Reliability

August 2016
Special Issue on IoT Security

IEEE
ReliabilitySociety

Reliability Society Administrative Committee (AdCom) Members

Officers (Excom)

President
Christian Hansen

Sr. Past President
Jeffrey Voas

Jr. Past President
Dennis Hoffman

Vice Presidents

Technical Activities
Shiuhpyng Winston Shieh

Publications
Jeffrey Voas (acting)

Meetings and Conferences
Carole Graas

Membership
Joe Childs

Secretary
Pradeep Ramuhalli

Treasurer
Bob Loomis

Elected Members-at-Large (with vote)

TERM EXPIRES 2016 (DEC 31)		***TERM EXPIRES 2017 (DEC 31)***		***TERM EXPIRES 2018 (DEC 31)***	
Lou Gullo	Zhaojun (Steven) Li	Joseph A. Childs	Carole Graas	Scott Abrams	Jason W. Rupe
Christian Hansen	Bob Loomis	Pierre Dersin	Samuel J. Keene	Evelyn H. Hirt	Alfred M. Stevens
Pradeep Lall	Pradeep Ramuhalli	Lance Fiondella	W. Eric Wong	Charles H. Recchia	Jeffrey Voas

Standing Committees and Activities/Initiatives

Web Master
Lon Chase

Standards
Lou Gullo

Chapters Coordinator
Loretta Arellano

Professional Development
Marsha Abramo

Constitution and Bylaws
Dennis Hoffman

Fellows
Sam Keene

Finance
Christian Hansen

Academic Education/Scholarship
Sam Keene

Meetings Organization
Alfred Stevens

Membership Development
Marsha Abramo

Transactions Editor
Eric Wong

Newsletter Editor
Lon Chase

Video Tutorials
Christian Hansen

Nominations and Awards
Jeffrey Voas

Life Science Initiative
Peter Ghavami

Transportation Electrification
Sam Keene
Pradeep Lall
Michael Austin

IEEE Press Liaison
Dev Raheja

IEEE Government Relations Committees

Energy Policy
Jeffrey Voas

Transportation and Aerospace Policy
Scott Abrams

Medical Technology Policy
Jeffrey Voas

Critical Infrastructure Protection
Sam Keene

Career and Workforce Policy
Christian Hansen
(corresponding only)

Intellectual Property Committee
Carole Graas
(corresponding only)

Research and Development Committee
Pradeep Lall

Combined TAB Ad Hoc Committee on Attracting Industrial Members
Dennis Hoffman

2013 TAB Awards and Recognition Committee (TABARC)
Dennis Hoffman

Technical Committees

Vice President for Technical Activities

Shiuhpyng Winston Shieh, National Chiao Tung University

Email: ssp@cs.nctu.edu.tw

Technical Committee on Internet of Things (IoT)

Chair: **Jeffrey M. Voas**, National Institute of Standards and Technology

Email: jeff.voas@nist.gov

Co–chair: **Irena Bojanova**, National Institute of Standards and Technology

Email: irena.bojanova@nist.gov

Committee Member:

1. George F. Hurlburt: CEO of Change Index

Technical Committee on System and Software Assurance

Chair: **Eric Wong**, University of Texas at Dallas

Email: ewong@utdallas.edu

Technical Committee on Prognostics and Health Management (PHM)

Chair: **Rex Sallade**, Sikorsky Aircraft Co.

Email: Rex.Sallade@SIKORSKY.COM

Co–chair: **Pradeep Lall**, Auburn University

Email: lall@eng.auburn.edu

Technical Committee on Big Data

Chair: **David Belanger**, Stevens Institute of Technology

Email: david.belanger@stevens.edu

Technical Committee on Trustworthy Computing and Cybersecurity

Chair: **Wen-Guey Tzeng**, National Chiao Tung University

Email: wgtzeng@cs.nctu.edu.tw

Co–chair: **Yu-Lun Huang**, National Chiao Tung University

Email: ylhuang@cn.nctu.edu.tw

Committee Member:

1. Raul Santelices: Assistant Professor, Department of Computer Science and Engineering, University of Notre Dam
2. Brahim Hamid: Associate Professor, IRIT Research Laboratory, University of Toulouse, France
3. Yu-Sung Wu: Assistant Professor, Department of Computer Science, National Chiao Tung University, Taiwan

Technical Committee on Reliability Science for Advanced Materials & Devices

Chair: **Carole Graas**, Colorado School of Mine & IBM Systems and Technology Group

Email: cdgraas@mines.edu

Technical Committee on Systems of Systems

Chair: **Pierre Dersin**, Alstom Transport

Email: pierre.dersin@transport.alstom.com

Technical Committee on Resilient Cyber-Systems

Chair: **Pradeep Ramuhalli**, Pacific Northwest National Laboratory

Email: pradeep.ramuhalli@pnnl.gov

Technical Committee on Cloud Computing, SDN and NFV

Co–chair: **Chih-Wei Yi**, National Chiao Tung University

Email: yi@cs.nctu.edu.tw

Co–chair: **Jason W. Rupe**, Polar Star Consulting

Email: jrupe@ieee.org

Committee Member:

1. Li-Ping Tung, National Chiao Tung University

Technical Committee on Power and Energy

Chair: **Shiao-Li Tsao**, National Chiao Tung University

Email: sltsao@cs.nctu.edu.tw

Technical Committee on Electronic and Computer System Reliability

Chair: **Terngyin Hsu**, National Chiao Tung University

Email: tyhsu@cs.nctu.edu.tw

Committee Member:

1. Kai-Chiang Wu: Assistant Professor, Department of Computer Science, National Chiao Tung University, Taiwan

Standards Committee

Chair: **Louis J Gullo**, IEEE RS Standards

Email: Lou.Gullo@RAYTHEON.COM

Committee Member:

1. Ann Marie Neufelder: Softrel, LLC – Owner; IEEE P1633 Standard Working Group Chair
2. Lance Fiondella: Assistant Professor, Dept. of Electrical and Computer Engineering, University of Massachusetts Dartmouth; IEEE P1633 Standard Working Group Vice Chair
3. Steven Li: Assistant Professor, Industrial Engineering and Engineering Management, Western New England University; IEEE P61014 Standard Working Group Chair
4. Diganta Das: Research Staff at the Center for Advanced Life Cycle Engineering, University of Maryland
5. Sony Mathews: Engineer at Halliburton, IEEE P1856 Standard Working Group Chair
6. Mike Pecht: Chair Professor and Director of Center for Advanced Life Cycle Engineering, University of Maryland
7. Arvind Sai Sarathi Vasan: Research Assistant at Center for Advanced Life Cycle Engineering , University of Maryland; IEEE P1856 Standard Working Group Vice-Chair
8. Joe Childs: Staff Reliability/Testability Engineer at Lockheed Martin

Working Group on Education

Chair: **Zhaojun (Steven) Li**, Western New England University

Email: zhaojun.li@wne.edu

Committee Member:

1. Emmanuel Gonzalez, Jardine Schindler Elevator Corporation

Editorial Board

Editor's Message

Welcome to this special issue of Reliability Magazine.

Just a decade ago, Internet-of-Things (IoT) was regarded as unrealistic fantasy. It was first presented as an innovative idea to stimulate the development of modern networking technologies. Within the last few years, as the maturity of tools, devices, equipment, infrastructure and services, IoT has become one of the most popular technologies in the 21st century. IoT intends to provide smart connectivity of devices on the Internet, ranging from home automation and entertainment products to industrial machinery and smart cities. It is designed to enable a variety of services by exchanging data with manufacturers, operators and consumers. Ideally, every IoT device can be uniquely identified and thus managed remotely, and is able to interconnect with other IoT devices in an automatic fashion.

Business processes can be empowered by this new technology, and various industries redesign their business models and processes along the IoT paradigm. For example, manufactures can monitor the status of things or predict when an IoT device is out of order. However, experts warn that the growing number of interconnected "thingbots" could endanger the IoT business. To maximize the social and economic benefit of the technology, security issues of interoperability, data management, platform and protocol validation have to be addressed.

In this special issue, we have collected two articles, which discuss security issues for IoT applications from different points of view.

The first article, "Secure and Safe Automated Vehicle Platooning" is by Jiafa Liu from the Computer and Information Science Department at the University of Michigan-Dearborn. This article discusses security issues when IoT is applied to automotive applications. Cyber attacks highlighted on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems.

The second article, "Anonymous and Secure Fault-Tolerable Routing Protocol for Overlay Networks" is by Chia-Chen Wu from the Computer Science Department at National Chiao-Tung University. The routing security is addressed for overlay networks and IoT applications. A novel protocol (SAFE) providing anonymity against adversaries is presented in the article. By randomly selecting intermediate nodes to forward data and by using layered encryption to hide an initiator from the intermediate nodes, SAFE can provide initiator and responder anonymities and fault tolerance of node failures. The fault tolerance provided by SAFE results in the reduced cost and frequency of path reconstruction, and the increased robustness of network against degradation attacks.

We hope you enjoy the articles in this issue, and that you find these contributions to the discussion of security of IoT applications within the reliability engineering profession useful. We look forward to your comments and suggestions.

