FINAL REPORT TEMPLATE

SECURING DISTRIBUTED SYSTEMS UNDER CONTESTED ENVIRONMENTS (SUBTITLE: INFORMATION DISSEMINATION ACROSS NETWORK DOMAINS)

Bharat Bhargava, Professor of CS, Computer Science Department,

Purdue University, West Lafayette, Indiana 47907

SECURING DISTRIBUTED SYSTEMS UNDER CONTESTED ENVIRONMENTS (SUBTITLE: INFORMATION DISSEMINATION ACROSS NETWORK DOMAINS)

Bharat Bhargava, Professor of CS, Computer Science Department,

Purdue University, West Lafayette, Indiana 47907

Abstract

Abstract text (***maximum one page***)

This research presents solutions to Integrity, Security, Reliability and Confidentiality/Privacy of data and communication in distributed systems. The solution helps in providing right data at the right time to meet the mission requirements of the user. We identified ideas to make distributed systems continue operations under contested environments under threat of attacks (single or multiple/collusive) on communications and sites. We explored both wired and wireless communication. The ideas for graceful degradation, adapting to type, extent, duration and timing of attack to deal with anti-access and area denial problem. The challenges in contested environments is subdivided into two sets of complementary terms; Anti-Access and Area Denial. We proposed research solution for accomplishing design and objectives of PACE (Primary, Alternate, Contingency, and Emergency). Adaptability research to provide continuity of operations due to multiple network partitions or site failures is presented. Using ideas of active bundle (data and access privileges/policies) we ensure that data can only be accessed by persons with correct security clearance. Block chain technologies are briefly investigated to develop decentralized highly efficient information dissemination while guaranteeing auditing and non-repudiation and techniques for sharing and archiving information across network domains via untrusted/insecure networks (internet) and devices.

SECURING DISTRIBUTED SYSTEMS UNDER CONTESTED ENVIRONMENTS (SUBTITLE: INFORMATION DISSEMINATION ACROSS NETWORK DOMAINS)

Bharat Bhargava, Professor of CS at Purdue University

INTRODUCTION

The challenges in contested environments can be subdivided into two sets of complementary terms; Anti-Access and Area Denial. Anti-access environment challenges access, complicates entry and makes force posturing very difficult. Area denial environment limits movement and maneuver of forces in military. Distributed systems to support Air and space power faces both challenges in contested environments.

- We explain how adversary attacks can affect systems to explore graceful degradation. Various attack types are considered. A combination or collusion of multiple attacks cause problems for consistency, integrity, privacy, communication failures, intermittent communication and connectivity, bandwidth limitation, network partitions, site failures in mobile, air vehicles environments. The solutions involve dealing with (a) All or Partial Interruptions, (b) Degradation, (c) Adaptation, (d) Response, We investigate cyber-attacks, network exploits, malware-based attacks exerted to disrupt, deny, and steal information or sometimes to take control of the friendly strategic cyber capabilities. Ideas to accomplish PACE objectives [5, 6] are developed.

This research will meet the objective of Agile and secure communications and networks, agnostic connectivity, autonomous link discovery, creation and utilization and privacy preserving dissemination of information securely to meet the mission of users. This plan is expressed in an order of communication precedence list called PACE plan [5]. It designates the order in which an element will move through available communications systems until contact can be established with the desired distant element [6].

DISCUSSION OF PROBLEM

The Ideas of weak consistency, read/write consistency, transaction consistency, data base correctness/integrity need investigation during attacks and failures in distributed databases system. Research on how these ideas can allow nonstop transaction processing during failures/attacks and how consistency can be eventually achieved is needed. The identification of malicious activities and congestion in both mobile and internet communication is a research problem. Another problems are to deal with site failures and network partitions. Preservation of privacy of data dissemination and sender/receiver needs solutions.

METHODOLOGY

2.1 Graceful Degradation: It is used to ensure that a system continues to operate and provide services to mission. This ideas has been used in hardware and software designs. It is illustrated in Figure 1. If the primary system or module fails to perform as expected by the acceptance test, it tries to execute a series of alternates or eventually weaken the acceptance test. Acceptance test can be the quality of service such as lower consistency, atomicity, or less details of output data. In video, it can be color versus black, low versus high resolution and changing frame rate. Degradation may involve ignoring or bypassing some parts of systems or make necessary decisions with incomplete data. The alternates can be older version or developed by another team to provide diversity. In case of communications, one can go from high speed network to mobile network or even a wired phone. Military used the PACE mechanism which is an acronym for Primary, Alternate, Contingency, and Emergency. It designates the order in which an element will move through available communications systems until contact can be established with the desired distant element [6].

