Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines

Sophia Kaplantzis [1], Alistair Shilton [2], Nallasamy Mani [1], Y. Ahmet Şekercioğlu [1]
[1] *Electrical and Computer Systems Engineering, Monash University*
Clayton, Victoria 3800, Australia, sophia.kaplantzis@eng.monash.edu.au
[2] *Electrical and Electronic Engineering, University of Melbourne*
Melbourne, Victoria 3000, Australia, apsh@ee.unimelb.edu.au

Abstract

Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members. The security models and protocols used in wired and other networks are not suited to WSNs because of their severe resource constraints, especially concerning energy . In this article, we propose a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and sliding windows. We find that our system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy.

1. INTRODUCTION

In recent years WSNs have become a cheap and viable solution for a variety of applications, including monitoring of critical infrastructure (water supplies, power grids, traffic networks, agriculture, telecommunications systems etc.), wildlife habitat monitoring, industrial quality control, disaster recovery situations, military command applications and much more. The miniaturization of sensor nodes and the advances in RF communications have allowed for such a technology to blossom. WSNs are the beginning of a "smart space" revolution, in which tiny devices will interface wireless information technology to our everyday living environments.

It is apparent that for security sensitive applications the stakes are high, as damage to the network may result in harm to the health and safety of people. The most common threats to the security of WSNs include node compromise, eavesdropping, compromise of privacy and Denial of Service (DoS) attacks [1]. Apart from physical damage to the nodes, which may render the network unavailable, attacks that target the data conveyed by the network can also have crippling effects. Such data targeting attacks are manifested via sensor node compromise. Node compromise is facilitated by the fact that sensor networks may include thousands of sensor node members, which are distributed over large areas and are usually deployed with the intention that they will operate in an unattended manner. Eavesdropping is the medium by which an adversary can gain access to private network information, which in turn can be used to harm the network. Eavesdropping is trivial to perform; all you need is to place a wireless receiver in the proximity of two communicating nodes. After the adversary has compromised a few nodes, and used eavesdropping and traffic analysis techniques to access private network data, the adversary can launch DoS attacks. DoS attacks aim to diminish or destroy the functionality of a network and are extremely difficult to protect against and recover from as they leave the network in a state of chaos. It is important to note here that such threats are common in all wireless ad hoc networks. However, the limited resources (memory, bandwidth, energy) associated with the individual sensor nodes in WSNs accentuate such features.

The existence of DoS threats has inspired new research that aims to address the security issues of WSNs, without diminishing their performance. Most of the current research can be slotted into one of the following four categories [2]:

- Key management: Establishing and maintaining cryptographic keys in an energy efficient manner in order to enable encryption and authentication.
- Secure routing: Discovering new protection techniques and applying them to new routing protocols, without sacrificing network connectivity, coverage or scalability.
- Secure services: Includes specialized security services such as data aggregation, localization and time synchronization.
- Intrusion Detection Systems (IDSs): Building simple, specialized systems that are protocol independent and are able to detect specific attacks without consuming excessive amounts of energy or memory.

In this paper, we focus on adapting a simple classification based IDS to detect a specific spectrum of malicious DoS attacks, namely the Selective Forwarding Attack, that may be launched against a WSN. This IDS uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. To the best of our knowledge this is the first attempt to apply SVMs as a solution in a WSN security scenario. We have chosen SVMs over other traditional classification methods, such as neural networks and nearest neighbor classifiers, because SVMs are able to provide very good results (even

for very difficult training tasks) while avoiding the problems of overfitting and the curse of dimensionality that plague many other methods. Also, in order to protect valuable energy resources in the network, we investigate the effectiveness of a centralized WSN security IDS over the many proposed distributed systems, which require additional computational, storage and bandwidth inputs from node members of the network. By centralized, we mean that the intrusion detection task (feature selection, data processing, anomaly detection) is carried out entirely by the base station, without further burdening the sensor nodes or unnecessarily reducing the lifetime of the network.