Yu-Lun Huang

Professor and Director, National Chiao-Tung University (NCTU)

Editor, IEEE Reliability Special Issue on Trustworthy Computing and Cybersecurity

ylhuang@cn.nctu.edu.tw

Reliability
IEEE Reliability Society
IEEE

Special Issue on IoT Security

Regular Issue

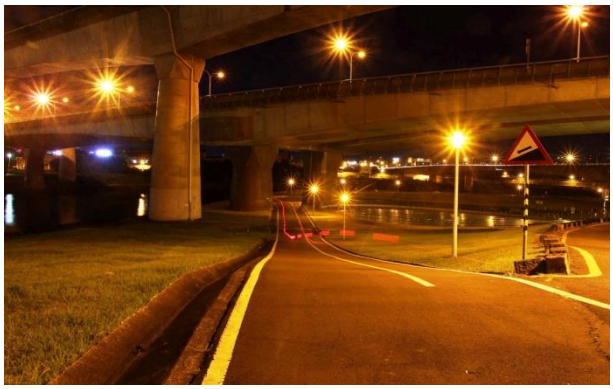
Secure and Safe Automated Vehicle Platooning

Jiafa Liu
University of Michigan-Dearborn
jiafal@umich.edu

Di Ma
University of Michigan-Dearborn
dmadma@umich.edu

André Weimerskirch
Lear Corporation
aweimerskirch@lear.com

Haojin Zhu
Shanghai Jiao Tong University
zhu-hj@cs.sjtu.edu.cn



Abstract - Cooperative adaptive cruise control (CACC) or platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. The complexity of automated vehicle platoon systems opens doors to various malicious cyber attacks. Violation of cybersecurity often results in serious safety issues as it has been demonstrated in recent studies. However, safety and security in a vehicle platoon so far have been considered separately by different sets of experts. Consequently no existing solution solves both safety and security in a coherent way.

In this article, we show that attacks on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems (CPS). Based on a deep comprehension on the interrelation of safety and security, we present a safety-security co-design engineering process to derive functional security requirements for a safe automated vehicle platoon system. Finally, we offer a vision of the future research issues on this important area of automated and connected vehicles.

Keywords - IoT security, vehicle to vehicle communication, cyber physical systems

I. INTRODUCTION

Vehicle platooning has been studied as a method of increasing the capacity of roads since the 1960's. In a vehicle platoon, a group of vehicles, following one another, acts as a single unit through coordinated movements. Because vehicles in a platoon travel together closely yet safely, this leads to a reduction in the amount of space used by the number of vehicles on a highway, thus has the great potential to *maximize highway throughput*. Cooperative adaptive cruise control (CACC) or automated vehicle platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. Automation-capable vehicles in tightly spaced, computer-controlled platoons offer additional benefits such as *improved mileage and energy efficiency* due to reduced aerodynamic forces, as well as increased *passenger comfort* as the ride is much smoother with fewer changes in acceleration.

The complexity of an automated vehicle platoon system – including inter-vehicle communications, vehicle's internal networking and its connection to external networks, as well as complicated and distributed platooning controllers – opens doors to malicious attacks. A number of research has demonstrated various attacks targeting every component of the platoon system [2], [8], [9], [14]. All these attacks could cause a wide array of problems in a deployed platoon, for example, an attacker could cause crashes, reduce fuel economy through inducing oscillations in spacing, prevent the platoon from reaching its (or each individual's) destination(s), or cause the platoon to break up. The full potential of automated vehicle platooning will not be realized until the issues related to communication and application security can be satisfyingly resolved.

The violation of cybersecurity could result in serious safety violations such as car crashes in a cyber physical system. However, safety and security in a vehicle platoon have so far been considered separately by different sets of experts. On one hand, the safety discipline usually considers system failures (including systematic/random hardware and systematic software failures) or natural disasters as safety hazard

resources. Safety solutions developed are usually not evaluated in an adversarial environment. On the other hand, the security discipline considers various attacks that can lead to different consequences such as loss of life, loss of privacy, financial loss, etc. The variety of security goals to address different types of attacks makes it very unlikely to be aligned with the goal of safety. Consequently security solutions proposed are rarely evaluated in terms of safety. For example, the model-based detection scheme [8], the only scheme proposed so far for platoon security, is designed from the **security point of view** by monitoring any misbehavior of the proceeding car. Although the scheme is able to detect vehicle misbehavior, whether it can lead to a safe platoon is not answered. To date, no existing platooning solution solves both safety and security in a reconciled and coherent way.

The need for a safety and security co-design is urgent today with the practicality of automated vehicle platooning technology. Actually there has been calls long ago for safety and security communities to work together [4]. Past efforts in the automotive industry have reached a consensus that functional safety hazards can arise from malicious activities in addition to systematic failures and random hardware failures [5]. So security should be considered as a pre-requisite for safety while safety should be one of the driving forces for security design. Although a couple of works have described a safety and security engineering process [5], [7], a lot of challenges need to be addressed to come up with a concrete safe and secure platoon system: How to reconcile different safety and security risks? How to align the goal of security with that of the safety? The most important, how to arrive at a solution that satisfies both the safety and security requirements? There are also performance challenges such as efficiency, real time, as well as maintaining the string stability of platoon.

In this article, we show cyber attacks on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems (CPS). Based on a deep comprehension on the interrelation of safety and security, we present a safety-security co-design engineering process to derive functional security requirements for a safe automated vehicle platoon system. Finally we offer a vision of the future research issues on this important area of automated and connected vehicles.

II. SECURITY-INDUCED SAFETY RISK ANALYSIS

The EU project EVITA provides a risk model to measure the safety risks of in-vehicle systems [1]. The risk analysis rationale of EVITA is that as it is too costly to protect against every threat, it is necessary to rank risks in order to prioritize countermeasures. Risk associated with a security attack depends on (1) **severity** of impact and (2) **probability** of successful attack. In this section, we analyze the severity as well as the probability of platooning attacks by using the EVITA model.

In response to various safety risks, ISO 26262 severity classification defines four severity levels (S0, S1, S2 and S3) in terms of the estimated personal injury that could result from the risk. S0 refers to no injuries. S1 refers to light or moderate injuries. S2 means severe to life-threatening injuries (survival probable). S3 means life threatening (survival uncertain) or fatal injuries. The EVITA model extends the ISO 26262 safety classification by including a fifth level S4 which means fatal injuries of **multiple vehicles** as cyber security attacks may have more widespread implication than unintended hardware or software bugs can cause.

Previous work has shown that many cyber attacks (such as message falsification attack, remote control attack, etc.) can result in serious safety issue. However, it is not clear the severity level of such attacks. To understand the severity level of a collision that resulted from a cyber attack, we introduce a new attack called leader crash attack by extending the collision induction attack proposed in [8]. In the leader crash attack, the leading car stops suddenly (intentionally or not) and causes the following cars to crash over each other. This crash attack can be mounted by any insider, not just the leader, in the platoon. However it is very likely a crash attack induced by the leader can have the most severe consequence.

We firstly argue collision induction attack is very possible (**probability**). It has been demonstrated successfully on several modern vehicle models that an attacker can totally control a vehicle by compromising its hardware or software locally or remotely through a wide range of attack vectors [6], [10]–[12]. When a leader or any insider of the platoon is compromised and can be remotely controlled, an attacker can issue an instruction to the victim vehicle to brake abruptly so that the following cars will crash into the front ones. The risk of insider crash attack will become more serious with the advancement in vehicle automation. If an insider car is a compromised driverless automated vehicle, such an attack can be mounted with severe consequence at a low cost. Also, we do not exclude the case when the driver himself is reckless.

We use the PLEXE simulator to demonstrate the consequence of this attack (**severity**). PLEXE is an Open Source extension to the known and widely used Veins simulation framework by adding platooning capabilities and controllers. In this simulation, initially a platoon of four vehicles is driving at the speed of 100 km/h with a gap of 5 meters. At the time of 50s, we instruct the leader vehicle to stop. We set the deceleration of the leader car extremely large so that the speed can decelerate to zero in a very short time interval. In this way, the leader vehicle acts just like it suddenly hits the brake so that it stops immediately. We see how the following

vehicles will respond under the CACC controller strategy. From the mobility traces of the platoon collected, we can we can see that following vehicles crash into preceding vehicles at 50.41s, 50.75s and 51.10s respectively.

To obtain an insight of speed changing of the platoon in the crash, we utilize the statistics collected from PLEXE which are shown in Figure 1. In Figure 1, Vehicle 0 with the red line is the leader vehicle. Vehicle 0 decelerates from 100 km/h (27.77 m/s) to 0 km/h in a very short time interval. The following vehicles are trying to prevent crash by decelerating, but the 5-meter gap is not long enough for them to fully stop before they crash into the car before it. The above three lines terminating at different time spot shows that each of them has crashed into the leader vehicle.

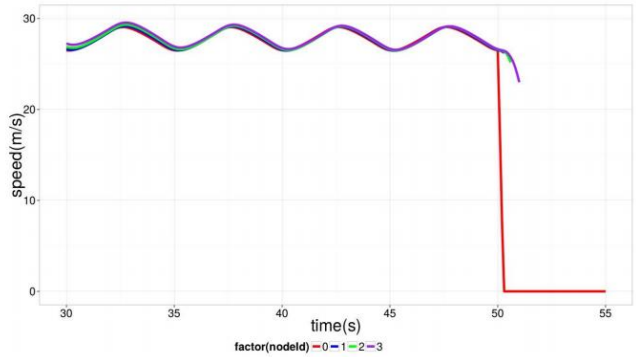


Fig. 1: Speed Changes of Platoon during the Crash

More on severity. The above simulation clearly demonstrates that the leader car crash attack can potentially result in multiple car damage and life injuries and has the highest level of safety severity. However, the maximum safety impact of security attack demonstrated is only a **local** event to several vehicles. We believe the worst security impact can potentially be *nation-wide* impacting thousands or millions of cars and suggest a new severity level of **S5: nation-wide spread and harmful impact**. For example, in the platoon context, suppose there is a security weakness that has an impact due to forged DSRC messages, also suppose future smartphones are DSRC enabled and malware spread on smartphones, we can easily see a nation-wide attack platform to attack the platoon mechanism.

