for valued domain is significant.	ssified
<ul> <li>Approved for public release, distribution is unli</li> <li>Approved for public release, distribution is unli</li> <li>DISTRIBUTION STATEMENT (of the abstract entered in Block 20, 11 different from Report)</li> <li>Unlimited</li> <li>SUPPLEMENTARY NOTES</li> <li>KEY WORDS (Continue on reverse side II necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>ABSTRACT (Continue on reverse side II necessary and identify by block number)</li> <li>A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm systems when the cost of transmitting values f valued domain is significant.</li> </ul>	SSIFICATION/DOWNGRADING
<ul> <li>SUPPLEMENTARY NOTES</li> <li>KEY WORDS (Continue on reverse side if necessary and identify by block number)         Byzantine generals, Byzantine agreement, fault to         distributed systems.         ABSTRACT (Continue on reverse side if necessary and identify by block number)         A binary Byzantine agreement algorithm can b         produce a multivalued Byzantine agreement algorit         sulting multivalued algorithm is cheaper than pre         algorithms when the cost of transmitting values f         valued domain is significant.     </li> </ul>	
<ul> <li>SUPPLEMENTARY NOTES</li> <li>KEY WORDS (Continue on reverse side if necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>ABSTRACT (Continue on reverse side if necessary and identify by block number)         <ul> <li>A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorithm swhen the cost of transmitting values f valued domain is significant.</li> <li>Supplement algorithm</li> </ul> </li> </ul>	
<ul> <li>KEY WORDS (Continue on reverse side if necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>ABSTRACT (Continue on reverse side if necessary and identify by block number)         <ul> <li>A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorith sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.</li> </ul> </li> </ul>	
<ul> <li>9. KEY WORDS (Continue on reverse side if necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>ABSTRACT (Continue on reverse side if necessary and identify by block number)</li> <li>A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.</li> </ul>	
<ul> <li>KEY WORDS (Continue on reverse side if necessary and identify by block number)</li> <li>Byzantine generals, Byzantine agreement, fault to distributed systems.</li> <li>ABSTRACT (Continue on reverse side if necessary and identify by block number)</li> <li>A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than prealgorithms when the cost of transmitting values for valued domain is significant.</li> </ul>	
Byzantine generals, Byzantine agreement, fault to distributed systems. ABSTRACT (Continue on reverse side II necessary and identify by block number) A binary Byzantine agreement algorithm can be produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre- algorithms when the cost of transmitting values for valued domain is significant.	
distributed systems. • ADSTRACT (Continue on reverse elde II necessary and identify by block number) A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	lerance in
ABSTRACT (Continue on reverse elde II necessary and identify by block number) A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	
ABSTRACT (Continue on reverse elde II necessary and identify by block number) A binary Byzantine agreement algorithm can k produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	
A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	
A binary Byzantine agreement algorithm can b produce a multivalued Byzantine agreement algorit sulting multivalued algorithm is cheaper than pre algorithms when the cost of transmitting values f valued domain is significant.	
algorithms when the cost of transmitting values f valued domain is significant.	
	e extended to hm. The re- viously published
PORM 1472 FOISION OF LINE CONTRACTOR	e extended to hm. The re- viously published rom the multi-

# Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement

Russell Turpin<sup>1</sup> Information Research Associates 911 West 29<sup>th</sup> Street Austin, TX 78705

Brian A. Coan<sup>2</sup> MIT Laboratory for Computer Science Cambridge, MA 02139

April 1984

NTIS GRA&I DTIC TAB Unannounced Justification By Distribution/ Availability Codes Avail and/or Dist Special A-/	Acce	ssion For				
DTIC TAB	NTIS	GRA&I				
Unannounced Justification By Distribution/ Availability Codes Avail and/or Dist Special A-/	DTIC	TAB				
Justification By Distribution/ Availability Codes Avail and/or Dist Special A-/	Unan	Unannounced				
By Distribution/ Availability Codes Avail and/or Dist Special A-/	Just	Justification				
By Distribution/ Availability Codes Avail and/or Dist Special A-/						
Distribution/ Availability Codes Avail and/or Dist Special	By					
Availability Codes Avail and/or Dist Special	Dist	ribution/				
Avail and/or Dist Special	Ava	ilability Codes				
Dist Special		Avail and/or				
A-/	Dist	Special				
A-/						
<b>A</b> -/						
	A-/					

## Abstract

A binary Byzantine agreement algorithm can be extended to produce a multivalued Byzantine agreement algorithm. The resulting multivalued algorithm is cheaper than previously published algorithms when the cost of transmitting values from the multivalued domain is significant.

### Keywords

Byzantine generals, Byzantine agreement, fault tolerance in distributed systems.

© 1984 Massachusetts Institute of Technology, Cambridge, MA 02139

<sup>&</sup>lt;sup>1</sup> This author eschews government funding.