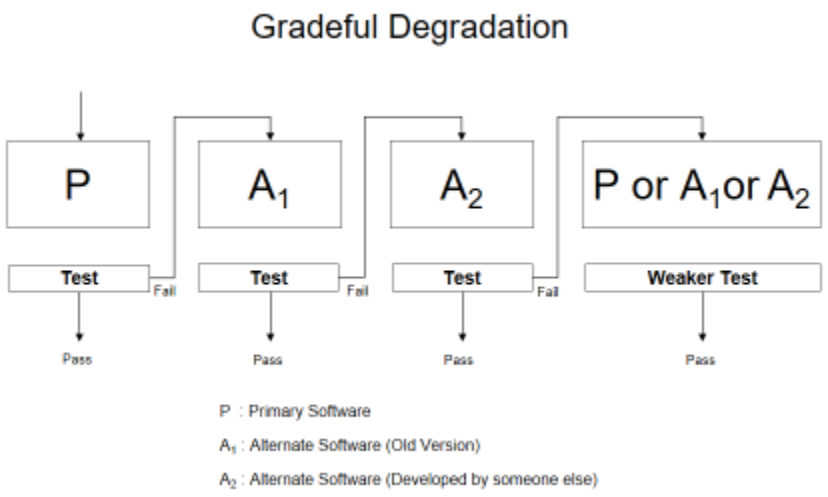

Figure 1

2.2 Consistency of Database: There are two types of correctness of database. One criterion is called transaction consistency that is based on serializable execution of correct transactions. The other type of correctness is based on database integrity assertions. Transaction consistency is based on the idea that a successful transaction takes the database from one consistent state to another consistent or correct state. But this requires a log of all transactions that have executed. If this log is available and a crash occurs in the middle of a transaction, the database that becomes inconsistent and can be rolled back by undoing transaction or going to a previous state based on a check point or some state after the execution of a few transactions in past. If the log is unavailable, we must try to find a state that satisfied a set of predefined integrity assertions and aim towards that database state is acceptable to users. These ideas are illustrated in the following figure 2.

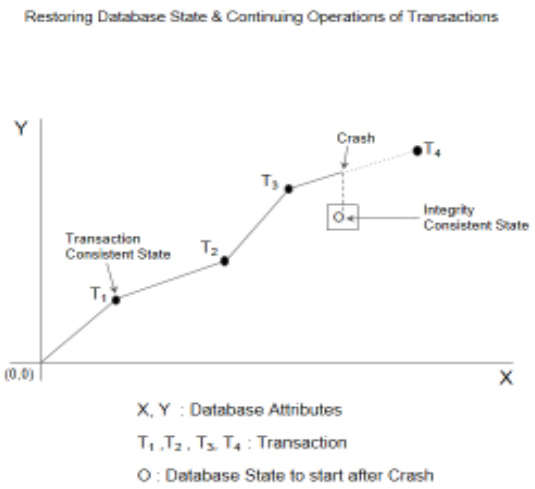

Figure 2

2.3 Consistency in distributed database systems: During network partitions and site failures, some copies of database cannot be updated. Maintaining the mutual consistency of replicated copies is not possible. For continuing nonstop transaction processing, we propose various types of weak consistencies [29]. One can say a copy is inconsistent for certain period of time or for a number of transactions. It may be possible to allow read–only transaction on inconsistent copies since they have an older version of a consistent database. The system must identify if copies have become inconsistent using the ideas of versions on data items or one can use the idea of fail locks [30]. A fail lock is set on an item that has been updated on an operational site while a copy on another sites was not possible. These fail lock are released after sites are connected back by either running a copier transaction (that copies a database from one site to other sites) or waiting for future incoming transactions to update the inconsistent copy. If this takes too long to make all copies fully consistent, the copier transaction can be issued. A series of experiments to determine how multiple failures cause inconsistency and the solutions to make mutually consistent database are presented in [30].