Due to the severity and probability of security attacks on platoon systems, we strongly argue the importance of designing safe and secure platoon systems.

III. SAFETY-SECURITY CO-DESIGN

Safety has a long tradition in many engineering disciplines and has had successful standardization efforts. In automotive systems, the international standard ISO 26262 [15] is the state of the art standard for safety critical system development. Automotive security has evolved quite recently with networked systems and concerns about privacy, data integrity, authenticity and protection. As long as safety critical systems were not networked, the two fields did not have to interact and as a result, the two domains have evolved separately so far with little overlap. As cyber-physical systems evolved into networked systems, security became a relevant issue for safety critical systems.

The Vehicle Cybersecurity Systems Engineering Committee of SAE has been working on J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [13]. J3601 is an overall guidebook on implementing cybersecurity for the entire vehicle. The safety-security co-design is being discussed in the SAE committee at the moment and there is no final product yet. We were able to work with several members of the SAE cybersecurity committee to understand the concepts and requirements as well as discuss the proposed safety-security engineering process.

We propose a safety-security co-design engineering process which consists of four main steps: (1) Define the safety goal for the system; (2) Define attack model; (3) Derive security goals; (4) Derive functional security requirements.

Safety Goal. Safety is very important in automotive industry and therefore highly regulated. For end users, it means that users do not face any risk or danger coming from the motor vehicle or its spare parts. Unacceptable consequences for safety are loss of human life and injuries. The safety goal of individual vehicle is to protect users from injuries and life threatening risks. In our context, we set up the safety goal of vehicle platoon as avoiding car collisions that can cause human life and injuries.

Attack Model and Security Goal. Unlike safety, cybersecurity has a broader range of unacceptable consequences such as human life and injury (safety), human security, financial loss, loss of privacy, etc. Figure 2 shows the interrelation of safety and security. From Figure 2, we can see that safety can be an objective (or impact) of a security attack. It can also be an unintended consequence caused by hardware or software bugs. Meanwhile, cyber security attacks can have different impacts. The intersection part concerns both safety and security, or safety-related security risks, which is of interest of this paper.

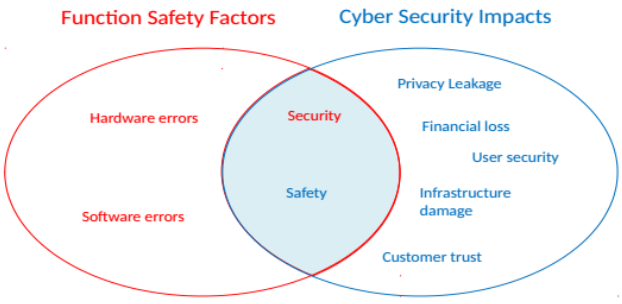


Fig. 2: Interrelation of Safety and Security

To derive our attack model that lead to safety, we summarize various attacks, targeting at automotive platoon systems, proposed by researchers in the literature and their corresponding possible consequences in Table I. From the table, we can see that there are five attacks which can lead to car collisions, result in safety issues, and thus belong to the intersection in Figure 2. The security goal for a safe platoon is to develop a system that is resilient to these attacks.

Reference	Attack	Impact
[3]	Message falsification attack	Collision
	Message spoofing	Collision
	Message replay	Collision
	DoS (jamming)	Dissolved platoon
	System tampering	Collision
[8]	Collision induction attack	Collision
	Reduced headway attack	Decreased string stability
	Joining without radar	Decreased string stability
	Mis-report attack	Decreased performance
	Non-attack abnormalities	Decreased performance
[14]	Destabilization attack	Decreased string stability
	Platoon control taken attack	Dissolved platoon

TABLE I: Attacks and impacts

If a vehicle is a victim of *System tampering* attack, we mean an attacker is able to control the vehicle remotely through compromised hardware or software. The victim vehicle will behave like the one in either collision induction attack or message falsification attack, without the awareness and involvement of the driver. For us, we only need to focus on attack behaviors without worrying about who, the driver or a remote attacker, initiates the attack. Therefore in the following of the paper, we only consider collision induction attack and message falsification attack and ignore who initiates the attack.

Based on the discussion above, we derive an attack model emphasizing on safety of platoon as follows:
Adversary Model for Safety: We consider cyber attacks that can lead to safety issues such as car crashes in this work. Attacks that result in different consequences such as system performance, driver privacy, financial loss, etc. are not considered in this model as they can be treated in the regular way without considering safety. The adversary or the vehicle controlled by the adversary is part of the platoon system and thus is able to send valid V2V messages. However, there is no guarantee on the correctness of information in the messages it sends. Also the adversary does not need to follow the control law. The adversary is able to control one or more vehicles, including the leader, in the platoon. However, it cannot control all the radars or radar signals of vehicles in the platoon because of the line-of-sight requirement.

Functional Security Requirements.

From the analysis above, we can derive functional security requirements as follows:

- It shall not be possible for an attacker to spoof a message;
- It shall not be possible to replay an old message;
- It shall not be possible for an attacker to broadcast a message with false information without being detected;
- The system shall be able to take a response action whenever a misbehavior is detected;
- The system shall ensure there is enough time for the system to respond.

IV. FUTURE RESEARCH ISSUES

The practical use of automated vehicle platooning systems relies on the security, safety, and reliability provided by such systems. Many existing techniques (such as cryptographic functions, secure hardware and software, etc.) can be used to defend against many attacks targeting a platoon system. Further work needs to be done to strengthen the security and safety aspects of such systems.

Securing platoon controllers. Stable coordinated movements in a platoon are described as string stability which ensures range errors decrease as they propagate along the stream of vehicles in a platoon to achieve constant inter-vehicle spacing. A lot of vehicle platooning control algorithms have been developed to achieve string stability. However, these algorithms have not been developed and analyzed under adversarial environment where an adversary wants to inhibit the performance of the control algorithm and hence cause instability of the system which may further cause intelligent collisions. It is clear that many potential attacks could happen to the underlying control algorithm. Thus it is important to systematically access the security risks/needs in automated platooning by looking at factors that affect, directly or indirectly, the coordinated movements of vehicles.

Resilient sensor fusion. There is a strong opinion today that a successful platoon will require wireless communication between vehicles for coordination. However, we believe that the wireless link is the weakest sensor of an automated car, compared to radar, LIDAR, and camera, and that it can easily be forged by a motivated attacker. Hence it seems that a vehicle in a platoon, and possibly an automated vehicle, must not rely on wireless communication if it has any impact to the vehicles control algorithms. Furthermore, it has recently been demonstrated that it is fairly easy to forge LIDAR and radar sensors by using a modulated laser. Hence we need strategies to fuse sensor input and detect forged individual input. One idea is to assign confidence levels to sensors (e.g. DSRC is lower than camera) and correct sensor input if individual

sensors show unreasonable inputs based on the confidence levels. Apparently more complex strategies are required to account for an attacker that will forge several sensors in parallel. It might be necessary to include some kind of heuristic, e.g. machine learning, to detect abnormal sensor input.

Securing the leader. The leader in a platoon is responsible for setting the trajectory and speed to the vehicles behind it. In a distributed platoon control algorithm, a vehicle adjusts its movements based on knowledge of the preceding vehicle and the lead vehicle to determine its next movement. Information of the preceding vehicle is usually direct hearing and can be further cross-verified with in-vehicle sensor data. However, information of the leading vehicle could be second-hand information — the vehicle might not be in the transmission range of the leader and receives the leader's status information indirectly from proceeding vehicles. It is important to protect the authenticity of messages of the leader and the leader itself to prevent leader impersonation. Especially, when a new car joins the platoon, the first task is to correctly identify the leader. Message authenticity has been well studied. It might be useful to have an endorsement mechanism to protect the leadership of the leader from being impersonated by using some efficient cryptographic primitives. The leadership is established through the endorsement of participating vehicles in the platoon. A vehicle who has endorsed the leader cannot deny its endorsement. An adversary should not be able to alter the endorsement even when it (and its collaborators) is one of the endorsers. A possible cryptographic primitive that can be used to protect leadership is the aggregate signature scheme which allows multiple entities to co-sign one document.

Securing the following vehicles. It appears that following vehicles need slightly different control and protection algorithms than the leading vehicle. The following vehicles cannot necessarily use their cameras which are the most resilient (against cybersecurity attacks) sensors, however, they are more dependent on the received wireless messages which are least reliable in terms of cybersecurity. Hence the control algorithms defined above will be revisited and refined for this case.

V. CONCLUSION

In this article, we show that cyber attacks on a platoon system can have the most severe and widespread safety impact as defined by the EVITA vehicle security risk model. We argue the importance of safety-security co-design for safety critical cyber physical systems and make the first effort toward a safety-security co-design engineering process which allows functional security requirements to be derived for a safe automated vehicle platoon system. We also offer a vision of the future research issues on this important area of automated and connected vehicles.

REFERENCES

[1] Evita: E-safety vehicle intrusion protected applications. http://www.evita-project.org/.

[2] Researcher hacks self-driving car sensors. http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors.

