POSTER: Signal Anomaly Based Attack Detection in Wireless Sensor Networks

Jeton Bacaj
Department of Computer Science,
Rochester Institute of Technology
102 Lomb Drive, Rochester, NY 14623
Jxb4803@rit.edu

Leon Reznik
Department of Computer Science,
Rochester Institute of Technology
102 Lomb Drive, Rochester, NY 14623
lr@cs.rit.edu

ABSTRACT
This paper presents a feasibility study of novel attack detection mechanisms in wireless sensor networks (WSN) based on detecting anomalies and changes in sensor signals and data values. Typical WSN attacks are considered in the empirical study of various attack detection techniques utilizing features based on sensor signal strength and other WSN technological parameters and using machine learning classification techniques such as clustering, rule learners, and neural networks. For the attack detection implementation the study employed WSN built from Sun kits available on the market and extended Sensor Network Anomaly Detection System (SNADS) framework of methods and tools.

Categories and Subject Descriptors
D.4.6 [Security]: Protection; K.6.5 [Security]: Protection

General Terms
Measurement, Security.

Keywords
Anomaly intrusion detection; wireless sensor networks.

1. MOTIVATION
Traditionally wireless sensor networks (WSN) security designers consider sensor networks simply as a communication system transmitting information in one direction from sensors to processing units. Based on this assumption most intrusion detection systems expand the signature based and other techniques popular in wireless communication. The fact that sensor networks are a concurrent data acquisition system is not paid a proper attention in intrusion detection. The data collected by sensors as well as sensor signal strengths and other technological parameters are available and could be used for anomaly intrusion detection. This paper's goal is threefold:
1) to investigate a feasibility of the distributed mechanisms of an intrusion detection in WSNs based on detecting anomalies and changes in sensor signals,
2) to promote these methods into the WSN design practice by developing and presenting a unified software framework executable on the sensor network kits available on the market,
3) to present the results of an empirical study of attacks detection, which were based on sensor anomaly detection methods.
Section 2 reviews a number of typical WSN attacks, which were described in publications [1-8] and indicates which of them could be detected with this technique. The detection principles are explained in section 3 in greater detail and their performance in detecting two typical attacks is presented in section 4.

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.

2. ATTACKS OVERVIEW
The attacks studied in literature [1-8] may change the legitimate communication signals that are expected in the WSNs. A sample of typical attacks is presented in Table 1. It should be noted that, for the purpose and scope of this study, the only attacks considered for attack detection deployment are sophisticated attacks, specifically those that do not rely on the WSN having a lack of encryption, authentication, and authorization mechanisms in place. As one can see from Table 1, in the Attack details column, most of these attacks rely on impersonation, passive information gathering (listening in), or state corruption of the sensor signals. A combination of encryption, authentication and authorization access control may alleviate most of these weaknesses but may require significant resources not available in WSN implementations. Last two columns demonstrate that most attacks could be detected by examining certain sensor signals and WSN parameters and their changes.

3. METHODS AND PRINCIPLES OF OPERATION
The detection idea is based on constant monitoring the values of the sensor signals and data communicated in WSN and certain WSN technological parameters, e.g. packet delivery ratio, and identifying anomalies in the patterns of their values or value derivatives. Values and features extracted for further analysis depend on the particular attacks and utilize the signals and values, which are the most dependable on this attack. The developed methods are implemented as an extension to the Sensor Network Anomaly Detection System (SNADS) [9]- see Figure 1 for further details. SNADS is designed as a signal analysis tool to decide whether signal changes should be identified as normal or anomalous. WSN detection mechanism may rely on a priori known model of the environment that the sensors are deployed in.

4. ATTACK DETECTION STUDY
4.1 Jamming attack
A few various WSN technological parameters have been considered as possible features to be used for this attack detection.

