Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 169654, 7 pages
http://dx.doi.org/10.1155/2015/169654

Research Article

An Immunology Inspired Flow Control Attack Detection Using Negative Selection with *R*-Contiguous Bit Matching for Wireless Sensor Networks

Muhammad Zeeshan,[1] Huma Javed,[2] Amna Haider,[3] and Aumbareen Khan[4]

[1] *Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat 26000, Pakistan*
[2] *Department of Computer Science, University of Peshawar (UoP), Peshawar 25000, Pakistan*
[3] *Institute of Management Sciences, Kohat University of Science and Technology (KUST), Kohat 26000, Pakistan*
[4] *Department of Information Technology and Management Science, Preston University Kohat Campus, Kohat 26000, Pakistan*

Correspondence should be addressed to Muhammad Zeeshan; its_zeeshan07@yahoo.com

Received 10 July 2015; Revised 30 September 2015; Accepted 8 October 2015

Academic Editor: Wei Wei

Wireless sensor networks (WSNs) due to their deployment in open and unprotected environments become suspected to attacks. Most of the resource exhaustion occurs as a result of attacking the data flow control thus creating challenges for the security of WSNs. An Anomaly Detection System (ADS) framework inspired from the Human Immune System is implemented in this paper for detecting Sybil attacks in WSNs. This paper implemented an improved, decentralized, and customized version of the Negative Selection Algorithm (NSA) for data flow anomaly detection with learning capability. The use of *R*-contiguous bit matching, which is a light-weighted bit matching technique, has reduced holes in the detection coverage. This paper compares the Sybil attack detection performance with three algorithms in terms of false negative, false positive, and detection rates. The higher detection, and lower false positive and false negative rates of the implemented technique due to the *R*-contiguous bit matching technique used in NSA improve the performance of the proposed framework. The work has been tested in Omnet++ against Sybil attacks for WSNs.

1. Introduction

Wireless sensor networks (WSNs) have become a popular area of research in recent years due to their huge potential to be used in various applications. WSNs offer different challenges and vast new research area in continuation to the various applications. These networks are very restricted in terms of battery power, resources, and the overheads involved in communication. Such a network is highly vulnerable to attacks [1]. In such a scenario there are more chances to compromise reliability, availability, integrity of the sensor data traffic, and the sensors data traffic [2].

Intrusion Detection System (IDS) is adopted to deal with WSN security vulnerabilities as a second line of defense in the layered approach. Authorization, authentication, and key management are the first line of defense for a secure environment. Algorithm for IDS should be simple using low computation, complexity, memory, energy, and highly specialized type of attack [3]. Shamshiobad et al. [4] have categorized data models into three techniques; supervised, semisupervised, and unsupervised based on the available training data. This approach suffers a major drawback because of its limitations to obtain normal data and model all possible anomalous behaviors. In 1987, Denning [4, 5] proposed the first real-time intrusion detection model to detect anomalies in a computer system by comparing the current user behavior with a normal behavior model. However, this technique lacks learning capabilities and is based on a normal model generated online which does not change over time during detection.

Artificial Immune System (AIS) is an alternative solution having learning capabilities based on natural and biological principles. It has been applied in engineering to maintain integrity and functionality [6]. Bioinspired engineering, such as AIS, is believed to be able to address various issues of adaptation to environmental changes and self-organization and enable an emergent behavior of a distributed autonomous system, such as WSNs [7]. The immune cells are densely populated in the body just as nodes distributed in a sensor field. The immune cells function autonomously and interact with each other to protect our body [8]. Their adaptive characteristics and properties have been applied in various autonomous systems such as mobile ad hoc network [9] and swarm robotics for anomaly detection to detect malicious attack and faulty robots.

Soleman and Payandeh [5] proposed an algorithm to detect anomalies by proposing some monitors in the promiscuous mode. Attack detection rules are applied by monitor nodes to check their neighbors. In order to increase detection accuracy, the proposed mechanism applies tolerance by decreasing the detection overhead using monitor nodes. However, distribution of monitors and the rules selection affects performance of algorithm [10].

The existing IDS mostly perform detection at the sink which can result in a central point of failure. This can result in vulnerabilities due to Hierarchical IDS Architectures. Moreover, limited resource (memory, processing, and battery life) constraint is another important issue which is not addressed in most of the design of IDS for WSNs. Most of the resource exhaustion occurs as a result of attacking the data flow and thus creating end-to-end latency. Also, IDS for WSN have very low detection rate for detecting new data flow control attack pattern. Learning capability is also missing in most of the IDS models implemented for WSN.

The most common data flow anomaly is caused by Sybil attack. In this attack, the attacker (Sybil node) tries to forge multiple identification in a certain region. Since WSNs communication medium is broadcast, this attack is particularly easy to perform. A Sybil node can rig the vote on group based decisions and disrupt network middleware services severely by broadcasting messages with multiple identifications. Existing solutions for Sybil attack prevention for the resource-poor sensor platforms are too costly [6]. Motes (nodes) have energy constrained and very limited computational resources; thus, algorithms that impose an excessive communication burden on nodes are not acceptable for WSNs.

