Sankardas Roy

Department of Computer Science, Phone: 1-(419)-372-2342
Bowling Green State University, Bowling Green, Ohio E-mail: sanroy@bgsu.edu

---

CURRENT POSITION

Assistant Professor
Department of Computer Science,
Bowling Green State University, Bowling Green, Ohio

EDUCATION

George Mason University, Fairfax, Virginia

Ph.D., Information Technology, September 2002 - November 2008

- Dissertation: "Secure Data Aggregation in Wireless Sensor Networks (WSNs)"
- Advisors: Prof. Sushil Jajodia, and Prof. Sanjeev Setia

Indian Statistical Institute, Kolkata, India

M.S., Computer Science, July 1999 - May 2001

- Dissertation: "A Hybrid Approach in Applying SVD for Image Compression"

Bengal Engineering College, WB, India

B.S., Electrical Engineering, July 1993 - May 1997

PROFILE

My research interests are in **security and computer networks** with emphasis on:

- Static analysis for security vetting of Android Applications
- Security and Privacy Issues of In-network Data Aggregation in WSNs
- Application of Game Theory for Cybersecurity
- Scheduling and Routing Protocols for DTNs, MANETs, etc.

Career Highlights:

- One book chapter and twenty refereed papers in reputed journals and conferences.
- Received more than 700 citations as listed on Google Scholar.
- Worked as an Instructor and Research Associate in 2012-2015 at K-State, USA.
- Worked as an adjunct faculty member in 2010-2012 at Howard University, USA.
- Mentored to graduate students at KSU and at University of Memphis, USA.

RESEARCH EXPERIENCE

Instructor & Research Associate **August 2012 - July 2015**
Department of Computing & Information Sciences, K-State, Manhattan, KS
Project 1: **Smart Phone Security**
Sponsor: Kansas State University (K-State)

- Static analysis for security vetting of Android Apps: The focus is on detecting vulnerable or malicious Android apps. We designed a flow-sensitive and context-sensitive static analysis algorithm. Our algorithm can precisely determine if the communication between two components (e.g., Activity C1, Broadcast Receiver C2, etc.) of the app contains any sensitive data, which is an important step forward from the status quo of the related field of research. Note that the previous best tool can only determine which components are reachable from a particular component. We built an analyzer tool named *Amandroid* that generates a precise inter-component data flow graph (IDFG) of the app. We demonstrated that IDFG enables Amandroid to detect a wide range of problems. For instance, by perform-

ing taint analysis, Amandroid can accurately find data leakage (if any), such as the GPS location or the app user's password being sent to the network, and so on. Furthermore, Amandroid can find data injection problems (e.g. *intent injection*) and vulnerable usage of critical APIs (e.g., crypto APIs) in an app. Our research paper discussing the above work has appeared in ACM Conference on Computer and Communications Security (CCS 2014), which is a top security conference.

Project 2: **Developing / Teaching CyberSecurity Curriculum**
Sponsor: The National Science Foundation (NSF)

- Designing and offering courses on cybersecurity for a wide range of students: The focus is building cybersecurity curriculum for students with varied backgrounds. The intended audience spans over at least two institutes namely, U.S. Army Command and General Staff College (CGSC) at Ft. Leavenworth and Kansas State University. We completed development of a course called Practical Cyber Security (CIS 490). In Spring 2013, I offered this course at KSU, which is being attended by a diverse population of undergraduate students. I also offered a concise version of this course at CGSC three times: in Nov-Dec of 2013, in March-April of 2014, and in May of 2014.

Postdoctoral Researcher **June 2010 - July 2012**
Department of Systems and Computer Science, Howard University, Washington, DC
Project 1: **Scheduling and Routing Algorithms for DTNs**
Sponsor: The National Science Foundation (NSF), and The GENI Project Office (GPO)

- Evaluating GENI (Global Environment for Network Innovation) interface of the ORBIT lab for DTN experiments: GENI is one of the flagship projects of National Science Foundation. In particular, we evaluated the efficacy of OMF (Orbit Management Framework) to instrument and realize a DTN (Disruption Tolerant Network). Our project was the first scientific effort to evaluate OMF from an experimenter's point of view. The main results (including our feedback and recommendation for ORBIT) were presented in the GENI Conference in Boston in 2012. Our other results on scheduling and routing protocols for DTNs were published in IEEE ICC 2012, IEEE Transactions on Vehicular Technology (in 2012), and IEEE Transactions on Communication (in 2013).