The remainder of this article is structured as follows; In section 2 we give some background including common threat models in WSNs, IDSs, the characteristic of the Selective forwarding attack and our implemented routing protocol. In section 3 we present related work in the area of intrusion detection for WSNs. In section 4 we highlight the basic concepts behind the one-class SVM classifier. In section 5 we introduce the simulated attack model and our proposed intrusion detection scheme. In section 6 we present the results of our simulation based experiment. Finally, in section 7 we consider future work, and in 8 we conclude the paper.

2. BACKGROUND

Attacks in WSNs take two forms based on the type of hardware the attackers uses to compromise the network [3]; mote-class attackers and laptop-class attackers. Mote-class attackers have access to a few sensor nodes with capabilities similar to those of legitimate sensor nodes. The malicious nodes are usually acquired during node compromise activities. Laptop-class attackers on the other hand have access to more powerful devices such as laptops, PDAs, smart phones, workstations or alike. Such malicious nodes have a great advantage over the genuine network nodes as they have more powerful CPUs, high powered sensitive antennas and larger battery reserves. Furthermore, the attacks themselves can be categorized into outsider and insider attacks. In outsider attacks, the adversary has no special access to network communications but rather needs to infiltrate them before an attack can be realized. In insider attacks however, the hacker is viewed as a legitimate and authorized participant of the network by its unsuspecting neighboring nodes. We will be concentrating on insider attacks launched by mote-class attackers.

Intrusion detection systems are considered a second line of defence when it comes to network security. They are implemented to protect the network in those scenarios where intrusion prevention techniques, such as authentication and encryption, fail. An IDS is used in a network to detect security breaches (both intrusions and misuse) caused by third parties. This is done by collecting and analyzing information generated in a network. Common intrusion detection techniques include misuse detection and anomaly detection. Misuse detection entails identifying and storing signatures of known intrusions and then matching the activities occurring on an information system to these signatures, in order to detect whether the system is undergoing an attack or not. Anomaly detection establishes a profile of normal activities (norm profile) and then compares activities on the information system to this norm profile. It signals an intrusion when the observed activities differ significantly from those usually undertaken by the user. In the current context, we will be using anomaly detection as the basis of our IDS . It is important to note here that traditional intrusion detection solutions, such as those applied to wired networks, cannot be applied directly to WSNs. Their foundations, regarding module placement and algorithm complexity, need to revised so as to address the severe resource constraints of WSNs.

DoS attacks are possible on all layers of a sensor network. In particular, the routing layer, which is responsible for end to end packet delivery, incorporates a number of vulnerabilities including neglect, greed, homing, misdirection, probing, blackholes and monitoring [4]. [3], gives specific names to these vulnerabilities i.e. spoofed data, selective forwarding, sinkholes attacks, the Sybil attack, wormholes, hello flood attack and acknowledgment spoofing. In this preliminary study, we concentrate specifically on identifying a spectrum of the selective forwarding attack, including the black hole attack. A description of these attacks follows.

Multihop networks, such as sensor networks rely on the fact that neighboring nodes will faithfully forward their messages to the base station. However, a malicious node that has included itself in the path of data flow can refuse to forward certain messages. This is known as a selective forwarding attack and is accomplished when the adversary drops packets coming from specific sources in the network. This attack can be crippling for the network as it isolates certain nodes from the base station and creates a discontinuity in network connectivity. It is also fairly difficult to detect. In a variation of this attack, known as the black hole attack, the hacker drops packets forwarded to it, without taking their source address into consideration. This attack is, however, much easier to detect.