[3] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. Zhang, J. Rowe, and K. Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *Communications Magazine, IEEE*, pages 126–132, 2015.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. on Dependent and Secure Computing*, 1:11–33, 2004.

[5] S. Burton, J. Likkei, P. Vembar, and M. Wolf. Automotive functional safety = safety + security. In *First International Conference on Security of Internet of Things (SecureIT 2012)*, 2012.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011, August.

[7] B. Czemy. System security and system safety engineering: different similarities and a system security engineering process based on the ISO 26262 process framework. *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.*, 6:349–359, 2013.

[8] B. DeBruhl. Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2015.

[9] E. B. Hamida, H. Noura, and W. Znaidi. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics 4.3*, pages 380–423, 2015.

[10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, and S. Savage. Experimental security analysis of a modern automobile. In *In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 447-462). IEEE*, 2010, May.

[11] C. Miller and C. Valasek. Remote exploitation of an unaltered passenger vehicle. In *Black Hat USA*, 2015.

[12] I. Roufa, R. M., H. Mustafaa, T. Taylora, S. O., W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb. Security and privacy vulnerabilities of incar wireless networks: A tire pressure monitoring system case study. In *In 19th USENIX Security Symposium, Washington DC (pp. 11-13)*, 2010, February.

[13] SAE International. Cybersecurity guidebook for cyber-physical vehicle systems. http://standards.sae.org/wip/j3061/.

[14] D. Soodeh, R. M. Gerdes, and R. Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015.

[15] I. Standards. Road vehicles – functional safety. http://www.iso.org/iso/home/store/catalogue tc/catalogue detail.htm?csnumber=43464.

AUTHOR BIOGRAPHY

Jiafa Liu is a graduate student in the Computer and Information Science Department at the University of Michigan-Dearborn. He is interested in vehicle security, platoon security and smartphone security. He received the B.S. degree in computer science from Shanghai Jiaotong University. He won the Shanghai Jiaotong University Scholarship Second Prize in 2014 and 2015.

Di Ma is an Associate Professor in the Computer and Information Science Department at the University of Michigan-Dearborn, where she leads the Security and Forensics Research Lab (SAFE). She is broadly interested in the general area of security, privacy, and applied cryptography. Her research spans a wide range of topics, including smartphone and mobile device security, RFID and sensor security, vehicular network and vehicle security, computation over authenticated/encrypted data, fine-grained access control, secure storage systems, and so on. Her research is supported by NSF, NHTSA, AFOSR, Intel, Ford, and Research in Motion. She received the PhD degree from the University of California, Irvine, in 2009. She was with IBM Almaden Research Center in 2008 and the Institute for Infocomm Research, Singapore in 2000-2005. She won the Tan Kah Kee Young Inventor Award in 2004.

Andre Weimerskirch is VP Global Cyber Security at Lear Corporation. Before that, André established the transportation cyber security group at the University of Michigan Transportation Research Institute (UMTRI), and co-founded the embedded systems security company ESCRYPT which was sold to Bosch in 2012. André is active in all areas of automotive and transportation cyber security and privacy, published numerous articles in the area of automotive and embedded cyber security, and is co-founder of the American workshop on embedded security in cars (escar USA). André is vice chair of the SAE Vehicle Electrical System Security Committee, and co-chairs the Michigan Mobility Transformation Center (MTC) cyber security working group.

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc. (2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. His current research interests include network security and data privacy. He published 33 international journal papers, including IEEE Trans. on Parallel and Distributed Systems, IEEE Trans. on Mobile Computing, IEEE Trans. on Wireless Communication, IEEE Trans. on Vehicular Technology, IEEE Wireless Communications, IEEE Communications, and 50 international conference papers, including ACM CCS, ACM MOBICOM, ACM MOBIHOC, IEEE INFOCOM, IEEE ICDCS, IEEE GLOBECOM, IEEE ICC, IEEE WCNC. He received a number of awards including: IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award (2014), Top 100 Most Cited Chinese Papers Published in International Journals (2014), Supervisor of Shanghai Excellent Master Thesis Award (2014), Distinguished Member of the IEEE INFOCOM Technical Program Committee (2015), Outstanding Youth Post Expert Award for Shanghai Jiao Tong University (2014), SMC Young Research Award of Shanghai Jiao Tong University (2011). He was a co-recipient of best paper awards of IEEE ICC (2007) and Chinacom (2008) as well as IEEE GLOBECOM Best Paper Nomination (2014). He serves as the Associate/Guest Editor of IEEE Internet of Things Journal, IEEE Wireless Communications, IEEE Network, and Peer-to-Peer Networking and Applications.

Investigating Anonymous and Secure Fault-Tolerable Routing Protocols for Overlay Networks

Chia-Chen Wu
National Chiao Tung University
chiachen.cs95g@gmail.com

Yu-Lun Huang
National Chiao Tung University
ylhuang@cn.nctu.edu.tw

Shiuhpyng Shieh
National Chiao Tung University
ssp@cs.nctu.edu.tw

Abstract - Anonymity is important for both data requests and responses in IoT applications running on overlay networks. Overlay routing reveals information since identities are required to locate and obtain sensor data from nodes (i.e. IoT devices). An anonymous and secure fault-tolerable routing protocol is hence required to provide anonymity against adversaries and tolerance of node failures. In this paper, we discuss and compare the existing anonymous systems in terms of key management, storage cost and anonymity. To secure a communication session, confidentiality and integrity should be provided. Layered encryption algorithms are then recommended to secure messages flowing through an overlay network. To provide anonymity, it is ideal to have every node along the path only know its previous and next hops, so that an intermediate node can identify neither the initiator nor the responder. To guarantee fault tolerance, grouping nodes within a certain distance or with the same prefix is recommended. Thus, any node on the routing path can easily take over message forwarding if any of its group nodes is detected inactive or failed.

Keywords - IoT security, overlay networks, anonymity route, fault-tolerance

I. INTRODUCTION

Security, productivity, connectivity and management bring the growth of IoT services running on overlay networks. Overlay networks [1] can decouple network addresses from physical placements of peers and enable Internet-of-Things (IoT) applications (see Figure 1). IoT applications allow users to request information and control devices (such as home appliance) remotely. Anonymity and security hence become much more important when IoT users and devices are communicating with each other [2]. Without protection, an adversary lurking in an IoT network may easily trace the communication peers and eavesdrop the conversation between nodes. A protocol securing the routing paths and providing anonymity is hence required for anonymity protection in such cases.

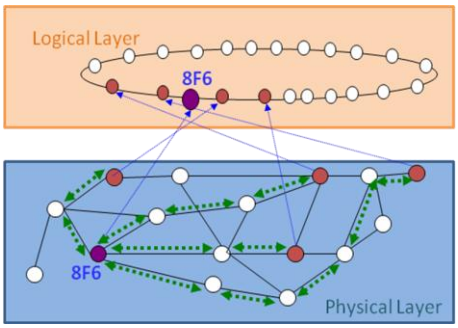


Figure 1 Overly Networks

In the past few years, researchers investigated different kinds of anonymity methods, including initiator anonymity, responder anonymity and relationship anonymity (unlinkability), for overlay and peer-to-peer networks [3][4][5][6][7]. Initiator anonymity hides the identity of an initiator to all other peers in the network, while responder anonymity hides the responder from all other peers. If both initiator anonymity and responder anonymity are provided, mutual anonymity is then guaranteed. Relationship anonymity ensures the unlinkability between an initiator and its responders. Nodes helping forward messages cannot locate the source and destination of a conversation.

Most anonymity related systems, such as Onion Routing [8], make all anonymous connections go through a fixed set of trusted nodes (e.g. IoT gateways), which are not preferred in decentralized overlay networks. By monitoring the traffic of either a colluding entry or exit, adversaries may easily identify the initiator or responders during any communication session. Failure of any fixed nodes along a routing path results in data

loss and larger jitter before the routing path is recovered or a new path is constructed.

Since 2000, many methods, including Surepath[3], Onion Routing [8], Crowds [9], Tarzan [10], , Tor [11], Cashmere[12], Agyaat [13], and Aqua [14] have been designed to exploit peer-to-peer overlays in anonymous communication. A number of random nodes are used to build up anonymous paths or tunnels. In these methods, messages delivery will be failed if any node along the route fails or misbehaves. When there is an error in the route, it is generally difficult for an initiator to locate the failure node. Consequently, the initiator needs to reconstruct another routing path for delivering messages. Frequent reconstruction of routing path, however, exposes the initiator to eavesdroppers and attacks. Hence, a secure, anonymous and fault-tolerable routing protocol is required for enhancing the route reliability for overlay services and IoT applications.

In this paper, we discuss the existing anonymous systems for overlay networks and explain the possibility to adopt layered encryption and random intermediaries to achieve anonymity and guarantee unlinkability between an initiator and its responders.

II. ANONYMOUS SYSTEMS

The section briefly introduces some of the popular anonymous systems, such as Crowds, Onion Routing, Tarzan, Tor, Cashmere, Agyaat, and Surepath.

In Crowds [9], no encryption is adopted. Any node on the path can observe the conversation traffic. Crowds can provide some anonymity by routing messages through anonymous paths involving a randomly chosen sequence of nodes. The initiator sends the message to a randomly-chosen node called "jondo." Upon reception, each jondo randomly decides to either send the message to the responder or forward it to another jondo. In Crowds, anonymous paths are vulnerable to node failures. Node failures pose a functionality problem for anonymous paths.

