

Pervasive Secure Infrastructures (PSI): Integrating Smart Sensing, Data Mining, Pervasive Networking and Community Computing - ITR Project Report

<http://crewman.uta.edu/psi>

Seamless integration of smart sensors, wireless networks and mobile agents herald a new paradigm of real time information processing and exchange. At PSI, we are working on synergistic and fruitful merging of disparate technologies with the ultimate aim of providing a pervasive secured environment. As part of our initiative, we also envision in building a reconfigurable network appliance for multifunction security.

1 Wireless Sensor Networks

Faculty Involved : Frank Lewis, Kalyan Basu, Sajal Das

Student Members : Jayanta Hajra, Wook Choi

Conserving energy is vital for wireless sensor networks. As part of our strategy in building an intelligent, all pervasive secure environment, we are currently investigating an energy-conserving sensor data collection strategy in wireless sensor networks which is based on the trade-off between coverage and data reporting latency, with the ultimate goal of maximizing the network's lifetime [4]. The basic idea of this strategy is to select in each data reporting round only a minimum number of sensors as data reporters which are sufficient for desired sensing coverage. Sensors that are not responsible for reporting sensed data in the current round, cache their data and wait for the next round; saving crucial sensor energy in the process. In the process, we are investigating such fundamental issues as event detection integrity and data reporting latency which are critical in deploying trade-off based data gathering scheme. For more details, refer to [1,4]

In view of the enormous amount of data being collected from wireless sensors, it is of utmost importance that all data relevant to a given problem be found, related, and processed. Unfortunately, sensor data collected is often conflicting in nature. In this project, we are studying Dempster-Schafer rules of evidence, Bayesian combination of measurements, Fuzzy Logic and Neural Network DSP to make a decision under such conflicting contexts. We have built a testbed for testing of algorithms developed under this grant. It consists of Microstrain sensor nodes and has been implemented on an air conditioning plant at Automation and Robotics Research Institute (ARRI) at UTA. With significant software development, we have also developed an architecture for real-time sensor sampling, processing, and display. For more details, refer to [2,3]

References

- [1] W. Choi, S. K. Das, and K. Basu, "Angle-based Dynamic Path Construction for Route Load Balancing in Wireless Sensor Networks", Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), 2004

- [2] A. Tiwari, "Design and Implementation of Wireless Sensor Networks for Condition Based Maintenance", M.S. Thesis, EE Dept, UTA, May 2004
- [3] A. Tiwari, F.L. Lewis, and S.S. Ge, "Wireless Sensor Networks for Machine Condition Based Monitoring", Proc. Int. Conf. Control, Automation, Robotics, and Vision, invited paper, Kunming, China, Dec 2004, (to appear)"
- [4] W. Choi, P. Shah, and S. K. Das, "Two-Phase Clustering Scheme for Energy-Conserving Delay-Adaptive in Wireless Sensor Networks", Proceedings of ACM MobiQuitous Networking Conference, Boston, Aug 2004

2 Computer and Network Security

Faculty Involved : Sajal Das, Raphael Finkel, Mukesh Singhal

Student Members : Afrand Agah, Wei Zhang, Sumantra Kundu

Wireless sensors deployed in hostile environments require the need for strong security services including confidentiality, integrity and authentication. In this area, we are investigating the application of game theory for intrusion detection in wireless sensor networks. Prevention of denial-of-service (DoS) attack is the prime concern of our research. We have defined a game theoretic framework which encourages cooperation between nodes and provides reputation for them. Nodes with good reputation contribute to the network life and can use the resources while members with bad reputation are gradually excluded from the network. In our approach, we have shown that the game achieves Nash equilibrium for both attacker and sensor network, thus leading to the defense strategy for the network. See reference [1] for more details.

Physical wired technology forms the communication and data backbone of high performance multi-hop wireless sensor networks. The performance of low end diverse wireless devices is closely interlinked with the security and quality of service being offered at the core network. In another related project, we aim to identify and limit malicious activity in such core networks. Our current investigation is on controlling malicious (that can cause DOS) at wired and wireless network routers.