In our simulations we consider a minimum energy routing protocol, called minimum transmission energy (MTE) [5]. In this protocol, nodes route data destined ultimately for the base station through intermediate nodes. Hence every node apart from being a data sensor also takes on the role of data router. In MTE, the next hop is chosen such that the transmission energy expended by the sending node is minimized, in an attempt to extend each individual node's lifetime. The transmission energy dissipated by a first-order radio model [5] is given by

$$E(k, d) = E_{elec} * k + \epsilon_{AMP} * k * d^2 \quad (1)$$

where k is the size of the transmitted packet, d is the distance of transmission, E_{elec} is the energy needed to run the transmitter circuitry and ϵ_{AMP} is the energy dissipated by the transmit amplifier. From the above equation it becomes apparent that in order to reduce transmission energy, a sensor node needs to select it's next hop based on distance. The closer a neighboring node is, the less the transmission energy required to forward a packet to it.

3. RELATED WORK

Much research has been conducted in the area of intrusion detection for wireless ad hoc networks. In their pioneering study, Zhang and Lee [6] proposed a distributed and cooperative IDS based on statistical anomaly detection techniques that use information from all communication protocol layers and local to each node.

However, intrusion detection specific to WSNs is mostly an unexplored area. There are many problems that render this area interesting. Primarily it is important to note that not every node can have a full powerered IDS agent associated with it, because of the hardware restrictions involved.

Other considerations include: fair distribution of the detection task among the nodes in the network, selection of features which are independent of the routing protocol used and timely propagation of alarms from the sensor nodes to the base station. Finally, an intrusion detection scheme must be capable of recognizing unseen attacks, whilst generating a minimal number of false alarms. To follow is a brief summary of some of the work that has been done in an attempt to address the above issues:

Loo et al. [7], present an intrusion detection scheme for sensor networks based on anomaly detection. Specifically, they use a fixed width clustering algorithm to allow for the detection of previously unseen attacks. They also came up with 12 general features for detecting sinkholes and periodic route error attacks based on the AODV protocol [8], which is not a pure WSN routing protocol. However, their proposed detection scheme requires no communication between the nodes hence minimizes the energy required to operate. They achieve up to 100% accuracy for active sinkhole attacks. We too follow the path of anomaly detection in this study.

Roman et al. [9], discusses the general guidelines of applying an IDS to static sensor networks. They also introduce an intrusion detection model based on spontaneous watchdogs, in which nodes elect independently whether they need to monitor the communications in their neighborhood. Implementation and simulation of this architecture is yet to be investigated. Krontiris et al. [10], define an IDS for sensor networks based on watchdogs for selective forwarding and sinkhole attacks. They adopt specification based rules and cooperative decision making techniques to create an IDS with low false positives and false negative alarms. No energy measurements were included in the simulation of this solution.

Onat and Miri [11], introduce an anomaly detection based security scheme for large scale sensor networks that exploits stability in neighborhood information to detect unwanted changes. In particular they employ a sliding window approach to detect spoofing and resource depletion attacks. The features they detect include average receive power and packet arrival times. They find that spoofing attacks can be detected relatively well just by looking for anomalies in the packet arrival rates. More realistic traffic models need to be implemented in this study.

Yu and Xiao [12], propose a detection scheme that uses multihop acknowledgements from intermediate nodes to raise alarms in the network. Their scheme focuses on selective forwarding attacks in which detection occurs in both the base station and source nodes. Simulations show that this scheme can achieve a 95% detection accuracy of malicious behavior, even with a high channel error rate.

Anjum et al. [13], proposed algorithms for improving the effectiveness of signature based intrusion detection techniques. These algorithms use minimum cut sets and minimum dominating sets to find the best placement for intrusion detection modules within an arbitrary sized sensor network. Simulation shows that these algorithms have very good detection performance compared to randomly placing the modules in the network.

Xiao et al. [14], present a simplistic intrusion detection model, which works with data link and network layer information and is based on a few simple checks including collision ratio, power used in the past seconds and packet integrity. The proposed architecture is a little naive for the task at hand and needs to be simulated.