Onion Routing[8] uses a static set of dedicated onion routers to redirect network traffic. Before sending a message, the sender selects a set of currently active routers to forward through. Session keys are distributed to the chosen routers during the setup phase. The initiator creates an onion by encrypting the message with the public key for every router in the routing path. To transfer a message, each router decrypts the outside layer with its private key. After that, the router discovers the next hop and forwards the message. Every relay node knows only its previous and next hops. Node churns, frequent node arrivals, departures, and failures, limit the scalability of Onion Routing.

Tarzan [10] provides anonymity with high resistance against traffic analysis by using layered encryption, multi-hop routing, cover traffic and a special mix selection protocol. The source chooses a set of relays to act as a path and iteratively establishes a tunnel through these relays with symmetric keys between them. The creation of a tunnel incurs both significant computation overhead and delay. The source wraps the packets in several layers of encryption and sends it through relay nodes. The relay node strips off one layer and sends it to next relay node, etc. Since none of the peers on a tunnel knows the whole path, an adversary cannot figure out communicating peers. Tarzan is still vulnerable if an adversary can observe traffic throughout the Internet. Another vulnerability of Tarzan is the resilience of node failures. Node failures pose a functionality problem for anonymous paths. Also, responder anonymity is not guaranteed in Tarzan.

Tor [11], the second generation of Onion Routing, is one of the most popular privacy enhancing systems. Tor provides mutual anonymity against non-global adversaries using rendezvous points. Tor uses a directory server to maintain router information, which limits the scalability. If the first or last router is compromised in an Onion Routing network, either source or destination can be revealed. Recent work also shows that the Tor anonymity network is vulnerable to the attack in which eavesdroppers may exploit the homogeneous routing policy by falsely advertising high bandwidth links, drawing traffic towards the nodes under its control.

Cashmere[12], a resilient anonymous routing system on structured overlay networks, provides both source anonymity and unlinkabality of source and destination. Cashmere is designed to use a prefix-routing based on structured overlay network, such as Tapestry and Pastry. As shown in Figure 2, nodes with the same prefix form a group. The routing path used in Cashmere is a set of distributed relay groups rather than a single node. Layered encryption is then applied on the routing path by the public/private key pair shared with all members of each relay group. Except all the members of the relay group in the routing path fail, the routing path is remained valid. The source node can randomly reorder the relay groups to hide the destination relay group containing the destination node.

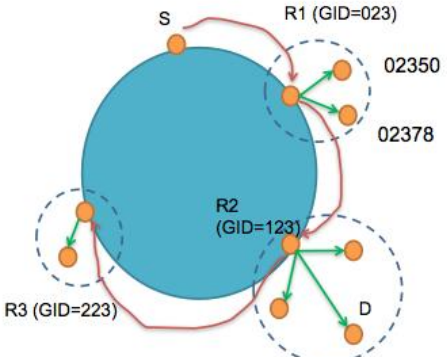


Figure 2 Cashmere

Agyaat [13] provides a compromise between anonymity and efficiency by means of a two-level hybrid architecture. In this system, the initiator can flood its request to every peer in its cloud. At the responder's end, some peers in the cloud of the responder get the request and then broadcast it in its cloud. Agyaat makes a key map onto a cloud linking to an appropriate peer.

In SurePath[3], a node seeking initiator anonymity generates a small number of RSA session keys, deploys the RSAs into an overlay network using distributed hash table (DHT), forms an anonymous path using a subset of the deployed RSAs, and sends messages through the resulting anonymous path, as illustrated in Figure 3. Leveraging the DHT routing infrastructure and data replication mechanism, SurePath is fault-tolerant to node failures. Nodes with similar identities can form a group and nodes in the same group can help forward messages if any node in the group fails. However, a malicious node can disclose the RSAs stored in its local storage to other colluding nodes such that the malicious nodes can pool their RSAs to break anonymity of other users.

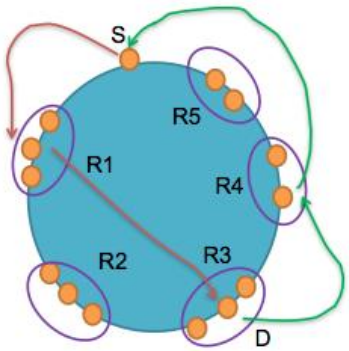


Figure 3 SurePath

More, no mechanism is provided in SurePath for detecting compromised tunnels. SurePath users need to reform their tunnels periodically to resist against the colluding malicious nodes.

III. COMPARISON

To secure communication sessions, confidentiality and integrity should be provided. Layered encryption algorithms are then recommended to secure messages flowing through an overlay network. To provide anonymity, it is ideal to have every node along the path only know its previous and next hops. Hence, an intermediate node can identify neither the initiator nor the responder. To guarantee fault tolerance, grouping nodes within a certain distance or with the same prefix is recommended. Thus, any node on the routing path can easily take over message forwarding if any of its group nodes is detected inactive. This section compares the existing anonymous systems in terms of key distribution, storage cost and anonymity.

(1) Key distribution and discovery

Since node identity is used as node's public key, newly joined nodes in Cashmere do not affect the existing nodes. In SurePath, adding or deleting a node requires extra key distribution or index management. The performance of SurePath decreases as the number of nodes in overlay networks increases. More, Tarzan, Onion Routing, SurePath, Cashmere use layered encryption and multi-hop routing to achieve anonymity. Hence, a trusted third party (like Certificate Authority) is required to generate public keys for protecting data secrecy. However, if algorithms like Fuzzy identity-based encryption scheme [15] is used, key generation and encryption can be done without CA involvement.

(2) Storage cost

Storage cost is one of the concerns when deploying security mechanism to IoT networks. In Cashmere, every node having an *m*-bit identity needs to keep *m* public keys and *m* private keys corresponding with each identifier prefix. In SurePath, each node stores several keys, including its private key, public keys of other nodes and the corresponding symmetric keys for relay sets.

(3) Anonymity

The systems and methods mentioned in the previous section are designed for generating anonymous routing path that provides initiator anonymity. Among them, SurePath forwards and replies messages via different routing paths so that they can prevent the traffic being analyzed by an adversary. For responder anonymity, SurePath and Cashmere know not only the data name but also the public key of the node storing the data. Considering a network in which every node has an *m*-bit identity, and an attacker has compromised a node in the network, 1) if the network runs with Cashmere, the attacker can obtain *m* public keys and *m* private keys associated with the prefix of the compromised node; 2) if the network runs with SurePath, the attacker can control *N-1* share keys where *N* is the network size.

IV. CONCLUSION

To secure communications for peer-to-peer or IoT applications (like smart home appliance control) running on an overlay network, a secure, anonymous and fault-tolerant routing protocol should be designed to provide anonymity against adversaries. Layered encryption and random intermediaries can be adopted to achieve anonymity for overlay networks. By grouping nodes with the same prefix or within a certain distance, and applying algorithms like Fuzzy identity-based encryption scheme, a node is allowed to decrypt the ciphertext encrypted with any other's public key if and only if the two nodes belong to the same group or are within a certain distance. Thus, any node can easily take over message forwarding if its neighboring node fails. Unlinkability between

initiator and responder should also be guaranteed by unlinking an immediate node and its previous node and next node. In the paper, we compare the existing anonymous systems in terms of key management, storage cost and anonymity to show how the existing systems work for routing messages in an overlay network.

REFERENCES

[1] Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma and Steven Lim, **"A Survey and Comparison of Peer-to-Peer Overlay Network Schemes,"** IEEE Communications survey and tutorial, Mar. 2004.

[2] Nguyen Phong Hoang and Davar Pishva, **"A TOR-based Anonymous Communication Approach to Secure Smart Home Appliances, "** in Proc. of 17th International Conference on Advanced Communication Technology (ICACT), PP. 517 – 525, 2015.

[3] Yingwu Zhu and Yiming Hu, **"SurePath: An Approach to Resilient Anonymous Routing,"** International Journal of Network Security (IJNS) Mar. 2008.

[4] Nikita Borisov, and Jason Waddle, **"Anonymity in Structured Peer-to-Peer Overlay Networks,"** Technical report, UC Berkeley, May 2005.

[5] Michael Kinateder, Ralf Terdic, and Kurt Rothermel, **"Strong pseudonymous communication for peer-to-peer reputation systems,"** ACM Symposium on Applied computing, Mar. 2005.

[6] Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr, **"Towards an Analysis of Onion Routing Security,"** In Proc. of PET, July 2001.

[7] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, **"Low-resource Routing Attacks Against Anonymous Systems,"** Technical Report CU-CS-1025-07, University of Colorado at Boulder, Feb 2007.

[8] Paul F. Syverson, David M. Goldschlag, and Michael G. Reed, **"Anonymous Connections and Onion Routing,"** IEEE Journal on Selected Areas in Communication, Special Issue, 1998.

[9] Michael K. Reiter and Aviel D. Rubin, **"Crowds: anonymity for Web transactions,"** ACM Transactions on Information and System Security, 1998.

[10] Michael J. Freedman and Robert Morris, **"Tarzan: a peer-to-peer anonymizing network layer,"** ACM CCS, Nov. 2002.

[11] Roger Dingledine, Nick Mathewson, and Paul Syverson, "**Tor: The Second-Generation Onion Router**," USENIX Security Symposium, Aug. 2004.