2.4 Site Failure and Network Partitions: If we use a consensus protocol for selecting which sites are operational, the problem is reducing to determining the majority. If further partitions occur, the idea of majority of majority can be used until the sites in the partition become too small. The other minority partitions cannot declare a majority even if they are connected. This can be enforced by using a version number on the sites. The higher number versions are considered to be most current. As an example, if there were 13 sites and they partition in two groups: one with 7 and the other with 6 sites. The group with 7 sites declares majority. If this further partitions into 4 and 3 sites, we declare group with 4 sites are majority of majority. Now even if the 3 sites and other 6 sites get connected to make a group of 9 sites, it can declare itself as majority and must wait to be connected with sites in group of 4 that is still operational. Now if group of 4 splits into 3 and 1, one can declare 3 as majority of majority or we could say 3 is too small to be operational and it must join some sites that were disconnected earlier. This gives rise to interesting in problems in merging of sites to declare majority once again.

To deal with site failure, we propose the idea of read one, write all or read all, write one. In such case after a single site failure, we can use the idea of read one and write all available (even if all available is one site in extreme case). To identify which sites have failed, we can use the idea of control transactions that announce a failure of a site when it cannot execute the update. The idea on incarnation numbers or

session numbers (or session vectors) can be used to identify which sites are up. This avoids sending updates to failed sites. The idea of session vector can also be used in network partitions to determine which sites are connected [31].

2.4 Attacks and Failures: We considered solutions to deal with site failures, network partitions and multiple failures. Various types of attacks on routing in wired networks that cause congestions and on route discovery in mobile ad hoc network are to be identified and mitigated. Collusive attacks on a distributed system must be considered.

Network environments are faced with myriad of security attacks, including worms and viruses, denial-of-service (DoS), spam and phishing attempts, route manipulations, and domain name system (DNS) exploitations. Wireless networks, especially mobile ad hoc networks (MANETs), in addition to the general network attacks, suffer from new classes of attacks such as denial-of-messages (DoM) where malicious nodes may prevent some honest ones from receiving broadcast messages, and replication attacks where adversaries insert hostile nodes into the network after obtaining secret information from captured nodes or via infiltration. In addition wormhole and black hole attacks along with collaboration among malicious nodes are major problems. Details are [21, 27]

In wired internet, we designed an integrated distributed monitoring, traffic conditioning, and flow control system for security of network domains. The edge routers monitor uses tomography techniques to detect quality of service (QoS) violations due to bandwidth theft attacks. To bound the monitoring overhead, a router only verifies service level agreement (SLA) parameters such as delay, loss, and throughput when anomalies are detected. The marking component of the edge router uses TCP flow characteristics to protect 'fragile' flows. Edge routers may also regulate unresponsive flows, and propagate congestion information to upstream domains. Simulation results show that these ideas can increase application-level throughput of FTP transfers; achieves low packet delays and response times for traffic; and detects bandwidth theft attacks and service violations. Details are in [23].

2.5 Detecting Malicious Collaborating Nodes: We developed a methodology for identifying multiple black hole nodes cooperating as a group with a slightly modified AODV protocol by introducing two key mechanisms: 1) Data Routing Information (DRI) Table and 2) Cross Checking. The process of cross checking the intermediate nodes is a onetime procedure which is affordable to secure a network from multiple black hole nodes. The cost of cross checking the nodes can be minimized by letting nodes share their trusted nodes list with each other. We have developed solution has two new key advantages: 1) Identification of multiple collaborative black hole nodes in a MANET; and 2) Discovery of secure paths from source to destination that avoid collaborative black hole nodes acting in cooperation. We use the bloom filter more effectively to achieve this. Details are in [28]

We have studied the impact of coordinated attacks on the existing routing protocols in MANETs, which provide insights on designing secure mechanisms. To defend against coordinated attacks, collaboration among the monitoring and detection agents of different mobile nodes is needed.