<sup>&</sup>lt;sup>2</sup> This author's work was supported in part by the Office of Naval Research under contract N00014-82-K-0154, the Office of Army Research under contract DAAG29-79-C-0155, and the NSF, under grants MCS-8118678, MCS-8302391, and MCS-8308854.

### Introduction

The concern of this paper is a set of potentially faulty processes that engage in a distributed computation to agree on some piece of information. Each process enters the computation with an initial value. The computation returns a common result value to each correct process. If all correct processes begin the computation with identical initial values, then the result value equals the initial value.

The computation can be briefly characterized as follows. The computation is fully distributed and symmetric. It includes several rounds of synchronous message exchange over a completely connected, totally reliable communications network. The correct processes communicate only through messages. The communications network correctly identifies the sender of each message to the recipient of the message. Processes are assumed to have no signature ability (authentication). That is, there is no immediate way of detecting whether or not a relayed message has been altered.

A process fails if it does not successfully perform the actions prescribed by the agreement algorithm. No assumptions are made restricting the messages sent by faulty processes. One can imagine that all faulty processes act maliciously, in collusion, and with magical knowledge of the state of the distributed system.

A computation that functions as described above solves the Byzantine generals problem without authentication [3]. (Authenticated protocols protect relayed messages from alteration.) Let P be the number of processes that engage in the agreement computation and let T be an upper bound on the number of processes that may fail during the agreement computation. Byzantine agreement without authentication requires P>3T [6], and cannot be achieved in fewer than T + 1 rounds [4].

A less general formulation of the problem assumes that a distinguished process transmits initial values to the other processes. This paper makes no assumption about the source of the processes's initial values.

This paper describes a method for extending a binary Byzantine agreement algorithm to reach agreement on values from an arbitrary domain V. Any binary algorithm that does not require a distinguished transmitter process may be used. Two rounds are prepended to the binary algorithm. In the first round, each process sends every other process its initial value. In the second round, each process broadcasts a single bit of information by sending or not sending null messages. The third and subsequent rounds follow the chosen binary algorithm.

Previous algorithms for reaching Byzantine agreement on values from an arbitrary domain V require processes to send messages whose length depends on the size of V in each round of the computation. Using the extension described in this paper, messages whose length depends on the size of V are sent only in the first round. Since the time that must be allotted each round of the computation depends in part on the length of messages sent in the round, the extension enables significant savings when the domain is large.

The prepended rounds are an integral part of the extended computation. In particular, agreement can be guaranteed only if no more than T processes fail during the computation, including the first two rounds, where P>3T. (The chosen binary algorithm may make additional assumptions.)

The body of this paper contains three sections: a description of the extension, a proof of its correctness, and a discussion of implementation concerns and performance characteristics.

#### **Description of the Extension**

In the first round, each process sends its initial value to every other process. A process is said to be *perplexed* if, in the first round, it receives at least as many as (P - T)/2 initial values different from its own. Processes that are not perplexed are said to be *content*. In the second round, each perplexed process sends a message to every other process. The semantics of this message is just "I am perplexed".

Each process maintains three local variables: two arrays indexed by process number and a boolean. These variables are are assigned values during the first two rounds. For process j, and  $i \neq j$ ,

these variables are defined as follows:

- v(j) The process's initial value.
- v(i) The initial value received from process i.
- p(j) A boolean that is set true if and only if process j is perplexed, that is,  $v(j) \neq v(i)$  for at least as many as (P T)/2 distinct values of i.
- p(i) A boolean that is set true if and only if process i sent a message claiming it is perplexed.
- alert A boolean that is set true if and only if at least as many as P 2T elements of p are true.

The binary computation is used to reach agreement on alert. If the binary computation agrees alert = true, there are correct processes with different initial values from V. In this case, all correct processes use a predefined default value from V as the result of the extended computation. If agreement is alert = false, then all correct content processes have the same initial value from V. This value is the result of the extended computation. Perplexed processes deduce this result by using the initial value that is common to a majority of the content processes. That is, each perplexed process tabulates as votes the values v(j) for which p(j) is false. The majority vote is for the value favored by the correct content processes.

#### **Proof of Correctness**

The extended computation is correct if (1) all correct processes obtain the same result value, and (2) the result value equals the common initial value whenever all correct processes begin with the same initial value.

The second claim is easily proved. If all correct processes have the same initial value from the domain V, then no correct process is perplexed and all correct processes have alert = false. The binary computation agrees alert = false and all correct processes, which are content, use their initial value as the result.

The first claim has two cases: the binary computation agrees alert = true or alert = false. In the

former case, all correct processes select the default value as the result of the extended computation. In the latter case, it is necessary to show that all content processes have the same initial value and that this value is deduced by all the perplexed processes. This will now be demonstrated.

Any subset of more than (P + T)/2 processes contains a majority of the correct processes. From this basic fact, it follows that each content process has the same initial value as a majority of the correct processes. (Observe that (P + T)/2 and (P - T)/2 sum to P.) Since there cannot be two distinct majorities, all content processes have the same initial value.