In wired routers, our work is based on RED (Random Early Detection). When the queue size at the router falls in between the pre-defined maximal and minimal threshold, RED randomly picks some packet in the queue at the router to drop. RED can be used to detect misbehaving/malicious flows since the probability of dropping a packet from a particular connection is roughly proportional to its current share of bandwidth through the router. With our new algorithm, TCP throughput can almost utilize 100% of the bandwidth, while with simple RED, only about 26% can be used. This is a work in progress and [3] highlights our approach.

In the same spirit, we are currently working on a prototype architecture for providing an unified and integrated hardware platform for virus screening and content blocking. Such an approach will assist us in thwarting DOS attacks in backbone networks and utilize the bandwidth for legitimate traffic. We plan to initiate a proof-of-concept experiment on a testbed of network processors to identify performance bottlenecks. This extensive and unified approach is a work in progress and [4] embodies our approach.

References

- [1] A. Agah, S. K. Das and K. Basu, "A game theory based approach for security in sensor networks", IEEE International Performance Computing and Communications Conference (IPCC), 2004
- [2] A. Agah, S. K. Das and M. Kumar, "Security Issues in Pervasive Computing", Wireless Information Highways, Idea Group Publication (in press)
- [3] P Chhabra, S. Das, A. John, W.Zhang?, Controlling Security Attacks at Internet gateways:Secure-RED," manuscript in preparation

- [4] S. Kundu, K. Basu, S.K.Das”, A Reconfigurable Network Layer Malware Appliance for Multifunction Security”, Non-disclosure with UTA-TTO

3 Pervasive Computing and Communications

Faculty Involved : Mohan Kumar, Behrooz Shirazi (PICO Lab), Sajal Das
Student Members : Hitha Alex, Pradip De

For efficient and real-time tracking of objects, we are developing a generic, distributed, scalable architecture based on Radio Frequency Identification (RFID) tags that could be globally deployed for implementing inter-organizational transactions of physical tagged objects. Based on our architecture, we have defined location tracking and update protocol for the real-time tracking of the mobile objects. In this project, we are working on a theoretical framework to get a stochastic estimate of the average spread of object distributions and the amount of messaging necessary for a Product Recall based on the concepts of Scale Free Networks and Epidemic Theory. More details about this project is available in [1,2]

Fusion of information arriving from disparate sources and making appropriate decisions is a challenging and laborious task. As part of the PSI project, we are in the process of creating communities of delegents (software agents) to aid in the information fusion aspects of the PSI project. We have identified and are developing delegents to play four different types of roles - perception, comprehension, projection and resolution. A Bayesian based network approach is being used to generate rules for delegent reactions to events. Integration of these rules into communities is expected to address issues of sufficiency and efficiency in identifying particular situations when certain events take place in the environment. For more details, refer to [3,4]

References

- [1] P. De, K. Basu and S. K. Das, "An Ubiquitous Architectural Framework and Protocol for Object Tracking using RFID Tags," Proceedings of ACM MobiQuitous Networking Conference, Boston, Aug 2004
- [2] P. De, "RFID Tracking of Mobile Objects", M.S. Thesis, CSE Dept, UTA, May 2004
- [3] H. Alex, M. Kumar and B. A. Shirazi, "Service Discovery in Wireless and Mobile Networks", Wireless Information Highways, Idea Group Publication (in press)
- [4] M. Kumar, B.A. Shirazi and S. K. Das, "Pervasively Secure Infrastructures (PSI) through Community Computing", Proc of the Texas Workshop on Security of Information Systems, April 2003, College Station, USA, pp. 5-10

4 Machine Learning, Data Mining and Computational Intelligence

Faculty Involved : Diane Cook, Lawrence Holder
Student Members : Jeff Coble, Miatrayee Mukherjee, Caleb Noble