In ad hoc networks, malicious nodes can carry wormhole attacks to fabricate a false scenario on neighbor relations among mobile nodes. The attacks threaten the safety of ad hoc routing protocols and some security enhancements. We propose a classification of the attacks according to the format of the wormholes. It establishes a basis on which the detection capability of the approaches can be identified. The analysis shows that previous approaches focus on the prevention of wormholes between neighbors that trust each other. As a more generic approach, we present an end-to-end mechanism that can detect wormholes on a multi-hop route. Only trust between the source and the destination is assumed. The mechanism uses geographic information to detect anomalies in neighbor relations and node movements. To reduce the computation and storage overhead, we present a scheme, Cell-based Open

Tunnel Avoidance (COTA), to manage the information. COTA achieves a constant space for every node on the path and the computation overhead increases linearly to the number of detection packets. We prove that the savings do not deteriorate the detection capability. The schemes to control communication overhead are studied.

2.6 Collaborative attacks:

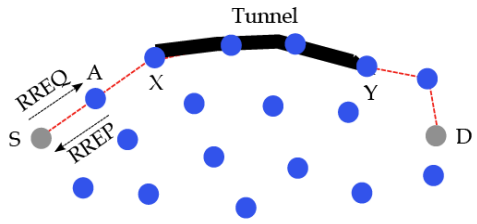

Figure 3. Combined attack: blackhole and wormhole attacks

In MANETs, a combination of attacks might become very successful. As an example, Figure 3 illustrates a situation in which two attacks take place simultaneously. Node A perpetrates a black hole attack and nodes X and Y collude to carry out a wormhole attack. If node A and X collaborate, then the data packets from node S will be forwarded through the tunnel, as shown in the Figure 1. Node A will receive a route request packet (RREQ) from node S and will reply with a route reply packet (RREP) stating maliciously that it has the shortest path to node D. Then node A will establish a route through node X which will build a tunnel to node Y, so the communication between the two end nodes (S and D) will be established through the path, including the tunnel.

With this setup, as node A does not drop packets, it will go undetected by various existing proposals for black hole attacks. Nodes X and Y will receive every packet of the connection and can tamper with their contents or simply selectively drop them. In this case, in order to be the selected path by the routing protocol, the tunnel does not need to be really attractive to the routing protocol. This is facilitated here by the malicious node A. The defense mechanism has to be smart enough to take tailored actions for each threat announced by the classification mechanism.

Collaborative attacks form a class of attacks where multiple malicious adversaries interleave and synchronize actions to accomplish disruption, deception, usurpation, or disclosure against some targeted organizations or network entities. Any robust defense mechanism must be able to deal with short-lived and long-lived attacks. These attacks make long-lived attacks more viable as most defense mechanisms are designed to defend against single attackers or multiple uncoordinated attackers. The potential damage associated with collaboration between attackers is much higher than attacks launched by a single attacker. In order to mitigate this potential damage, defense mechanisms of the future must incorporate accurate characterizations of these attacks. For example, many defense mechanisms are not designed to detect or prevent botnet attacks (which is a simple and special case of collaborative attacks) subsequently allowing these attacks to continue for long periods of time. Many other forms of coordinated attacks exist. For instance, in MANETs, various attacking machines could collude to incorrectly report routes or distance to destination. Unlike single and uncoordinated group attacks, coordinated attacks may cause more devastating impacts on the Internet or wireless environments as they combine efforts of more than one attacker. We have examined such attacks in REAct system [28]. In MANETs, identification of

malicious activity is hard when one node misbehaves in route formation. If multiple nodes act maliciously, simultaneously, or alternately, the schemes to deal with them will become very slow at most nodes. It is further possible that multiple attacks may interfere with each other and use resources needed by other attackers. Collaborative attacks offer the possibility of earlier detection due to multiple suspicions and additional communication among them. The defense mechanisms should identify the presence of an attack whether it is independent or collaborative and try to create actions that will interfere with the actions of attacks and their collaboration.

An important piece missing from the current research is an understanding of the impact of multiple attacks when they run concurrently. Coordinated attacks can cause havoc for the computer networks and are hard to anticipate, avoid, detect, and defeat. The problem is exacerbated if the multiple attackers can coordinate and gain the knowledge from each other. Such attacks may overlap and run concurrently, follow one after the other, attack during recovery, and corrupt a large part of a network. The damage could be geographically distributed or be concentrated on a small part of critical cyber operations.