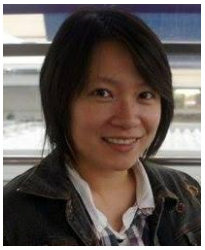
[12] Li Zhuang, Feng Zhou, Ben Y. Zhao, and Antony Rowstron, **"Cashmere: Resilient Anonymous Routing,"** 2nd USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2005.

[13] Aameek Singh, Bugra Gedik, Ling Liu, **"Agyaat: Mutual Anonymity over Structured P2P Networks,"** In Emerald Internet Research Journal (Special Issue on Privacy and Anonymity in the Digital Era), VOL. 16, ISSUE 2, 2006.

[14] Stevens Le Blond, et al., **"Towards Efficient Traffic-Analysis Resistant Anonymity Networks,"** in Proc. of Proceedings of the ACM SIGCOMM 2013, PP. 303-314.

[15] Sahai and B. Waters, **"Fuzzy Identity-Based Encryption,"** In Eurocrypt 2005, LNCS 3494, pp. 457-473, Springer-Verlag, 2005.

AUTHOR BIOGRAPHY



Chia-Chen Wu received her M.S. degree in computer science from the Computer Science Department at National Chiao-Tung University in 2008. She is interested in routing security, elliptic curve cryptography. Contact her at chiachen.cs95g@gmail.com

Yu-Lun Huang received the B.S., and Ph.D. degrees in Computer Science, and Information Engineering from the National Chiao-Tung University, Taiwan in 1995, and 2001, respectively. She has been a member of Phi Tau Phi Society since 1995. She is now an associate professor in the Department of Electrical & Computer Engineering of National Chiao-Tung University (NCTU). She is now the Associate Dean of NCTU Academic Affairs, Director of Center for Continuing Education and Training at NCTU, and Director of Center for Teaching and Learning Development at NCTU. She has been serving the Secretary General of Taiwan Open Course Consortium since 2014. Her research interests include wireless security, virtualization security, embedded software, embedded operating systems, risk assessment, secure payment systems, VoIP, QoS and critical information infrastructure protection (CIIP), IoT Security, LTE Security, creative and innovative teaching model, etc.

Shiuhpyng Shieh received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, respectively. He is a distinguished professor and past chair of the Department of Computer Science, NCTU; and the Director the Taiwan Information Security Center at NCTU. He is an IEEE fellow and ACM Distinguished Scientist. Dr. Shieh is a Senior Member of IEEE, a steering committee member of ACM SIGSAC, and an editor of IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Reliability, Journal of Computer Security, and is also a former editor of ACM Transactions on Information and System Security, IEEE Internet Computing, and Journal of Information Science and Engineering. Contact him at ssp@cs.nctu.edu.tw

A Density-Based Clustering Method for Machinery Anomaly Detection

Jing Tian
University of Maryland
jingtian@calce.umd.edu

Michael H. Azarian
University of Maryland
mazarian@calce.umd.edu

Michael Pecht
University of Maryland
pecht@calce.umd.edu

Abstract - Anomaly detection is a critical task in condition-based maintenance of machinery. In many applications clustering-based anomaly detection is preferred due to its ability to analyze data which may not follow a well studied distribution and are unlabeled. This paper introduces a density-based clustering method for machinery anomaly detection. This method assumes that the data from healthy states are located in regions with high densities and the data from faulty states are located in low density regions. By finding the boundaries of these regions, data from the anomalous states can be identified. The values of the densities for healthy machinery and faulty machinery are evaluated. The rate of change of the density from healthy to faulty is identified as a fault threshold. This method can be valuable for applications where faulty data are too difficult or costly to acquire.

Keywords - anomaly detection, clustering, machinery, feature extraction, machine learning

I. INTRODUCTION

Rotating machinery such as bearings and gears are widely used in electromechanical systems like computer cooling fans, wind turbines, and induction motors. Machinery failures have been a research focus due to their frequency and criticality. For example, in induction motors, bearing failures account for more than 40% of the system failures [1]. In wind turbine, where availability is a major concern, gearbox failure is the top contributor for system downtime [2]. Repairing or replacing failed machinery can require costly maintenance, not to mention the cost of the consequent system downtime.

A machinery fault is an abnormal condition that leads to the failure of the machinery, which is a state in which the machinery cannot perform its required function. Commonly observed faults in bearings include pits, indents, and wear. For gears, pits, root crack, wear and missing teeth are typical faults. In most cases, when a fault emerges, the machine can still perform its required function until the fault develops to a certain degree. Usually there is a time gap between the emergence of a fault and the failure. If faults can be detected at an incipient stage and if their development can be monitored, prognostics and health management (PHM) can be performed to reduce the failure frequency and severity as a result of optimized maintenance.

In-situ monitoring is preferable for PHM of machinery because it provides non-intrusive monitoring during the actual life cycle of the machinery. Widely used in-situ monitoring data of machinery include vibration acceleration signals and current signals of the motor that is linked with the machinery. For example, if a fault develops on a computer cooling fan bearing, the vibration profile of the cooling fan will be changed, which can be monitored by an accelerometer. If the fault leads to an increase of friction in the bearing, the current profile would be also changed. By analyzing vibration signals and current signals, the fault can be detected. To analyze the raw signal, fault features are extracted. Commonly extracted features are statistical characteristics of the signal, such as peak-to-peak, rms, and kurtosis [3] of the signal's amplitude in the time domain, characteristic frequency components in the frequency domain, and wavelet coefficients and empirical mode decomposition energy in time-frequency domain. Usually a single feature is not adequate to reflect the machinery health conditions, and multiple features are extracted.

These features reflect different aspects of the health conditions of the machine. They need to be analyzed together to determine whether some data points are anomalous. The assessment is achieved by anomaly detection.

Anomaly detection techniques include classification-based techniques, nearest neighbor-based techniques, statistical techniques, and clustering-based techniques [4]. Classification-based anomaly detection techniques construct classes of healthy and anomalous states from labeled data. An anomaly is detected if a test point is classified as belonging to an anomalous class. Representative methods include support vector machine [5] and hidden Markov model [6]. These techniques require training data from the faulty system, which are often unavailable. Nearest neighbor-based anomaly detection techniques assume that anomalies occur far from the nearest neighbors in the healthy reference data. A

representative method is k-nearest neighbor [7]. Outliers in the healthy reference data may lead to false negative errors since they can be regarded as close neighbors by an anomaly. Also, these techniques do not consider the influence of the distribution of the data on anomaly detection. Statistical anomaly detection techniques assume that anomalies occur in the low probability regions of a stochastic model of the healthy data. These techniques rely on the assumption that the data follow certain distributions. However, real data may not follow these distributions. Representative work includes nonparametric statistical analysis [8]. Clustering-based techniques assume that normal data points and faulty data points belong to different clusters. Clustering techniques such as *k*-means algorithm [9] are applied to partition the data into clusters. Clusters for faulty data are identified by evaluating properties of the clusters. In this paper, the research focus is on clustering-based techniques because of the following merits. First, labeled data are not required, and thus these techniques address a practical challenge that healthy data and faulty data are often mixed without labels. Second, they are robust to outliers. Third, some clustering techniques do not require the data to follow particular statistical distributions.

A variety of criteria have been developed to identify the clusters of anomalies. One criterion assumes healthy data are close to healthy clusters, while anomalous data are far from healthy clusters. For example, the *k*-means algorithm partitions the data into clusters according to the mutual distances between the data points. Close data points are grouped into the same cluster. If we know the healthy clusters, other clusters are anomalies. To apply this method, healthy clusters must be known in advance, and the number of clusters should be pre-determined.

It has been observed in experiments and field data that healthy data and faulty data have different densities. This observation is explored in this paper, and an anomaly detection method is developed based on a density-based clustering.

II. THEORETICAL BACKGROUND OF DENSITY-BASED CLUSTERING

In density-based clustering, for each object of a cluster, the neighborhood of a given radius has to contain a minimum number of data points (MinPts), and if this requirement is satisfied, a cluster is initiated [10], [11]. Following this idea, some popular density-based clustering methods have been developed, including density-based spatial clustering of applications with noise (DBSCAN) [12], and generalized density-based spatial clustering of applications with noise (GDBSCAN) [13]. Both methods require the user to input two parameters: MinPts and the radius of the neighborhood. These two algorithms face two challenges. First, there is no guideline to determine the radius of the neighborhood. Second, if clusters have a large difference in densities above a certain value, these methods may fail.

When a healthy machine becomes faulty, the data can exhibit a sharp decrease of density and therefore DBSCAN and GDBSCAN are not suitable to separate the healthy and faulty data. Ordering Points to Identify the Clustering Structure (OPTICS) [10] was developed as a generalization of DBSCAN. It does not need the radius of the neighborhood as an input and it can partition clusters with a large difference in densities.

The OPTICS algorithm works by ordering all data points in a sequence according to two distances, namely core distance and reachability distance. Given a data point p, if MinPts are found in its neighborhood within a radius of ε, p is called a core point. The minimum ε that enables p to be a core point is called the core distance. The reachability distance of point q to p is their Euclidean distance or the core distance of p. The reachability distance is the larger of the two distances.

The reachability distance can be regarded as a measure of density. A larger reachability distance means a smaller density. Clusters are usually separated by sparse regions, which result in high value of reachability distances, so the peaks of the reachability distance can be used to identify the boundaries of the clusters.

Identification of the clusters with different densities using the reachability distance is illustrated in Fig. 1.

