2d Lt James Marvin

Literature Review

The focus of my research is making software products that use sensor data more secure by using machine learning. My literature review has led me to find examples of this in wireless sensor networks (WSN). WSNs are networks composed of multiple sensor nodes that transmit events to a main repository or sink [1]. The main source I used to learn about them was the paper “Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications” [1]. This source was a great survey paper and directed me to the other related sources I found. It started off by explaining various machine learning algorithms that have been used in sensor networks and their application. This source provided me multiple case studies that I will use to demonstrate how machine learning will make software that relies on sensors more secure.

The first case study I delved into was “Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines” [2]. The problem this case is looking to solve is that common security models and protocols used in wired and other networks are not suited for WSNs because of resource constraints. These resource constraints are mainly computational ability, memory, and power supply. Support Vector Machines work well because detection is done at the base station and not at the nodes, so bandwidth, energy, and memory are less of a concern. Results of this technique showed great detection rate for 100% selective forwarding, good results for 80 percent selective forwarding, and decently accurate for 50 and 30% selective forwarding attacks. This case matters to me because it shows that machine learning models work for implementing security controls on software that receives a plethora of sensor input.

The next case I examined was detailed in the paper “Outlier Detection in Wireless Sensor Networks using Bayesian Belief Networks” [3]. Outlier information is important because outlier can contain important hidden information. This machine learning model was able to accurately categorize outlier events from the sensor data at the sensor level so that it could avoid sending it to the main sink. It was also able to aggregate the outlier data and draw threat predictions from it. This paper provides another solid example of machine learning amplifying input synthesizing.

The next case I looked at “Distributed Event Detection in Wireless Sensor Networks for Disaster Management” [4]. The authors detailed how they used decision trees coupled with a reputation-based voting method for aggregating the detection results of individual sensor nodes and reach a consensus among neighboring nodes. Their results showed a high event detection rate and its low computational complexity was able to save power even though the operations were taking place at the remote sensing level. This provides another avenue for my suite of machine learning solutions to provide to the software developer.

Moving away from use cases I examined some of the resource challenges presented by WSNs and a solution in “An Architecture for Energy Management in Wireless Sensor Networks”[5]. Most of the machine learning models incur a small to significant energy cost to implement on the network. This architecture design helps lower the energy used by the network and would help allow the addition of these machine learning widgets. This is important to my research solution because it aids its practicability.

These are the main resources I’ve found so far to support my idea. Areas that I’m still looking for are technical challenges of adding machine learning support to existing input processing software. Can it be bolted on or does it have to baked in? Another area I haven’t been able to find usable resources in is possible alternatives to machine learning in input security and how they compare to my current direction. I will find resources to answer to these questions by the time the paper is complete.

Sources:

1. Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys & Tutorials*, *16*(4), 1996-2018.
2. Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007, December). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on* (pp. 335-340). IEEE.
3. Janakiram, D., Reddy, V. A., & Kumar, A. P. (2006, January). Outlier detection in wireless sensor networks using Bayesian belief networks. In *Communication System Software and Middleware, 2006. Comsware 2006. First International Conference on* (pp. 1-6). IEEE.
4. Bahrepour, M., Meratnia, N., Poel, M., Taghikhaki, Z., & Havinga, P. J. (2010, November). Distributed event detection in wireless sensor networks for disaster management. In *Intelligent Networking and Collaborative Systems (INCOS), 2010 2nd International Conference on* (pp. 507-512). IEEE.
5. Jiang, X., Taneja, J., Ortiz, J., Tavakoli, A., Dutta, P., Jeong, J., ... & Shenker, S. (2007). An architecture for energy management in wireless sensor networks. *ACM SIGBED Review*, *4*(3), 31-36.