# Protecting Water Bodies and Systems Against Waterborne Biochemical Warfare

Mukesh Singhal
Department of Computer Science
University of Kentucky
Lexington, KY 40506

Yelena Yesha
Department of Computer Science
1000 Hilltop Circle
University of Maryland at Baltimore
Baltimore, MD 21250

**Abstract:** Water bodies and water systems are essential for survival and protecting them against terrorist threats like biochemical warfare agents and against threats from toxic industrial chemicals is of at most importance. This paper will examine the issues in protecting water bodies and water systems against waterborne biochemical warfare. We will also present preliminary ideas on a sensor network-based system to detect and prevent such threats.

**Key words:** Water bodies, water systems, waterborne threats, biochemical warfare, sensors, sensor networks.

## 1. Introduction

Water bodies and water storage and supply systems are essential for human survival. These water bodies and systems are vulnerable to terrorist threats, like biochemical warfare agents, and to threats from toxic industrial chemicals [1, 2, 4-7]. These systems are not adequately protected and there are no real-time technology to detect waterborne biochemical warfare agents and toxic industrial chemicals.

Industrial waste-water discharged into municipal sanitary sewers can pass untreated through the treatment plant and into the drinking water. Water resources and systems are also vulnerable to terrorist attacks by means of biochemical hazards. Current on-site detection typically has a detection limit much higher than that of an infectious dose. Also, the time required for detection is generally much longer than desired, due to time involved in the diffusion process of those agents. Therefore, an exposure may not be recognized until significant damage has occurred.

In this paper, we will examine the issues in protecting water bodies and water systems against waterborne biochemical warfare and also present preliminary ideas on a sensor network-based system to detect and prevent such threats.

## 2. Issues

Protection of water resources and systems against these threats involves addressing of several important issues: (i) development of miniaturized integrated sensors capable of high-sensitivity, real-time detection of multiple biochemical agents with in water bodies, (ii) communication and collection of data, (iii) security in communication of data, and (iv) tools for data analysis and visualization of the information.

## 3. Basic Approach

Basic approach is to design a sensor network that is capable of high sensitivity, real-time detection of multiple biochemical agents with in water bodies and that can react and take preventive or corrective actions in real-time. The front-end of the protection systems includes software and tools for data analysis, processing of the collected data and for visualization of the information. The middle part of the systems consists of a secure networking infrastructure for propagating information from sensor to the front end processing center. The system also includes an automated remote response mechanism.

The analytical demand of such a system will best be met by robust, low-power, network-deployable/addressable micro-sensor systems that will allow quantification of the density of biological and chemical agents and will be able to detect changes in the toxicity of industrial chemical runoffs, farm wastes, and malicious materials as well as to monitor changes in the quality of drinking water, including water in streams, rivers, lakes, etc. [8, 9, 10]. With minimal alteration in the sensor design, such systems can be installed in public buildings, sports arenas, transportation hubs, etc., as well as for use in battlefields and military facilities [3].

## 4. Secure Communication

Providing secure communication between sensors and the front-end processing center is a highly critical and the most challenging task because of high failure, limited energy, and frequently changing network [11-14]. It is also important to prevent an adversarial or compromised sensor node from compromising the security of the sensor networks because of untraceable sensor nodes, and less physical protection. We briefly discuss our initial ideas for security in sensor networks.

A research challenge is to secure the cluster head against threats such as tampering and eavesdropping. Securing the cluster head is more important, because it is responsible for communicating with other cluster heads on behalf of its group. An attacker can take control of the cluster head and then get the private key and decode the encoded data sent by other cluster heads. We will use a technique in which instead of keeping the private key in the cluster head, we will split the key (as partial keys) using a secret function and distribute those among the sensor nodes in the hierarchy. In this model, when a cluster head wants to decode some data, which is encrypted by another cluster head it must accumulate the partial-keys to reform the private key. An attacker will not be able to get the private key by attacking the cluster head and for an adversary to launch an attack in the multiple sensor nodes would be extremely difficult as it requires more resources.