4. SUPPORT VECTOR MACHINES

Support vector machines (SVMs) are a class of machine learning algorithms, due originally to Vapnik [15]. While originally formulated for binary classification, they have since been extended to include (amongst others) regression, density estimation, and one-class classification. Over the last decade SVMs have gained popularity due to their ability to tackle complex, highly nonlinear problems in a consistent, structured manner, while simultaneously avoiding problems of overfitting on simpler problems. For further details on the attributes of SVMs, [15], [16] can be referred.

In the present context we will be using one-class SVMs to detect selective forwarding attacks in a sensor network. We have chosen the one-class approach based on the fact that we are unlikely to know the form of any attack a-priori, and hence any attack training set we could construct, would be unlikely to provide an accurate representation of any *actual* attack on the network.

The one-class SVM problem [17], [18] is formulated as follows: We are given the training set

$$\Theta = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}\}$$
where $\mathbf{x}_i \in \mathbb{R}^{d_L}$, i=0,1,2,...,N-1

and N is the size of our training set and d_L is the dimensionality of our input space. In the present paper, the vectors $\mathbf{x}_i$ represent normal operating characteristics of the network. Based on this training set we wish to construct a decision function $g : \mathbb{R}^{d_L} \rightarrow \pm 1$ of the form

$$g(\mathbf{x}) = \operatorname{sgn}\left(\mathbf{w}^T \boldsymbol{\varphi}(\mathbf{x}) + b\right) \tag{2}$$

that is able to correctly differentiate between "normal" vectors $\mathbf{x}$ (i.e. those of the same class as vectors in the training set, which we will label class $+1$) and anomalous training vectors (which are not of the same class as vectors in the training set. . We will label these class -1), where in (2) the map $\boldsymbol{\varphi} : \mathbb{R}^{d_L} \rightarrow \mathbb{R}^{d_H}$ is an implicitly defined map from input space

to feature space, $\mathbf{w} \in \mathbb{R}^{d_H}$ is the weight vector and $b \in \mathbb{R}$ is called the bias. This may be achieved by solving the one-class SVM primal problem [17], [18]:

$$\begin{aligned} &\min_{\mathbf{w},b,\boldsymbol{\xi}} R(\mathbf{w},b,\boldsymbol{\xi}) = \tfrac{1}{2}\mathbf{w}^T\mathbf{w} + \tfrac{1}{N\nu}\sum_i \xi_i + b \\ &\text{such that} \\ &\qquad \mathbf{w}^T\boldsymbol{\varphi}(\mathbf{x}_i) + b \geq -\xi_i \, \forall i \in \mathbb{Z}_N \\ &\qquad \boldsymbol{\xi} \geq \mathbf{0} \end{aligned} \tag{3}$$

where $0 < \nu \leq 1$ is some constant and $\boldsymbol{\xi} \in \mathbb{R}^N$ is a vector of slack variables, wherein each ξ_i corresponds to a single training vector $\mathbf{x}_i$ and provides a measure of the success (if $\xi_i = 0$) or failure (if $\xi_i > 0$) of that training vector to be correctly classified.

In expression (3), the first term is a regularization term included to prevent overfitting, the second term is an empirical risk estimation function, and the final term is included to bias the result to detecting anomalies (so that those parts of input space either not covered (or only sparsely covered) by the training vectors are more likely to be labeled class -1 (anomalous)).