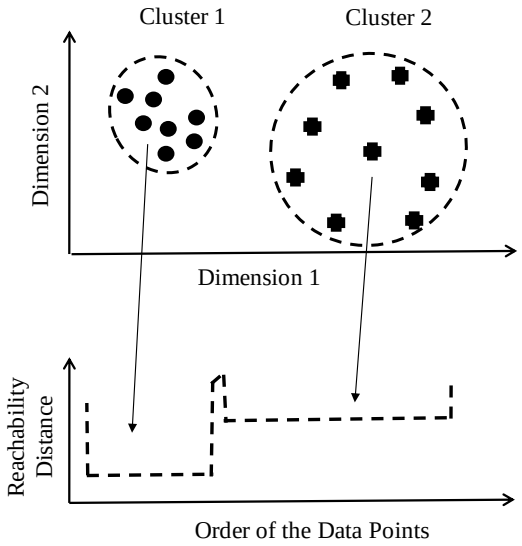


Fig. 1. Identification of clusters using reachability distance

.

III. ANOMALY DETECTION METHOD USING DENSITY-BASED CLUSTERING

When a machine is healthy, it behaves in a consistent pattern where the features extracted from health monitoring signals are distributed with small variances. Therefore, the healthy data form dense clusters. When the machine begins to degrades, its behavior deviates from being normal, and the features extracted from the signals are distributed with shifted mean and larger variances. As a result, the anomalous data form sparse clusters. By estimating the density of the data, anomalies can be detected. However, in the available literature there is no density-based anomaly detection method for the situation where the healthy and anomalous data are mixed. In this research, OPTICS is applied to fill this research gap.

To apply OPTICS in anomaly detection, raw signals should be processed so that the features representing different aspects of the machinery healthy state are extracted and their correlations are reduced. OPTICS is then applied to combine

the features to make an aggregated evaluation. This procedure is realized by the anomaly detection method of this paper.

The method consists of six steps. At first, health monitoring signals are selected according to their sensitivity to the fault and their availability for in- situ monitoring. For example, in computer cooling fan bearing monitoring [14], vibration acceleration signals and motor current signals are usually monitored because they are sensitive to bearing faults, and they can be monitored in-situ.

In the second step, statistical features such as rms and kurtosis of the vibration signals that represent different aspects of the health conditions are extracted. The statistical features have different scales, and they are correlated and may be high-dimensional. Therefore they are normalized in the third step using techniques such as Z-score. In the fourth step, dimensionality reduction technique such as principal component analysis (PCA) is applied to generate fault features that have reduced correlation and dimensionality. These three steps are regarded as a feature extraction module that transforms raw signals to a feature space within which clustering can be performed. In the fifth step, the OPTICS algorithm is applied to partition the data into dense and sparse clusters. In the final step, decisions about the health states are made based on the densities of the clusters.

The framework is illustrated in Fig. 2.

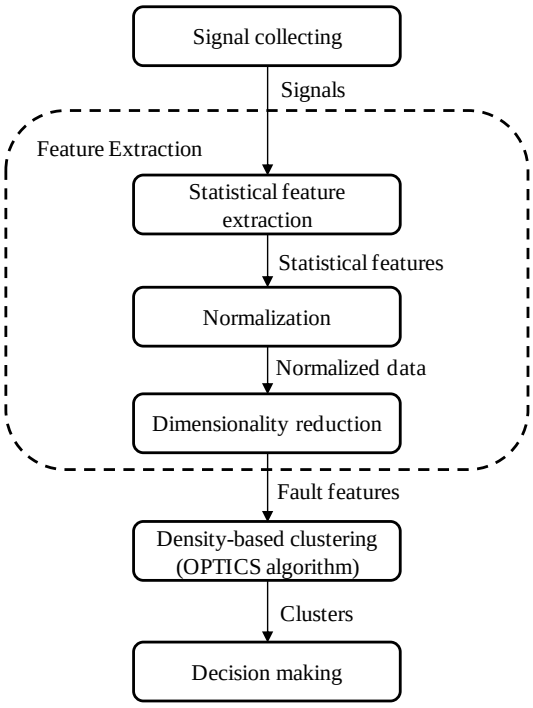


Fig. 2. Framework of the methodology

IV. EXPERIMENTAL STUDY

The density-based clustering anomaly detection method developed in this research was evaluated with the data from a cooling fan accelerated life experiment, which was described in [14, 15].

A. Experimental Setup

A new cooling fan with a ball bearing was tested. Normally, the ball bearing was lubricated by grease and oil. To accelerate the test, the bearing was only lubricated by oil. After an initial measurement, the cooling fan was run at its rated speed of 4,800 rpm in a chamber at the fan's rated maximum operating temperature of 70℃.

Vibration acceleration signals and motor current signals were collected after the following time intervals: 0 hours, 8 hours, 16 hours, 24 hours, 48 hours, and 72 hours. For each measurement, the cooling fan was run at room temperature of about 20℃, and 10 seconds of signals were collected at a sampling rate of 102,400 Hz for both the vibration signal and the motor current signal. At the end of the test, there were 60 seconds of data consisting of 6144,000 data points. The collected signals formed a 6,144,000 by 2 matrix. Each row is an observation, and each column is a signal.

B. Feature Extraction

At first, observations of the signals were segmented sequentially. Each segment has 20,480 observations, equal to 0.2 seconds of measurement. Altogether there were 300 segments. Vibration features and motor current features were extracted from each segment. Five commonly used time domain statistics were used as features, as listed in Table I.

Table I. STATISTICAL FEATURES

Signals	Vibration	Current
Features	rms	rms
	Kurtosis	Standard deviation
	Peak-to-peak	-

A 300 by 5 matrix of statistical features was extracted, where there were 300 observations for each of the 5 statistical features. The first 10% of the observations (30 observations) were used as reference data to set up a baseline. The mean and standard deviation of the reference data were calculated, and the whole 300 observations were normalized by calculating Z-scores referring to the mean and standard deviation of the reference data.

An analysis of the Pearson's correlation coefficients of the reference data shows that some of the statistical features are highly correlated, and PCA was applied to reduce the correlation. The first three PCs account for 98.8% of the total variance. The remaining two PCs account for 1.2% of the total variance, so discarding them would not result in any significant loss of information. The result is shown in Fig. 3. The reference data were concentrated in a dense region within the circle in Fig. 3.

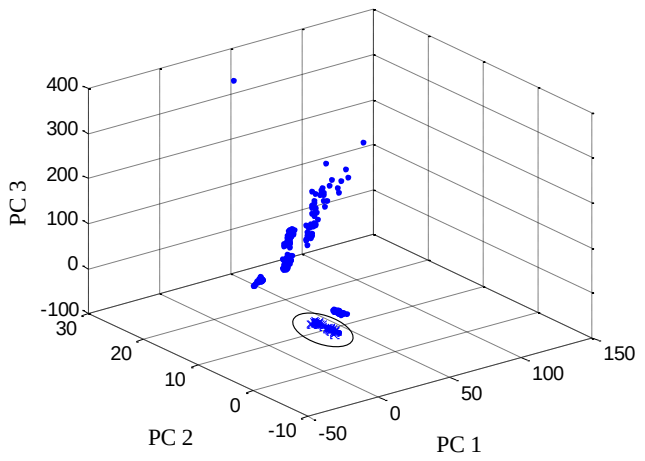


Fig. 3. Scatter of the extracted fault features

C. Anomaly Detection Using Density-Based Clustering

The density-based clustering algorithm OPTICS was applied to the extracted 300 by 3 matrix in the feature space.

In the initial measurement at 0 hours, 50 observations were collected in the features space. We assume at least more than half of the observations, such as 30 observations, can be regarded as healthy, and these healthy observations can form a cluster, so at least 10% of all the 300 observations should be able to form a cluster. Therefore, we chose 10% of the data size as MinPts.

After the analysis of OPTICS, the data were rearranged that the points connected by the similar reachability distance were ordered together. The order-reachability distance plot is shown in Fig. 4. The *y* axis is the value of the reachability distance, which is the reciprocal of the density. Each valley is a cluster, and the peaks are boundaries between the clusters.

From Fig. 4, we can identify at least 5 clusters. The first cluster contains the reference data, so this cluster was used to represent the healthy state. The second and third clusters have smaller reachability distances. In other words, they have higher densities, so they are not regarded as faulty. The last two clusters have much larger reachability distances. These are two sparse clusters, and they are likely to be faulty.

Using the reachability distance as a health indicator, an anomaly detection threshold can be defined based on the empirical distribution of the first cluster, which represents the healthy state. Using 99th percentile, the threshold was calculated to be 9.83. After the 151st observation, reachability distances of all the observations are larger than this threshold. Therefore, cluster 4 and cluster 5 in Fig. 4 are the two anomalous clusters. Cluster 4 corresponds to the data collected after 24 hours of test, and cluster 5 corresponds to the data collected after 48 and 72 hours of test.