The coordination and/or the collaboration among various attackers need to be examined. For collaboration and potential cooperation among any attackers there has to be some degree of awareness and intent in advance. There may also be implied collaboration. We can consider coordination to take place in advance of launch of attack while collaboration is during the execution of the attack. Usually this can be done through message exchanges identifying and communicating what has been accomplished and what are the next steps for the success of the attack. Attacks in Internet are sophisticated and an individual attacker, even having taken over many machines, may not be able to launch complex and powerful attacks without any coordination or collaboration in various stages. But, with employing the simplest form of collaboration among attackers, a severe DDoS attack can be conducted.

We propose to address issues of identifying, characterizing, and modeling collaborative attacks and defending against them. There is no requirement on the attack actions of the attacker as long as each attacker executes at least one attack action. This definition encompasses many forms of attack. These attacks can be classified broadly as *no-knowledge*, *semi-knowledge*, and *full-knowledge* attacks. In a no-knowledge attack, each attacker has no knowledge of any other attacker and therefore does not intentionally share information with any other attacker. An attacker in a no-knowledge collaboration is interested solely in her own gain. In a semi-knowledge attack, attackers may have knowledge of some attackers but not all. Subsequently, attackers may or may not be interested in the gain of other attackers. In a full-knowledge attack, attackers share information before or while attacking the target. At least one attacker is aware (or can become aware) of all other attackers. Attackers take actions for the “good” of the whole group of attackers. In this proposal, we are only mildly interested in no-knowledge attacks. We are far more concerned with semi-knowledge and full-knowledge attacks. In these latter forms of attacks, more sophisticated techniques can be used to violate a network’s security policy. For instance, for threshold-based based detection methods, semi-knowledge or full-knowledge attack may be used to identify where the threshold may be for the enforcement mechanism. Determining this threshold would involve attackers effectively sacrificing themselves for the greater “good” of the other attackers. Once the threshold has been identified, other attackers will able to cause potential harm to the target network without being detected. Because such sophisticated coordination is only possible in a semi-knowledge or full-knowledge attack, these forms of attacks are of primary interest in this proposal. Throughout this proposal, when referring to collaborative attacks, we use the word collaboration and coordination interchangeably.

2.7 Coordinated Defense: Attackers would like to launch the attacks while cloaking themselves. They do not want to leave evidences on their attacks and minimize the possibility that their activities are detected. In the collaborative attacks and defenses, for example, defense system can trace all attackers by starting from discovery and focus on one attacker. The attackers would like to maximize safety of themselves and would like to devise sophisticated communication schemes to avoid such tracing. For instance, in single attacks attackers can employ dynamic IP addresses, launch the attacks, and go offline to avoid detection. However, in coordinated attacks, if the attackers communicate extensively and use similar IP addresses (e.g. IP addresses within the same sub network), then they are more likely to be identified. Attackers can use better strategies: A simple improvement would be launching the attacks from different sub networks, thus giving them better cloaking. On the defense side, the defenders would be happy to see that attackers leave more information so that the defenders can discover, locate and repair the damage caused and develop better defending techniques. Adversaries have collaboration together to conduct more complex and subtle attacks to prevent detection or identification. To address these attacks, we will employ advanced machine learning and signal processing techniques.

2.8 Coordinated Defense using Bio-Inspired Ideas: This is an idea that we like to explore in future research. Human immune network is an advanced natural cooperative defense system against collaborative attacks from viruses, bacteria and cancer. Both RNA-containing and DNA-containing viruses, two obviously different classes of virus, can cause cancer, and so bacteria with the viruses and cancer can cause the overload and damages of the immune system. Thus, the biological immune network inspires us to design more advanced defense system against such advanced attacks. In general, the human immune network has a large number of immune cells (e.g. B cells and T cells) and immune molecules (e.g. antibodies). In many cooperative immune responses, the immune cells and immune molecules make up the parallel immune tier, which realize immune responses in parallel cells and molecules. At first, the immune network against the attacks determines whether the strange objects are selfs and detect the attacks. The selfs of the biological immune systems are normal cells (including immune cells) and normal molecules such as antibodies. If they are selfs, the objects are not relative with the attacks; otherwise, the objects are the non-selfs that cause the attacks. The non-selfs are foreign or the damaged selfs. Detecting the selfs and the attacks is the first mission of the native immune tier, and recognizing and classifying the known attacks are the other responsibilities of the tier. To recognize the unknown attacks, immune learning and memory are required for the adaptive immune tier of immune network. According to the bio-inspired ideas, a novel cooperative immune model against the collaborative attacks, such as blackhole attacks and wormhole attacks in MANET environments has been studied to detect the attacks and minimize the attacks.