The ability to mine relational data is a crucial challenge in security-related domains. In this project, we are investigating two methods for graph-based anomaly detection that have been implemented using the Subdue system [5]. The first, anomalous substructure detection, looks for specific, unusual substructures within a graph. In the second method, anomalous subgraph detection, the graph is partitioned into distinct sets of vertices (subgraphs), each of which is tested against the others for unusual patterns. In addition, we have introduced a measure of graph regularity called conditional substructure entropy, which defines the number of bits needed to describe an arbitrary substructure's surroundings. We have tested our anomaly-detection

methods using the 1999 KDD Cup network intrusion dataset [4].

As part of the U.S. Air Force program on Evidence Assessment, Grouping, Linking and Evaluation (EA-GLE), a domain has been built to simulate the evidence available about terrorist groups and their plans prior to their execution. We have addressed two different relational learning problems in this domain . First, we attempt to learn patterns distinguishing vulnerability exploitation cases (terrorist attacks) from productivity exploitation cases (legitimate uses). Second, we attempt to learn patterns distinguishing threat groups from non-threat groups. Reference [1,2,3,5] provides more details on these approaches.

References

- [1] L. Holder, D. Cook, J. Coble and M. Mukherjee, "Graph-based Relational Learning with Application to Security", submitted to the Fundamenta Informaticae Journal Special Issue on Mining Graphs, Trees and Sequences, 2004
- [2] L. Holder, "Connecting the Dots: Graph-based Discovery Informatics for Learning Patterns of Asymmetric Threats", Visionary Lecture Series in Discovery Informatics, Johns Hopkins University School of Professional Studies in Business and Education, March 2004.
- [3] C. Noble and D. Cook, "Graph-based Anomaly Detection", Proceedings of the ACM Conference on Knowledge Discovery and Data Mining, 2003
- [4] <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>
- [5] D. Cook and L. Holder, "Graph-based data mining," IEEE Intelligent Systems, 15(2):32-41, 2000.

5 Multi and Stream Databases

Faculty Involved : Sharma Chakravarthy

Student Members : Satyajee Sonune, Altaf Gilani, Laali Elkalifa

With the marked emphasis on monitoring text streams to detect complex patterns or aberrant characteristics, information filtering is the focal point of research in this project. Text stream monitoring and pattern detection have far reaching applications such as tracking information flow among terrorist outfits, web parental control, continuous monitoring of rival websites in e-commerce, and so forth. InfoFilter, a content-based information filtering system being developed for this project, detects complex patterns in text streams that include but are not limited to news feed, email, web pages and caption text from streaming videos. For many applications, pattern characterization is complex and requires an expressive specification than what is currently provided by Information Retrieval Query Languages (IRQLs). In essence, pattern specification and detection play a major role in information filtering. For this project, we are developing InfoFilter, which allows users to specify complex patterns such as sequential or structural patterns, wild cards, word frequencies, proximity, Boolean operators and synonyms using the proposed Pattern Specification Language Psnoop and to detect these patterns using the data flow paradigm over Pattern Detection Graphs (PDGs) [1].

Traditional DBMS were not designed to support the requirements of stream-based applications. They were designed to satisfy to the needs of business data processing applications. A Data Stream Management System (DSMS) termed MavStream is being developed for providing a query execution platform for streaming based application. This is a complete system where in a query, submitted by the user, is processed at the server and the output is returned back to the user. It uses a client server architecture. For more details, refer to [2,3].

References

- [1] L. Elkalifa, "InfoFilter: Complex Pattern Specification and Detection Over Text Streams", MS Thesis, Spring 2004
- [2] Mr. S. Sonune, "Design and Implementation of Window-based Operators and a Scheduler for Steam Data", Fall 2003
- [3] Mr. A. Gilani, "Design and Implementation of Stream Operators, Query Instantiation, and Stream Buffer Manager", Fall 2003