As is usual in SVM approaches, rather than solving the primal problem (3) directly we instead solve the dual form [17], [18], which defining a Lagrange multiplier α_i for each of the first set of constraints in (3), it can be shown to be:

$$\begin{aligned} &\lim_{\boldsymbol{\alpha}} Q(\boldsymbol{\alpha}) = \tfrac{1}{2}\boldsymbol{\alpha}^T\mathbf{K}\boldsymbol{\alpha} \\ &\text{such that:} \quad \mathbf{0} \leq \boldsymbol{\alpha} \leq \tfrac{1}{N\nu}\mathbf{1} \\ &\qquad\qquad\quad \mathbf{1}^T\boldsymbol{\alpha} = 1 \end{aligned} \tag{4}$$

where $\mathbf{1}$ is a vector of ones, $K_{i,j} = K(\mathbf{x}_i, \mathbf{x}_j) = \boldsymbol{\varphi}^T(\mathbf{x}_i)\boldsymbol{\varphi}(\mathbf{x}_j)$ is the kernel function, which may be any function satisfying Mercer's theorem [19] and implicitly defines the feature map $\boldsymbol{\varphi}$. Specifically, for any function K satisfying Mercer's condition [19] it can be shown that there exists a map φ such that $K(\mathbf{z},\mathbf{y}) = \boldsymbol{\varphi}^T(\mathbf{x})\boldsymbol{\varphi}(\mathbf{y})$ for all $\mathbf{x},\mathbf{y} \in \mathbb{R}^{d_L}$. Now, it may be noted that while K appears in the dual (4), the feature map $\boldsymbol{\varphi}$ does not (explicitly). Moreover, it can be shown [14,15] that g has the form

$$g(\mathbf{x}) = \sum_i K(\mathbf{x}_i, \mathbf{x}) + b \tag{5}$$

which does not contain $\boldsymbol{\varphi}$ explicitly. The result of this is that we may start with any kernel function K satisfying Mercer's condition, find $\boldsymbol{\alpha}$ and b and use the trained machine all without knowing the exact form of the feature map $\boldsymbol{\varphi}$. This is useful, as it decouples the dimensionality of feature space (and hence the potential complexity of g) and the dimensionality of the training problem (which is always N), allowing us to use very high (or even infinite) dimensional feature spaces with relative impunity.

5. Attack Model & Detection Scheme

We simulate an application in which the goal of the deployed sensor network is to report the presence of a mobile intruder to the base station as quickly as possible. This is done by having each node initiate a packet destined to the base station when its sensors sense the vehicle in its vicinity. From these packets the base station is able to analyze the movement pattern of the vehicle and its status.

However, in our scenario we suppose that an intelligent adversary has included herself in the position of maximum node degree, so that she can intercept the maximum number of data flow paths. The nodes use MTE to forward the packets to the base station. At any given time the base station records incoming bandwidth utilization and number of hops each message took to reach it.

Simulation parameters are as follows: We use a field size of 100 x 100 m^2, where 50 nodes have been deployed randomly (see Figure 1). There is a single base station located on the far left end of the network. Each node has a maximum signal strength of 30m. The detection range of each sensor is 10m. Sensors are activated in 1 sec intervals. Each node has an initial energy of 400 Joules and $\epsilon_{AMP} = 10pJ/bit/m2$ and $E_{elec} = 50nJ/bit$. The simulated packet size is 26 bytes.

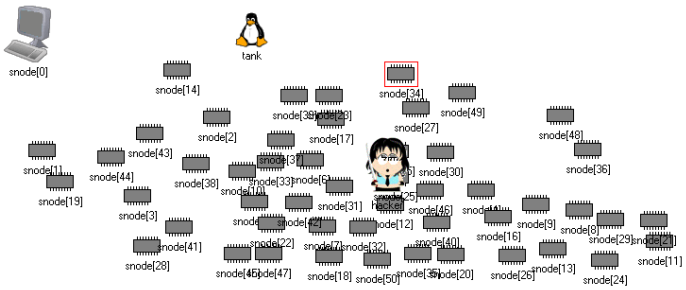

Fig. 1: Simulated network topology, including a hacker (South Park figure) and mobile phenomenon (penguin)

We perform five simulation runs. In the first run the hacker does not interfere with network communications, this is referred to as the normal run. In the second, third and fourth run, the hacker drops packets coming for 30%, 50% and 80% of the nodes in the network respectively. These are referred to as the selective forwarding runs. In the last run, the hacker drops every single packet it gets it hands on, hence executing a black hole attack or a 100% selective forwarding attack.