2.9 Privacy preservation: Privacy preservation in a peer-to-peer system tries to hide the association between the identity of a participants and the data that is being communicated. We have developed a trust-based privacy preservation method for peer-to-peer data sharing. It adopts the trust relation between a peer and its collaborators (buddies). The buddy works as a proxy to send the request and acquire the data. This provides a shield under which the identity of the requester and the accessed data cannot be linked. A privacy measuring method is developed to evaluate the proposed mechanism. Dynamic trust assessment and the enhancement to supplier's privacy are achieved [21]. A mechanism is proposed that allows the peers to acquire data through trusted proxies to preserve privacy of requester. The data request is handled through the peer's proxies. The proxy can become a supplier later and mask the original requester. The requester asks one proxy to look up the data on its behalf. Once the supplier is located, the proxy will get the data and deliver it to the requester. The advantage is that other peers, including the supplier, do not know the real requester. The disadvantage is that the privacy solely depends on the trustworthiness and reliability of the proxy. To avoid specifying the data handle in plain text, the requester calculates the hash code and only reveals a part of it to the proxy. The proxy sends it to possible suppliers. After receiving the partial hash code, the supplier compares it to the hash codes of the data handles that it holds. Depending on the revealed part, multiple matches may be found. The suppliers then construct a bloom filter based on the remaining parts of the matched hash codes and send it back. They also send back their public key certificates. Examining the filters, the requester can

eliminate some candidate suppliers and finds some who may have the data. It then encrypts the full data handle and a data transfer key kdata with the public key. The supplier sends the data back using kdata through the proxy. The advantages are: (a) It is difficult to infer the data handle through the partial hash code, (b) The proxy alone cannot compromise the privacy, (c) Through adjusting the revealed hash code, the allowable error of the bloom filter can be determined. This scheme does not protect the privacy of the supplier. To address this problem, the supplier can respond to a request via its own proxy. The trust value of a proxy is assessed based on its behaviors and other peers' recommendations. Details of these ideas are in [32, 33, and 34]. Some ideas using blockchain are discussed in {24, 25] but they need further investigations.

3. Conclusions: This is a collection of research ideas that contribute to securing distributed systems and networks. We have identified the algorithms and ideas needed to build secure distributed systems. They include weak consistency for sites or set of sites disconnected from operating sites. We proposed incremental update of inconsistent database on recovered or now connected sites by using the ideas of fail locks on data in operational sites. For efficiency we propose the inconsistent data should be allowed to eventually recover by future transactions rather than by expensive copier transactions that copy data from consistent to inconsistent data items. The ideas that can be identify inconsistency are using version numbers on data items. If no logs or audit trail is available, we propose using the consistency based on data integrity predefined by users rather than transaction based consistency. The ACID properties need to be softened so that non-stop operations are possible during attacks and failures. We proposed ideas to comprehensively deal with collusive attacks rather than require the system to deal with each attack. The future is in accepting some degradation of operations, consistency, and atomicity but ensure durability that is ensured by the ideas of block chain.

RESULTS

The main results is that weak consistency can allow for graceful degradable system in contested environments. The need for ACID properties in distributed systems are too restrictive and weaker form of these properties will allow for success of PACE requirements. Malicious activities and attacks in communication system (mobile as well as wired) can be identified and mitigated. Collusive attacks are more difficult to deal with but a comprehensive defense mechanism is needed. Achieving privacy is possible through the use of proxies and active bundles. The block chain can enable auditing and any non-denial of transaction activity since they have a log of all transactions. This topic needs further study.