Project 2: **P2P overlay to improve Broadcast-based Messaging Service**
Sponsor: The Department of Defense (DoD)

- Pub/Sub on P2P overlay to make Broadcast-based Messaging Service scalable: We added Publish/Subscribe feature to the publicly available P2PP source code, confirming to the P2PSIP protocol. We used a P2P overlay to reduce the messaging overhead in a distributed-agents application compared to solely using a broadcast-based messaging service, such as Apache ActiveMQ. We tested the system on **PlanetLab** involving more than 500 nodes. One document with the **PlanetLab** deployment and experiment results was reported to the sponsor.

Postdoctoral Researcher **May 2009 - May 2010**
Department of Computer Science, University of Memphis, Memphis, TN
Project Topic: **Game Theoretic Approaches to Protect Cyberspace**
Sponsor: The Office of Naval Research (ONR)

- Imperfect Information Stochastic Games for Cybersecurity: Extended prior stochastic game models by relaxing the assumption that the attacker and the defender have

perfect information about the current state of the system. Computed the best strategy for each player. Published one paper in the Fifth International Conference on Information Warfare and Security, 2010.

- Games to Model DDoS Attacks and Potential Defense Mechanisms: Focused on active bandwidth depletion attacks. Built game models to compute the Nash equilibrium that represents the best strategy of the defender. Validated via extensive simulation-based experiments using **NS-3** and emulation-based experiments using the **DETER testbed**. Published the results in the Spring Simulation Multiconference, 2010 and in IEEE CIIS Symposium, 2011. Furthermore, one paper on taxonomy of the current Game-theoretic approaches appeared in the 43rd Hawaii International Conference on System Sciences, 2010.

Postdoctoral Researcher **November 2008 - May 2009**
Department of Computer Science and Engineering, Lehigh University, Bethlehem, PA
Project Topic: **Secure Data Retrieval in Disruption Tolerant Networks (DTNs)**
Sponsor: Defense Advanced Research Projects Agency (DARPA)

- Attribute-based Encryption (ABE) Systems for Secure Data Retrieval in DTNs: Designed an ABE system which could support revocation of compromised users. In particular, constructed a Ciphertext Policy ABE (CP-ABE) scheme which could accommodate a non-monotonic access policy. Also, implemented our construction using the **pairing-based crypto** (PBC) library. One paper with the main results appeared in the ACM SIGMOBILE MobiOpp workshop, 2010.

Graduate Research Assistant **August 2002 - November 2008**
Center for Secure Information Systems, George Mason University, Fairfax, VA

- **Attack-resilient Data Aggregation Protocols for WSNs:** Designed secure algorithms for hierarchical data aggregation in sensor networks to compute important aggregates such as Predicate Sum and Order-statistics. Developed a simulation system, written in Java, to evaluate the secure protocols in presence of attacks. Published the main results in the top networks security venues, such as ACM SASN 2006, SecureComm 2008, Elsevier Ad Hoc Networks Journal (in 2009), and IEEE Transactions on Information Forensics and Security (in 2012 and in 2014).
- **Preserving Privacy during Data Aggregation in WSNs:** Designed a privacy preserving data aggregation protocol that does not leak individual sensed values during the data aggregation process. The proposed protocol is also robust to data-loss. Published this work in (Wiley) Security and Communication Networks (in 2009).
- **Secure Multicast Routing Protocols for Wireless Ad Hoc Networks (MANET):** Assessed the vulnerability of MAODV, a well-known multicast routing protocol. Examined, via a detailed simulation (in C++ using NS-2 simulator), the impact of the attacks and the authentication framework. Published the main results in IEEE SECON 2005, a premiere ad hoc networks security conference.

TEACHING EXPERIENCE

1. Instructor, Kansas State University: Designed and offered an undergraduate course, CIS 490 (Practical Cyber Security)[1] in Spring 2013. Taught a concise version of this course at the U.S. Army Command and General Staff College (CGSC) three times: in Nov-Dec of 2013, in March-April of 2014, and May of 2014.

[1] More information is available at `http://people.cis.ksu.edu/~sroy/cybersec13/cybersec13.htm`

2. Adjunct Faculty Member, Howard University, Washington, DC, 08/2010 - 05/2012.

(a) Taught *Unix Systems Tools* (an undergraduate course) in Fall 2010 and in Fall 2011.

(b) Taught *Scientific Computing for Engineers (with C, Maxima, and Excel)* (an undergraduate course) in Spring 2012. In Spring 2011, co-taught the same course.