For each of these simulations we collected time series information of hop count and bandwidth at the base. This was then smoothed using a sliding window approach with a window width of 10 samples. The resulting smoothed data for the first simulation (without a hacker present) was split into training (60%), testing (20%) and validation (20%) sets, and the later simulations (with the hacker present) into testing (20%) and validation (80%) sets. The one-class SVM was then trained offline using the training set extracted solely from the first (no hacker) simulation, and parameter selection was carried out based on the testing sets, as described presently. Finally the validation set was used to generate the final results (see Section 6).

As alluded to above, parameter selection was done by choosing an allowable false alarm (i.e. hack detected when no hacker present) rate and then attempting to select parameters to maximize the rate of event detections on the test set

without exceeding this threshold for false alarms (see Figure 2). In all cases the kernel was selected from the set of polynomial kernels from linear up to order 5 and RBF kernels with $\gamma \in \{0.01, 0.02, 0.05, 0.1, 0.2, \ldots, 5, 10, 20, 50\}$. ν was selected from the range $\nu \in \{0.1, 0.2, 0.3, \ldots, 0.8, 0.9\}$.

All network simulations were carried out using OMNeT++ [20], and all SVM training and testing using a modified version of SVMheavy [21].

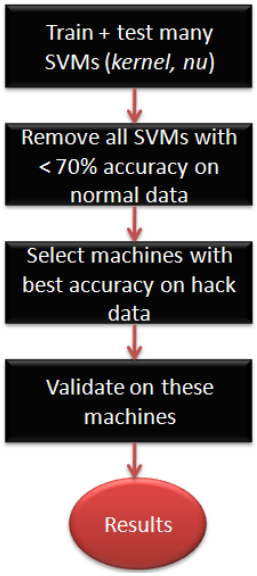

Fig. 2: SVM selection process

6. Results & Discussion

The results of our simulation experiments are summarized in *Tables 1* and *2*. For *Table 1* the allowable false alarm rate is set to 30% and for *Table 2* is set to 20%. In these Tables we present the validation results for the most accurate SVMs given the respective allowable false alarm rates.

Table 1: RBF SVMs with 30% false alarm rate

Gamma	Nu	Normal	30%	50%	80%	Black Hole
10.0	0.1	87.12%	13.04%	24.68%	55.62%	100%
2.0	0.3	65.48%	35.07%	49.78%	84.57%	100%
10.0	0.3	66.58%	36.86%	51.43%	84.64%	100%

Table 2: RBF SVMs with 20% false alarm rate

Gamma	Nu	Normal	30%	50%	80%	Black Hole
10.0	0.1	87.12%	13.04%	24.68%	55.62%	100%
10.0	0.2	75.07%	28.21%	41.90%	77.78%	100%

For both alarm rates, we can see that all SVMs can detect a black hole attack with 100%, using a sliding window of bandwidth and hop count only. Also, our proposed intrusion detection scheme achieves such accuracy without depleting the sensor nodes of any of their precious resources.

Since our IDS is centered at the base station, the nodes do not need to expend energy or memory collecting and communicating features amongst themselves, as is common in many of the distributed IDSs [10], [12]. This is all taken care of by the base, which has unlimited power supplies and memory compared to that of the individual nodes. Furthermore, as referred to in Section 3, the selected features (bandwidth and hop count) are independent of the implemented protocol and the SVMs are trained on the non-hack data, so all identified attacks are previously unseen and the alarms do not need to propagate to the base station because they are generated there.

For the 80% selective forwarding attack the SVMs still exhibit high detection accuracy. However, the less the participation of the hacker in the network (with 50% and 30% of source nodes being targeted), the lower the detection accuracy of the SVMs. This verifies the comment made in [3], that selective forwarding attacks are a more subtle attack than the black hole attack and are extremely tricky to detect accurately.