Table 1. Typical WSN attacks and their possible detection metrics

Attack name	Attack content	Countermeasures	Possible detection	Possible metrics used for detection
Preliminary or passive attacks				
Passive information gathering	Information interception and collection during communication without altering it	Encryption and access control	No	n/a
Traffic and node activity analysis	Gathering information on sensor activities and traffic patterns. Used for future attack preparation	Encryption and access control	No	n/a
Node subversion by tampering or destruction	Capturing a node. Collecting information available including keys if applicable	Protection and access control	No	n/a
Node malfunctioning	Node malfunctions. Generate inaccurate measurements or violate traffic/ routing	Tests	Yes	Sensor signals or absence thereof
Cluster leader or an aggregate node outage	A node and possibly a part of the network will cease functioning. Generate inaccurate measurements or violate traffic/ routing	Flexible network structuring and re-routing	Yes	Sensor signals or absence thereof
Active attacks				
False node and Byzantine attacks [1,4]	Addition of malicious node by adversary. Inject false data and malicious information	Key distribution and control, node verification	Yes	Sensor signals, network traffic characteristics
Malicious message corruption	Data integrity is violated and if control messages are modified the network functioning could be at risk	Access control and encryption	Yes	Sensor signals
Routing modifications and loops	Routing information is maliciously altered. Network functioning is at risk, more traffic is generated and the resources are wasted	Access control and encryption	Yes	Sensor signals, network traffic characteristics
Sinkhole/blackhole or Wormhole attack	Re-forwarding traffic to a compromised node or through particular low latency links.	Implicit acknowledgment multipath routing	Yes	Sensor signals, network traffic characteristics
Denial of service [6]	Denial of service at the physical level. Radio jamming, battery exhaustion	Depending on the attack, identify jammed regions and rerouting	Yes	Received signal strength, average time required to sense an idle channel and the packet delivery ratio
Denial of sleep [5]	Various DoS attacks on MAC protocols depending on the protocol knowledge, such as sending false messages, increasing collision rates, etc. Significant reduction in wireless sensor network lifetime	Link-layer authentication, anti-replay protection, jamming identification, broadcast attack defense	Yes	Power level monitoring
DoS on Sensing [2]	Physical attacks on the sensor nodes aimed at changing measurements before they enter communication channel. Faulty and corrupted measurements	Special distribution of the sensor nodes across the region with assumed mobility	Yes	Change in sensor signals
Jamming [7]	Corrupting traffic by adding up streams and messages. Bandwidth and other resource exhaustion	Spread spectrum communication if radio resources available, rerouting around jammed areas	Yes	Traffic and sensor signals
Interrogation [6]	Repeatedly sending RTS messages to elicit CTS responses from a targeted node. Node resource exhaustion	Link layer authentication and anti-replay protection	Yes	Node power level
Hello flood	Broadcasting a hello message with stronger transmission power to reach more nodes. Node resource exhaustion	Link layer authentication and anti-replay protection	Yes	Traffic and sensor signals
Sensor stimuli	Subverted nodes send request for more readings. Bandwidth and other resources exhaustion	Monitoring sensor sample rates	Yes	Traffic and sensor signals
Selective forwarding	Malicious nodes drop certain messages. Latency reduction and the neighboring nodes deceive	Key distribution and control, node verification	Yes	Sensor signals, network traffic characteristics
Sybil attack [3,8]	Malicious creation of the node clones. Builds up copies of legitimate nodes to disrupt routing	Key distribution and control, node verification	Yes	Sensor signals, network traffic characteristics