V. Conclusions

A density-based anomaly detection method was developed in this paper. With appropriate fault feature extraction, the clustering technique is able to partition the data into clusters according to the density of the data, and a density measure named reachability distance is extracted as a health indicator. By examining this health indicator, clusters of anomalous data

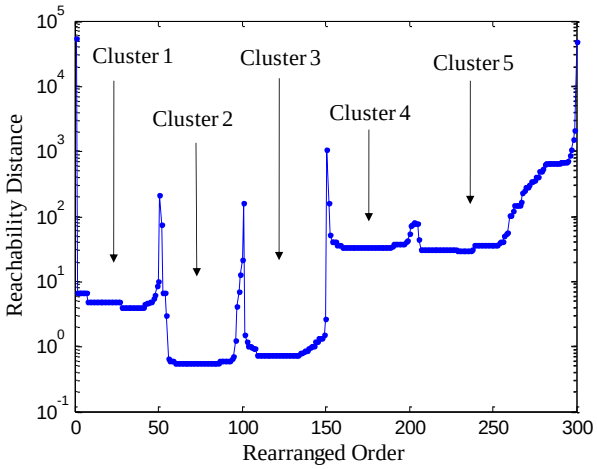


Fig. 4. Clustering Based on Reachability Distances

can be identified. This study evaluated the feasibility of using the cluster density of the health monitoring data to detect machinery anomalies. The density-based anomaly detection method developed in this research provides a novel approach to detect anomalies. Unlike distance-based anomaly detection method, where only the distance between the test data and the healthy reference data is used as a measure of health, the density-based method also analyzes the relationship inside the test data for anomaly detection. Therefore, this method is more robust. The method is unsupervised, so labeled training data are not required. It is suitable for application where faulty data are unavailable. Future work includes optimizing the minimum number of data points for OPTICS in anomaly detection.

Acknowledgment

The authors would like to thank the more than 100 companies and organizations that support research activities at the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland annually. Also special thanks go to the members of the Prognostics and Health Management Consortium at CALCE for their support of this work.

References

[1] C. Bianchini, F. Immovilli, M. Cocconcelli, R. Rubini, and A. Bellini, “Fault detection of linear bearings in brushless AC Linear motors by vibration analysis,” IEEE Tranactions on Industrial Electronics., vol. 58, no. 5, pp.1684-1694, 2011.

[2] H. Link, W. LaCava, J. van Dam, B. McNiff, S. Sheng, R. Wallen, M. McDade, S. Lambert, S. Butterfield, and F. Oyague,“Gearbox reliability collaborative project report: findings from phase 1 and phase 2 testing”, NREL Report, No. TP-5000-51885, 2011.

[3] D. Siegel, C. Ly, and J. Lee, “Methodology and Framework for predicting helicopter rolling element bearing failure”, IEEE Transactions on Reliability, vol. 61, no. 4, pp. 846-857, 2011.

[4] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, pp. 15, 2009.

[5] M. Hejazi and Y. P. Singh, “One-class support vector machines approach to anomaly detection,” Applied Artificial Intelligence, vol. 27, pp. 351-366, 2013.

[6] G. Georgoulas, M. O. Mustafa, I. P. Tsoumas, J. A. Antonino-Daviu, V. Climente-Alarcon, C. D. Stylios, et al., "Principal Component Analysis of the start-up transient and Hidden Markov Modeling for broken rotor bar fault diagnosis in asynchronous machines," Expert Systems with Applications, vol. 40, pp. 7024-7033, 2013.

[7] M. Xie, J. K. Hu, S. Han, and H. H. Chen, "Scalable hypergrid k-NN-based online anomaly detection in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 24, pp. 1661-1670, 2013.

[8] R. F. Luo, M. Misra, S. J. Qin, R. Barton, and D. M. Himmelblau, "Sensor fault detection via multiscale analysis and nonparametric statistical inference," Industrial & Engineering Chemistry Research, vol. 37, pp. 1024-1032, 1998.

[9] J. Zhao, K. Liu, W. Wang, and Y. Liu, "Adaptive fuzzy clustering based anomaly data detection in energy system of steel industry," Information Sciences, vol. 259, pp. 335-345, 2014.

[10] M. Ankerst, M. M. Breunig, H. P. Kriegel, and J. Sander, "OPTICS: ordering points to identify the clustering structure," ACM SIGMOD Record, vol. 28, no. 2, pp. 49-60, 1999.

[11] M. Daszykowski, B. Walczak, D. L. Massart, "Looking for natural patterns in analytical data. Part 2. Tracing local density with OPTICS," Journal of Chemical Information and Computer Sciences, vol. 42 pp. 500-507, 2002.

[12] M. Ester, H. P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," Proceedings of KDD 96, Portland OR, pp. 226-231, August 2-4, 1996.

[13] J. Sander, M. Ester, H. P. Kriegel, and X. Xu, "Density-based clustering in spatial databases: The algorithm gdbscan and its applications," Data Mining and Knowledge Discovery, vol. 2 no. 2, pp. 169-194, 1998.

[14] H. Oh, M. Azarian, and M. Pecht, "Estimation of fan bearing degradation using acoustic emission analysis and Mahalonabis distance," MFPT: The Applied Systems Health Management Conference 2011, Virginia Beach, Virginia, May 10-12, 2011.

[15] Q. Miao, M. H. Azarian, and M. Pecht, "Cooling fan bearing fault identification using vibration measurement," IEEE: International Prognostics and Health Management Conference, Denver CO, June 21-23, 2011.

AUTHOR BIOGRAPHY

Jing Tian received the B. Eng degree in Machinery Design and Manufacturing and Automation from the University of Electronic Science and Technology of China. He is a Research Assistant doing Ph.D. research at the Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park. His sponsored research projects include drive train data analysis for condition-based maintenance, prognostics and health management (PHM) algorithm development, and machinery anomaly detection. Prior to joining CALCE in 2010, he had worked as an engineer and researcher for 7 years, where he performed data analysis and design work on several rugged computer products, which have been well accepted by the market. His research focuses on machine learning and its application in PHM.

Michael H. Azarian received the B.S.E. degree in chemical engineering from Princeton University and the M.E. and Ph.D. degrees in materials science and engineering from Carnegie Mellon University.

He is a Research Scientist with the Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park. Prior to joining CALCE he spent over 13 years in industry. His research focuses on the analysis, detection, prediction, and prevention of failures in electronic and electromechanical products. He is the holder of five U.S. patents.

Dr. Azarian is co-chair of the Miscellaneous Techniques subcommittee of the SAE G-19A standards committee on detection of counterfeit parts. He has previously held leadership roles in various IEEE reliability standards committees and co-chaired iNEMI's Technology Working Group on Sensor Technology Roadmapping. He is on the Editorial Advisory Board of Soldering & Surface Mount Technology.

Michael Pecht received the M.S. degree in electrical engineering and the M.S. and Ph.D. degrees in engineering mechanics from the University of Wisconsin, Madison.

He is the Founder of the Center for Advanced Life Cycle Engineering, University of Maryland, College Park, where he is also a George Dieter Chair Professor in mechanical engineering and a Professor in applied mathematics. He has consulted for over 100 major international electronics companies. He has written more than 20 books on electronic-product development, use, and supply chain management and over 400 technical articles.

Dr. Pecht is a Professional Engineer and a fellow of ASME and IMAPS. He is the editor-in-chief of IEEE Access. He was the recipient of the IEEE Reliability Society's Lifetime Achievement Award, the European Micro and Nano-Reliability Award, the 3M Research Award for electronics packaging, and the IMAPS William D. Ashman Memorial Achievement Award for his contributions in electronics reliability analysis.

Submission Instructions

Authors should use the designated IEEE Reliability Manuscript Central Website to summit their papers. Please refer to the following steps to submit your papers:

1. Login to IEEE Reliability Manuscript Central. If you have no account, sign up for one.
2. Click "Authors: Submit an article or manage submissions".
3. Please click "CLICK HERE" at the bottom of this page, and you will be brought to the five-step submission process.
4. You need to 1) choose the section that you are going to submit your paper to; 2) complete the submission checklist; 3) enter the comments for the editor, which is optional; 4) save and continue.
5. If you have any supplementary files, please upload them in step 4.

Manuscript Types

Manuscripts for regular issues fit within the scope of the magazine, but are not intended for a special issue. Special issue manuscripts cover a specific topic scheduled on our editorial calendar. Please select the appropriate issue (manuscript type) when uploading your manuscript. For more information and to see upcoming special issue topics, see our Editorial Calendar at http://rs.ieee.org/reliability-digest/author-guidelines.html.

Typing Specifications

The manuscript should be written in Times New Roman in a double-column format. The typical length of the submitted manuscript is 4 single-spaced pages. The text portion of the manuscript should be in 10-point font and the title should be in 24-point font, bold.

Manuscript Length

The typical length of the submitted paper is 4 pages, including text, bibliography, and author biographies. Please note that proper citations are required.

Illustrations

The illustrations in the articles must be cited in the text and numbered sequentially. Captions that identify and briefly describe the subject are needed as well. In order to avoid dense and hard-to-read illustrations, graphs should show only the coordinate axes, or at most the major grid lines. Line drawings should be clear. To prevent potential layout problems from happening, related figures described within the same section of text should be grouped together as parts (a), (b), and so on.

References

All manuscript pages, footnotes, equations, and references should be labeled in consecutive numerical order they are mentioned in the text. Figures and tables should be cited in text in numerical order.

Biographical Sketch

A brief biographical sketch should contain the full title of the paper and complete names, affiliations, addresses, and electronic mail addresses of all authors. The corresponding author should be indicated.

Please provide a short biography and a picture for each author of your paper at the end of your paper. The short biography should contain no more than 150 words

Copyright

IEEE Reliability Society owns the copyrights of the articles published in Reliability. If you wish to reproduce the copyrighted materials, please contact us and seek the permissions. The contents on this website can be referenced with proper citation.

Special Issue Proposal Submissions

For a special issue in Reliability, experts are welcome to serve as our guest editors. To know more information, please contact Editor-in-Chief on Reliability, Shiuhpyng Shieh: ssp@cs nctu.edu.tw.