CONCLUSION

We have identified the algorithms and ideas needed to build secure distributed systems. They include weak consistency for sites or set of sites disconnected from operating sites. We proposed incremental update of inconsistent database on recovered or now connected sites by using the ideas of fail locks on data in operational sites. For efficiency we propose the inconsistent data should be allowed to eventually recover by future transactions rather than by expensive copier transactions that copy data from consistent to inconsistent data items. The ideas that can be identify inconsistency are using version numbers on data items. If no logs or audit trail is available, we propose using the consistency based on data integrity predefined by users rather than transaction based consistency. The ACID properties need to be softened so that non-stop operations are possible during attacks and failures. We proposed ideas to comprehensively deal with collusive attacks rather than require the system to deal with each attack. The future is in accepting some degradation of operations, consistency, and atomicity but ensure durability that is ensured by the ideas of block chain. We are investigating the ideas of semantics of mission needs and storing them in the schema of distributed database. This will allow for non-stop operation in contested environment and still allow a system to meet the mission needs.

REFERENCES

1. W. Song, K. Birman and authors, Freeze frame file system SoCC '16, October 05 - 07, 2016, Santa Clara, CA, USA. https://www.researchgate.net/publication/308495613
2. Y. Lin, S. Kulkarni, A. Jhumka, Automation of fault-tolerant graceful degradation. Distributed Computing. 32(1): 1-25 (2019)
3. Brigadier General Mehmet Yalinalp, TUR AF, Air Operations in Contested Environments, Joint Air & Space Power Conference 2016 https://www.japcc.org/air-operations-contested-environments/
4. Rear Admiral (LH) Thomas Ernst, DEU N, Commander, Maritime Air NATO, Agile Command and Control in a Degraded Environment, Joint Air & Space Power Conference 2016
5. PACE in military, https://en.wikipedia.org/wiki/PACE_Communication_Plan
6. MAJ Michael S. Ryan, A short note on PACE plans, https://www.benning.army.mil/infantry/magazine/issues/2013/Jul-Sep/pdfs/Ryan.pdf
7. N. Ahmed and B. Bhargava, Bio-inspired Formal Model for Space/Time Virtual Machine Randomization and Diversification, Accepted in IEEE Transactions on Cloud Computing, April, 2020, On page(s): 1-11 Print ISSN: 2168-7161 Online ISSN: 2168-7161 Digital Object Identifier: 10.1109/TCC.2020.2969353
8. H. Chen, Y. Zhang, Y. Cao, B. Bhargava, Security Threats and Defensive Approaches in Machine Learning System Under Big Data Environment, Wireless personal Communication, Springer-US, pp 1-21, 2021, https://doi.org/10.1007/s11277-021-08284-8
9. A. Hu, R. Jiang and B. Bhargava, "Identity-Preserving Public Integrity Checking with Dynamic Groups for Cloud Storage," in IEEE Transactions on Services Computing, Vol. 14, No. 4, 1097-1110, 1 July-Aug. 2021, doi: 10.1109/TSC.2018.2859999
10. N. Ahmed and B. Bhargava. From Byzantine Fault-Tolerance to Fault-Avoidance: An Architectural Transformation to Attack and Failure Resilience. IEEE Transactions on Cloud Computing, Volume 8, No. 3, pp 847-860, September, 2020.
11. J. Xu, S. Wang, B. Bhargava and F. Yang "A Blockchain-enabled Trustless Crowd-Intelligence Ecosystem on Mobile Edge Computing", IEEE Transactions on Industrial Informatics 15(6): 3538-3547 (2019)
12. J. Fu, L. Yun, B. Bhargava, "Source-Location Privacy Protection based on Anonymity Cloud in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Vol. 15, 100-114, May, (2020)
13. R. Ranchal, B. Bhargava, P. Angin and L. Ben Othmane, "EPICS: A Framework for Enforcing Security Policies in Composite Web Services," in IEEE Transactions on Services Computing, 12(3): 415-428 (2019)
14. N. Wang, J. Fu, J. Zeng, B. Bhargava, Source-location privacy full protection in wireless sensor networks. Information. Science. 444: 105-121 (2018)
15. R. Jiang, X. Wu, B. Bhargava, SDSS-MAC: Secure data sharing scheme in multi authority cloud storage systems, Computers & Security Vol. 62, pp 193–212, 2016
16. L. Othmane, R. Fernando, R. Ranchal, B. Bhargava, E. Bodden, Incorporating Attacker Capabilities in Risk Estimation and Mitigation, Journal of Computers and Security, Volume 51, pp. 41–61, June 2015
17. H. Kim, R. Oliveira, B. Bhargava, J. Song, A Novel Robust Routing Scheme against Rushing Attacks in Wireless Ad Hoc Networks, Wireless Personal Communications , Volume 70, Issue 4, pp 1339-1351, ISSN: 0929-6212, 2013.
18. T. Gong, B. Bhargava, "Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model", Security and Communication Networks Vol. 6: pp. 58-68, 2013.
19. B. Bhargava, P. Angin, R. Ranchal, R. Sivakumar, A. Sinclair, M. Linderman A Trust based approach for Secure Data Dissemination in Mobile Peer to Peer Network of AVs, International Journal of Next Generation Computing, Vol 3, No. 1, 2012