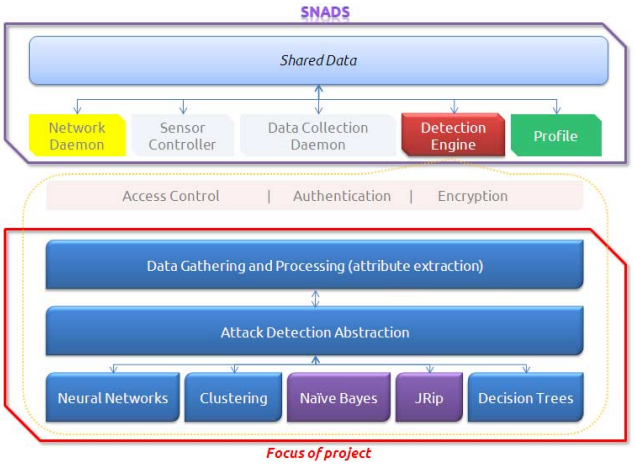

Figure 1. Integration with SNADS framework

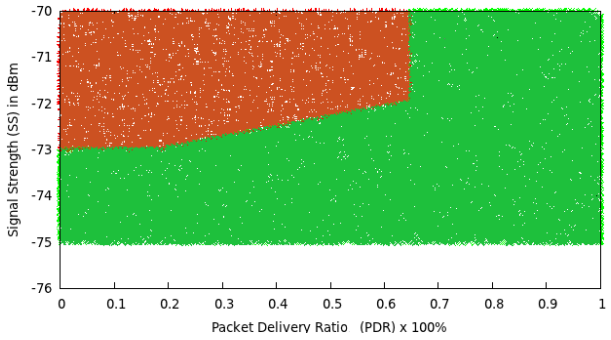

Figure 2. Jamming attack detection data distribution

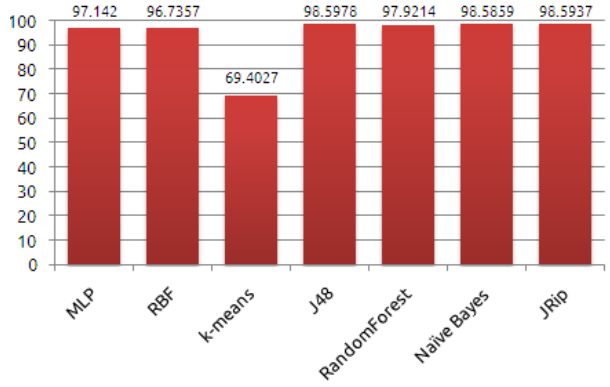

Figure 3. Classification techniques performance in DoS attack detection

One can see from Figure 2 that by using only two WSN technological parameters such as a signal strength and a packet delivery ratio it would be easy to subdivide the whole plane into two distinguish areas: attack's and no attack's [6]. This is valid for different types of Jamming attack manifestations: constant, reactive, deceptive and random jammers.

4.2 Denial of Service on Sensing attack

Seven signals have been identified as features for an anomaly detection. The traffic data were collected from the WSN built from Sun World Spots available on the market [10]. A few different machine learning techniques have been tested to build classifiers for the attack detection. Figure 3 presents their performance that might be considered as quite good but could be further improved by specific measures.

5. REFERENCES

[1] P. Addesso, S. Marano, and V. Matta, "Sequential Sampling in Sensor Networks for Detection With Censoring Nodes," in IEEE Transactions on Signal Processing, vol. 55, November 2007, pp. 5497–5505.

[2] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attacks," IEEE Transactions on Signal Processing, vol. 57, pp. 16–29, Jan. 2009.

[3] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74–81, 2008.

[4] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," in IEEE Transactions on Vehicular Technology, vol. 58, January 2009, pp. 367–380.

[5] A. Czarlinska and D. Kundur, "Distributed Actuation Attacks in Wireless Sensor Networks: Implications and Countermeasures," in DSSNS '06: Proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems. Washington, DC, USA: IEEE Computer Society, 2006, pp. 3–12.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," in IEEE Network, vol. 20, June 2006, pp. 41–47.

[7] J. R. Douceur, "The Sybil Attack," in IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. London, UK: Springer-Verlag, 2002, pp. 251–260.

[8] J. Yin and S. K. Madria, "Sybil attack detection in a hierarchical sensor network," in Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007, Nice, France, September 2007, pp. 494–503.

[9] L. Reznik and K. Nathan, "A Framework for Measurement Anomaly Detection in Sensor Networks," in IEEE Sensors 2009 Conference, Christchurch, New Zealand, October 2009, pp. 597–600.

[10] Sun Microsystems, now Oracle, Inc., "SunSPOTWorld," http://www.sunspotworld.com/.