3. Guest Lecturer, George Mason University, Graduate Course CS 818 (Wireless Networks Security), Spring 2008.

4. Lecturer, Institute of Engineering and Management (IEM) , Kolkata, India, 01/2002 - 07/2002. Offered undergraduate courses: Theory of Computation, and Design and Analysis of Algorithms.

Technical Skills

Programming: C, C++, Java, Scala, Shell Script, Perl, SQL, ActiveMQ-CPP
Programming IDE: Eclipse, Visual C++ 2010, NetBeans
Scientific/Simulation Tools: Maxima, MATLAB, NS-2, NS-3, WEKA, SPSS, Excel
Operating Systems: Linux, Unix, Windows, Mac, Android
Version Management Tools/Publishing: Git, SVN, LaTeX, Winedt, Dia
Familiarity / Expertise: Network Security Protocols, PlanetLab, DETER, ORBIT lab

Publications

Book Chapters

1. Sanjeev Setia, Sankardas Roy, and Sushil Jajodia. *Secure Data Aggregation in Wireless Sensor Networks.* Wireless Sensor Network Security, J. Lopez, J. Zhou (Eds.), ISBN 978-1-58603-8137, IOS Press, 2008.

Refereed Journal Papers

1. Harkeerat Bedi, Sankardas Roy, and Sajjan Shiva. *Mitigating Congestion-based DoS Attacks with an Enhanced AQM Technique.* Elsevier Journal of Computer Communications (ComCom 2015).

2. Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia. *Attack-resilient Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact.* IEEE Transactions on Information Forensics and Security (TIFS) 9(4): 681-694 (2014).

3. Jiazhen Jhou, Sankardas Roy, Jiang Li, and Yi Qian. *Minimizing the Average Delay of Messages in Pigeon Networks.* IEEE Transactions on Communication 61(8): 3349-3361 (2013).

4. Harkeerat Bedi, Sajjan Shiva, and Sankardas Roy. *A Game Inspired Defense Mechanism against DDoS Attacks.* (Wiley) Security and Communication Networks (2013).

5. Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia. *Secure Data Aggregation in Wireless Sensor Networks.* IEEE Transactions on Information Forensics and Security (TIFS) 7(3): 1040-1052 (2012).

6. Jiazhen Jhou, Jiang Li, Yi Qian, Sankardas Roy, and Kenneth Mitchell. *Quasi-Optimal Dual-phase Scheduling for Pigeon Networks.* IEEE Transactions on Vehicular Technology 61(9): 4157-4169 (2012).

7. M Chuah, P Yang, S Roy, B Sheng. *Performance Evaluation of Dissemination Schemes for Coded Packets in Heterogeneous Sparse Ad Hoc Networks.* Ad Hoc & Sensor Wireless Networks 15 (2-4), 151-181, 2012.

8. Bo Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy, and Lingyu Wang. *Localized Multicast: Efficient and Distributed Replica Detection in Large-scale Sensor Networks.* IEEE Transactions on Mobile Computing 9(7): 913-926 (2010).

9. Sankardas Roy, Mauro Conti, Sanjeev Setia and Sushil Jajodia. *Secure Median Computation in Wireless Sensor Networks.* (Elsevier) Ad Hoc Networks 7(8): 1448-1462,

2009.

10. Mauro Conti, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia and Luigi V. Mancini. *Privacy-preserving Robust Data Aggregation in Wireless Sensor Networks.* (Wiley) Security and Communication Networks 2(2): 195-213, 2009.

Refereed Conference Papers

1. Sankardas Roy, Jordan DeLoach, Yuping Li, Nic Herndon, Doina Caragea, Xinming Ou, Venkatesh Ranganathan, Hongmin Li and Nicolais Guevara. *Experimental Study with Real-world Data for Android App Security Analysis using Machine Learning.* Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2015.

2. Fengguo Wei, Sankardas Roy, Xinming Ou and Robby. *Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps.* Proceedings of the ACM Conference on Computer and Communications Security (CCS 2014).

3. Harkeerat Bedi, Sankardas Roy, and Sajjan Shiva. *Mitigating Congestion-based Denial of Service Attacks with Active Queue Management.* Proceedings of the IEEE Global Communications Conference (Globecom 2013).

4. Jiazhen Zhou, Sankardas Roy, Jiang Li, and Yi Qian. *A Geographical Partitioning-based Pigeon Assignment in a Pigeon Network.* Proceedings of the IEEE International Conference on Communications (ICC 2012).