20. B. Bhargava, Y. Zhang, N. Idika, L. Lilien, M. Azarmi, “Collaborative Attacks in WiMAX Networks”, Wiley Journal on Security and Communication Networks, 2(5): 373-391, 2009
21. Y. Lu, W. Wang, D. Xu, and B. Bhargava. ``Trust based Privacy Preservation in Peer to Peer Data Sharing,” IEEE Transaction on Systems Man and Cybernetics (Special issues based on best papers in Secure Knowledge Management Conference), Vol. 36, No. 3, pp. 498-502, 2006
22. L. Lilien and B. Bhargava. ``A Scheme for Privacy Preserving Data Dissemination,” IEEE Transaction on Systems Man and Cybernetics (Special issues based on best papers in Secure Knowledge Management Conference), Vol. 36, No.3, pp. 502-506, 2006
23. A. Habib, S. Fahmy, S. Avasarada, V. Prabhakar, and B. Bhargava. ``On Detecting Service Violations and Bandwidth Theft in QoS Network Domains,” Computer Communications, Vol. 26, Issue 8, May 2003, pp. 861-871.
24. D. Ulybyshev, M. Villarreal-Vasquez, B. Bhargava, G. Mani, S. Seaberg, P. Conoval, D. Steiner, J. Kobes "Blockhub: Blockchain-based Software Development System for Untrusted Environments", IEEE CLOUD July, 2018
25. D. Ulybyshev, B. Bhargava, A. Alsalem "Secure Data Exchange and Data Leakage Detection in Untrusted Cloud", ICACCT 2018
26. D. Ulybyshev, B. Bhargava, D. Steiner, L. Li, J. Kobes, H. Halpin, M. Villarreal –Vasquez, A. Alsalem, R. Ranchal, Privacy – Preserving Data Dissemination in Untrusted Cloud, Proceedings of IEEE Cloud Conference, Honolulu, June 2017
27. W. Wang, Y. Lu, and B. Bhargava. ``On Vulnerability and Protection of Ad Hoc On-Demand Distant Vector Protocol,” in Proceedings of IEEE International Conference on Telecommunications, Tahiti, February 2003.
28. W. Wang, B. Bhargava, and M. Linderman, Defending against Collaborative Packet Drop Attacks on MANETs, in IEEE Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009), in conjunction with IEEE SRDS 2009.
29. E. Pitoura and B. Bhargava. ``Data Consistency in Intermittently Connected Distributed Systems,” IEEE Transactions on Knowledge and Database Engineering, Vol. 11, No. 6, December 1999, pp. 896-915.
30. B. Bhargava. ``Transaction Processing and Consistency Control of Replicated Copies during Failures,” Journal of Management Information Systems, Vol. 4, No. 2, 1987, pp. 93-112.
31. B. Bhargava and Z. Ruan. ``Site Recovery in Distributed Database Systems with Replicated Data,” in Proceedings of the Sixth IEEE International Conference on Distributed Computing Systems, Cambridge, 1986, pp. 621-627
32. Trust-Based Privacy Preservation for Peer-to-peer Media Streaming, Y. Lu, W, Wang, D. Xu, and B. Bhargava, in Proceedings of Secure Knowledge Management (SKM) Amherst, NY, September 2004
33. Private and Trusted Collaborations, B. Bhargava and L. Lilien, in Proceedings of Secure Knowledge Management (SKM) Amherst, NY, September 2004.
34. Privacy - Preserving Data Dissemination in Untrusted Cloud. Denis Ulybyshev, Bharat Bhargava, Miguel Villarreal-Vasquez, Aala Oqab Alsalem. IEEE Cloud, 2017.