7. Future Work

For future work, we would like to model more DoS attacks on the routing layer, including spoofing attacks that manipulate packet content and are significantly more difficult to detect [3]. Furthermore, we wish to employ different classification techniques, such as neural networks and k-means nearest neighbors and gauge how these systems perform in this application in comparison to SVMs. Also, it would be interesting to make our intrusion detection scheme distributed and measure whether the detection accuracy of low participation selective forwarding (e.g. 30% and 50%) attacks becomes more efficient. If so, we would like to measure the tradeoff between detection accuracy and energy depletion in the network.

8. Conclusions

WSNs are vulnerable to a number of DoS attacks that may be used compromise their security and cause real world damage. In this paper, we proposed a centralized IDS that uses only 2 features to detect selective forwarding and black hole attacks. Our system can detect black hole attacks with 100% accuracy and selective forwarding attacks in which 80% of the network is ignored with approximately 85% accuracy. This intrusion detection is performed in the base station and hence the sensor nodes expend no energy to support this added security feature.

To the best of our knowledge, this is the first study to use SVMs for intrusion detection in WSNs and it is the first study to consider a centralized and not distributed IDS, that does not have further implications on node power.

References

[1] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, pp. 103–105, October 2003.

[2] R. Roman, J. Zhou, and J. Lopez, "On the security of wireless sensor networks," *Lecture Notes in Computer Science*, vol. 3482, no. III, pp. 681 – 690, 2005.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the First IEEE workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[4] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54 – 62, 2002.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, p. 10, January 2000.

[6] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, (New York, NY, USA), pp. 275–283, ACM Press, 2000.

[7] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

[8] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *WMCSA'99: Proceeding of the Second IEEE Workshop on Mobile Computer systems and Applications*, p. 90, 1999.

[9] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *CCNC 2006: Proceeding of the 3rd IEEE Consumer Communications and Networking Conference*, vol. 1, pp. 640–644, January 2006.

[10] I. Krontiris, T. Dimitriou, and F. C. Freling, "Towards intrusion detection in wireless sensor networks," in *EW 2007: Proceeding of the 13th Eurpoean Wireless ConferenceL Enabling Technologies for Wireless Multimedia Communications*, April 2007.

[11] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *WiMob' 2005: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 3, pp. 253 – 259, 2005.

[12] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," *IPDPS 2006: 20th International Parallel and Distributed Processing Symposium*, pp. 8–15, 2006.

[13] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," in *BROADNETS '04: Proceedings of the First International Conference on Broadband Networks*, pp. 690–699, IEEE Computer Society, 2004.

[14] D. Xiao, C. Chen, and G. Chen, "Intrusion detection based security architecture for wireless sensor networks," in *ISCIT'05: Proceeding of the International Symposium on Communications and Information Technologies*, vol. I, pp. 1365 – 1368, 2005.

[15] C. Cortes and V. Vapnik, "Support vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[16] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Knowledge Discovery and Data Mining*, vol. 2, no. 2, pp. 121–167, 1998.

[17] L. M. Manevitz and M. Yousef, "One-class SVMs for document classification," *Journal of Machine Learning Research*, vol. 2, pp. 139–154, 2001.

[18] J. Schray and C. A. Manogue, "Octonionic representations of clifford algebras and triality," *Foundations of Physics*, vol. 26, pp. 17–70, 1996.

[19] J. Mercer, "Functions of positive and negative type, and their connection with the theory of integral equations," *Transactions of the Royal Society of London*, vol. 209, no. A, 1909.

[20] A. Varga, "OMNeT++: Discrete even simulation system," 2005. `http://www.omnetpp.org/`.

[21] A. Shilton, "SVMHeavy: a support vector machine optimiser," 2001. `http://www.ee.unimelb.edu.au/staff/apsh/svm/`.