5. Harkeerat Bedi, Sankardas Roy, and Sajjan Shiva. *Game Theory-based Defense Mechanisms against DDoS Attacks on TCP/TCP-friendly flows.* Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI 2011).

6. Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya and Qishi Wu. *A Survey of Game Theory as Applied to Network Security.* Proceedings of the 43rd Hawaii International Conference on System Sciences(HICSS), 2010.

7. Sajjan Shiva, Sankardas Roy, Harkeerat Bedi, Dipankar Dasgupda, and Qishi Wu. *A Stochastic Game Model with Imperfect Information.* Proceedings of the 5th International Conference on Information Warfare and Security (ICIW), 2010.

8. Qishi Wu, Sajjan Shiva, Sankardas Roy, Charles Ellis, and Vivek Datla. *On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks.* The Spring Simulation Multi-conference (SpringSim), 2010.

9. Sankardas Roy, Mauro Conti, Sanjeev Setia and Sushil Jajodia. *Securely Computing an Approximate Median in Wireless Sensor Networks.* Proceedings of the Fourth International Conference on Security and Privacy in Communication Networks (SecureComm), 2008.

10. Bo Zhu, Venkata Addada, Sanjeev Setia, Sushil Jajodia, and Sankardas Roy. *Efficient Distributed Detection of Node Replication Attacks in Sensor Networks.* Proceedings of Computer Security Applications Conference (ACSAC), 2007.

11. Sankardas Roy, Venkata Addada, Sanjeev Setia, and Sushil Jajodia. *Securing MAODV: Attacks and Countermeasures.* Proceedings of the Second IEEE Comm. Society Conference on Sensor and Ad Hoc Comm. and Networks (SECON), 2005.

Refereed Workshop Papers

1. Mooi Choo Chuah, Sankardas Roy, and I. Stoev. *Secure Descriptive Message Dissemination in DTNs.* Second International Workshop on Mobile Opportunistic Networking (MobiOpp), 2010.

2. Sankardas Roy, Sanjeev Setia, and Sushil Jajodia. *Attack-resilient Hierarchical Data Aggregation in Sensor Networks.* Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor networks (SASN), 2006.

Technical Reports

1. Sankardas Roy, and M. Chuah. Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs. CSE Technical Report, Lehigh University, May, 2009.

Professional Activities

Recently Served as a Technical Program Committee Member for:

- IEEE Consumer Communications & Networking Conference (CCNC 2016)
- IEEE Region 10 Technical Symposium (TenSymp 2015)
- IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2015)
- IEEE GLOBECOM 2014: Comm. and Info. Systems Security (CISS) Symposium.
- 10th Intnl. Conf. on Sec. and Privacy in Comm. Networks (SecureComm 2014).
- International Conference on Game Theory for Security (GameSec 2014).
- IEEE/SAE International Conference on Connected Vehicles & Expo 2013.
- IEEE GLOBECOM 2013: CISS Symposium.
- SecureComm 2013.
- IEEE Vehicular Technology Conference (VTC Fall 2013, VTC Spring 2013).

Recently Served as a Reviewer for:

- IEEE INFOCOM 2015, 2011
- ACM Symp. on Information, Computer and Comm. Sec. (ASIACCS) 2015, 2014
- Annual Computer Security Applications Conference (ACSAC 2014)
- International Conference on Distributed Computing and Networking (ICDCN 2014)
- Elsevier Journal of Information and Software Technology (2014)
- IEEE Transactions on Wireless Communications (2014)
- IEEE Transactions on Parallel and Distributed Systems (2013-2014)
- IEEE Transactions on Cybernetics (2013-2014)
- IEEE Transactions on Vehicular Technology (2013)
- IEEE Transactions on Information Forensics and Security (2012-2013)
- IEEE Transactions on Computational Intelligence and AI in Games (2013)
- Elsevier CoSe 2012
- IEEE Transactions on Mobile Computing (2011-2012)
- IEEE/ACM Transactions on Networking (2011-2012)

Honors and Awards

1. Best Paper Award for "On Modeling and Simulation of Game Theory-based Defense Mechanisms ..." in Spring Simulation Multiconference (SpringSim), 2010
2. CSIS Grad. Research Endowed Assistantship, George Mason University, 2006 - 2007.
3. Provost's High Potential Grad. Assistantship, George Mason University, 2002 - 2005.
4. M.S. with Distinction, Indian Statistical Institute, 2001.