Another important issue is Energy and Communication Efficient Level Security (ECLS) protocol which reduces the communication overhead, computes key dynamically for secure communication and chooses the cluster head based on the coverage of a particular region. ECLS will be scalable and able to handle node failures in the network. For preventing the breaking of the entire network because of a single compromised node ECLS will provide the group key carefully to the authentic nodes and revoke it from compromised node. Two types of levels will be considered in this protocol, one is based on the physical level and the other is data aggregation level. When a data aggregation target (called cluster head) is chosen, the surrounding sensors will collaborate with it to form the group key. For forwarding the data to a different region both encryption and authentication will be used.

Recently, different security protocols have been proposed by different researchers for sensor networks. However most of these protocols are designed to provide uniform security. That means, all the nodes in a network have same level of security. All the nodes may not need to have secure communication all the time. For example, in a water supply facility a sensor network is collecting data of water temperature. If there is any behavior change of the water is sensed (chemical leakage, exposure of biohazard material) then the network dynamically needs to form a secure path to report the event to the control center. The state machine approach is used in the base station to trigger the security events. The session keys are generated to provide different level of security.

Role Based Hierarchical Sensor Network model can provide role-based multilevel security in sensor networks. Each group is organized in such a way that, they can have different roles and based on their roles can have different levels of access. The multilevel security is based on assigned keys to different nodes. To achieve this goal, we organize the network using Hasse diagram then compute the key for each individual node and extend it to construct the key for a group. The reasons for using Hasse diagram to setup the architecture for multilevel access are as follows:

1. The role of each node can be defined and changed dynamically based on the application. The role is assigned by the cluster head of each group.
2. Each node in each group can have different levels of access, and therefore, nodes needs to have different sets of keys.

## 5. Concluding Remarks

Water bodies, resources and systems are also vulnerable to terrorist attacks by means of biochemical hazards and toxic industrial chemicals. Protecting these systems against these threats is of at most national importance. In this position paper, we briefly examined the issues in protecting water bodies and water systems against waterborne biochemical warfare. We also presented our preliminary ideas on a sensor network-based system to detect and prevent such threats. Much work remains to be done in this and we need to develop a comprehensive protection system, test it, and deploy.

## 6. References


1. "Water Security", EPA Website and publications. http://cfpub.epa.gov/safewater/watersecurity/index.cfm
2. Claudia Copeland, "Terrorism and Security Issues Facing the Water Infrastructure Sector", CRS Report for the Congress, Novembre 2008, http://fas.org/sgp/crs/terror/RL32189.pdf.
3. Allan R. Hoffman, "The Connection: Water and Energy Security", http://www.iags.org/n0813043.htm.
4. 2009 Water Security Congress, Washington, DC, April 8-11, 2009, http://www.awwa.org/Conferences/Content.cfm?ItemNumber=753&navItemNumber=3543.
5. "Water Infrastructure Security Enhancements (WISE)", http://www.awwa.org/Resources/Content.cfm?ItemNumber=29824.
6. "Water System Security", DHS Publication, http://www.oregon.gov/DHS/ph/dwp/security.shtml.
7. "Improving the Nation's Water Security: Opportunities for Research", Academic Press, 2007, http://www.nap.edu/catalog.php?record_id=11872.
8. "Water Sensors", Campbell Scientific, http://www.campbellsci.co.uk/index.cfm?id=274.
9. "Water Quality Sensors", http://www.globalw.com/products/waterquality.html.
10. "Revolutionary Water Sensors", http://www.ecoworld.com/blog/editor/guest/2009/03/27/revolutionary-water-sensors/.
11. Eliana, Stavrou, "Wireless Sensor Networks Security Requirements", http://webhosting.devshed.com/c/a/Web-Hosting-Articles/Wireless-Sensor-Networks-Security-Requirements/.
12. Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston, "Security for Sensor Networks", University of Maryland Baltimore County.
13. David Boyle and Thomas Newe, "Securing Wireless Sensor Networks: Security Architectures", JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008.
14. Adrian Perrig, Robert Szewczyk, J. D. *Tygar*, Victor Wen, David E. Culler: *SPINS*: Security Protocols for Sensor Networks, MOBICOM 2001: 189-199.