Since the result of the binary computation is alert = false, there are at least T + 1 correct content processes, for otherwise there would be at least P - 2T correct perplexed processes and all correct processes would be alert and the result of the binary computation would be alert = true. Each perplexed process has p(j) false for all content processes and possibly for some incorrect processes. Since there are at most T incorrect processes, the content processes are a majority of those for which p(j) is false. Taking a majority vote of the v(j) for which p(j) is false produces the value shared by the content processes.

#### Implementation and Performance Analysis

Many binary algorithms favor one of the two values in the binary domain. The binary algorithms (without authentication) described in [1,2,3,5] all reach agreement for the favored value whenever more than T correct processes begin with that value. (Assume that the threshold LOW equals T + 1 in [1,2,5].)

In the extended algorithm, the second round together with the binary computation can be interpreted as reaching binary agreement on which processes are perplexed, providing agreement is reached for perplexed whenever (P - T)/2 or more correct processes are initially perplexed. If the chosen binary algorithm exhibits the bias described above, the second round of the extended algorithm can be omitted. (The chosen binary algorithm must require that each process sends all other processes initial binary values so that the values in the array p can be set.)

A good multivalued Byzantine agreement algorithm is presented in [5]. Agreement is reached in 2T + 4 rounds and requires  $O(P^3)$  messages each comprising  $O(\log P \log |V|)$  bits. The extension described in this paper using the algorithm in [5] to reach binary agreement reaches multivalued agreement in 2T + 5 rounds (the second round of the extension is not needed) and requires  $O(P^3)$ messages having  $O(\log P)$  bits and  $O(P^2)$  messages having  $O(\log |V|)$  bits. The latter messages are sent only in the first round.

The above analysis shows that the extension of the binary algorithm in [5] yields a multivalued algorithm that is cheaper in message bits than the multivalued algorithm described in [5]. The extension enables this savings because only in the first round does it send messages whose length depends on the size of the value domain. The actual time savings possible depends on a variety of factors, including the cost of an additional communication round relative to the cost of sending large messages, the size of the value domain, and the bandwidth of the communications network.

#### Conclusion

This paper shows that reaching Byzantine agreement on values from an arbitrary domain is not essentially more difficult than reaching binary Byzantine agreement, except for the necessity of initially exchanging and comparing values. Using the technique described in this paper to extend a good binary algorithm yields a multivalued algorithm faster than those previously published when agreement must be reached on large sets of data.

#### Acknowledgments

Mani Chandy, while teaching a distributed algorithms class, first posed the Byzantine generals problem to Russell Turpin, who also thanks Jay Misra and Doug Neuse for their criticism and advice, and J. C. Browne and the employees of Information Research Associates for their support. Brian Coan thanks Nancy Lynch, Jennifer Lundelius, and Eugene Stark for helpful discussions and suggestions. Both authors are indebted to David Gries for editorial advice.

### References

[1] D. Dolev, M. Fischer, R. Fowler, N. Lynch, and H. R. Strong

An Efficient Byzantine Agreement without Authentication

IBM Research Report RJ3428, March 82,

Watson Research Center Distribution Services, PO Box 218, Yorktown Hts., NY 10598

[2] D. Dolev and H. R. Strong

#### **Polynomial Algorithms for Multiple Processor Agreement**

14<sup>th</sup> ACM Symp. on Theory of Computing (May 82) 401-407

[3] L. Lamport, R. Shostak, and M. Pease

#### The Byzantine Generals Problem

ACM Transactions on Programming Languages and Systems, 4 (3) (1982) 382-401

[4] N. Lynch and M. Fischer

A Lower Bound for the Time to Assure Interactive Consistency

Information Processing Letters, 14 (4) (1982) 183-186

[5] N. Lynch, M. Fischer, and R. Fowler

#### A Simple and Efficient Byzantine Generals Algorithm

2<sup>nd</sup> Symp. on Reliability in Distributed Software and Database Systems (1982) 46-52

[6] M. Pease, R. Shostak, and L. Lamport

**Reaching Agreement in the Presence of Faults** 

J. ACM 27 (2) (1980) 228-234

# OFFICIAL DISTRIBUTION LIST

# 1984

Director Information Processing Techniques Office Defense Advanced Research Projects Agency 1400 Wilson Boulevard Arlington, VA 22209	2	Co <u>p</u> ies
Office of Naval Research 800 North Quincy Street Arlington, VA 22217 Attn: Dr. R. Grafton, Code 433	2	Copies
Director, Code 2627 Naval Research Laboratory Washington, DC 20375	6	Copies
Defense Technical Information Center Cameron Station Alexandria, VA 22314	12	Copies
National Science Foundation Office of Computing Activities 1800 G. Street, N.W. Washington, DC 20550 Attn: Program Director	2	Copies
Dr. E.B. Royce, Code 38 Head, Research Department Naval Weapons Center China Lake, CA 93555	1	Сору
Dr. G. Hopper, USNR NAVDAC-OOH Department of the Navy Washington, DC 20374	1	Сору