The prevention of Sybil attack in WSN using Dendritic Cell Algorithm (DCA) utilizes the signal produced in the tissue in order to detect pathogen related signatures [11, 12]. This technique proved to be light weighted for WSN but its performance for data flow anomaly attack detection, especially for Sybil attack, has shown degradation. Sybil attack prevention technique using Remote Password Comparison (RPC) Algorithm [13] checks the node duplication rate in the network and continuously verifies node identity and its location. However this technique has limitations for identifying duplicated node when the topology of WSNs changes or a route failure occurs. The leader node in the Neighbor Listening (NL) Algorithm [14] informs other nodes about their neighborhood, to set channel and configure global common channel, thus avoiding Sybil attack in WSNs. However, multiple channels setting for every node in the WSNs can create communication overhead and can affect throughput of WSNs.

In order to have IDS with decentralized detection, learning capability, and light-weighted algorithm to avoid resource constraints, an ADS framework inspired from the Human Immune System (HIS) is proposed in this paper for detecting Sybil attack which causes data flow anomaly in WSNs. The proposed technique implements an improved, decentralized, light-weighted, and customized version of the Negative Selection Algorithm (NSA) for anomaly detection with learning capability for new data flow control attacks.

The rest of the paper is as follows. The related work in intrusion detection algorithms for WSNs is presented in Section 2. The proposed Intrusion Detection System for data anomaly detection and its simulation is discussed in Section 3. Conclusion is drawn in Section 4.

2. Material and Methods

In Human Immune System (HIS) each cell has only a small set of tasks to perform which can be assumed as light-weight distributed agents collaborating in a noncentral configuration [15, 16]. The existing literature shows number of general purpose algorithms based on AIS. These algorithms are mainly based on the discrimination of self from nonself. The Idiotypic network theory (INT) is a bioinspired network model used to simulate immune networks [17–19]. The INT states that the immune system is an interacting network of molecules and lymphocytes that have variable (V) regions. These V regions bind to the things that are foreign to the vertebrate. They also bind to the V regions within the system.

The Dendritic Cell Algorithm (DCA) and the following danger theory are more recent and have been named as a second generation algorithm for detecting data flow control attacks. The DCA takes advantage of positive and negative feedback loops from the signals produced in the tissue regarding the safe or dangerous context of the tissue and the detection of pathogen related signatures [20, 21]. This algorithm has been shown to be very light weighted [11, 12]. However the false positive rates when evaluated for new Sybil attacks which are one of the data flow attack have shown high rates. Due to the absence of learning capabilities in the system, the false positive and false negative rates have shown high rates that have impacted the attack detection rate of new data anomaly.

Sara Janovic and Le Boudec [22, 23] have worked on misbehavior detection of data flow in traditional networks using immune inspired methods and have mainly concentrated on algorithms inspired by negative selection on AIS. The algorithms have improved the system by giving it memory and adding a negative feedback loop to make it more adaptable. This algorithm is not applicable for WSNs because of its high algorithmic complexity and the limited resource limitation for WSNs [24]. Xu et al. [25] focus on BeeAdHoc which is a Swarm Based Routing Protocol and propose BeeAIS-DC that overcomes the weaknesses of previous Anomaly Detection Systems for this routing protocol: BeeAIS and BeeSec. BeeSec is not an immune inspired algorithm and is a cryptographic system which requires key management. This is usually a challenge in ad hoc network, because it requires a central point of contact [26].

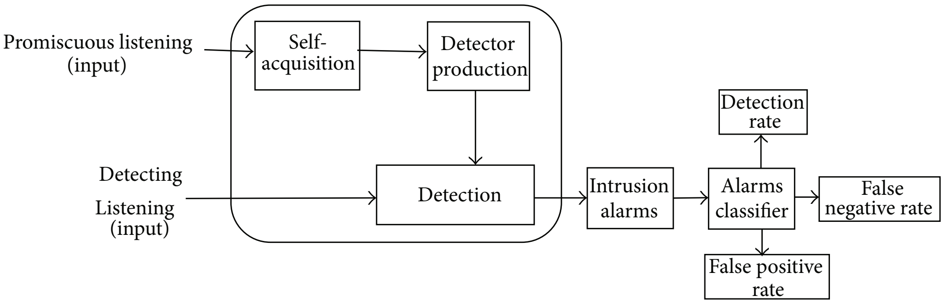


Figure 1: Intrusion detection model.

In Greensmith and Resdak [27], an energy aware method has been devised to detect misbehavior in ad hoc networks. The algorithm uses a set of features that are applied as cascading classifiers, with the energy cost of the classifier increasing as need for precision in detection is recognized. This algorithm requires change in the data link layer of AODV, in order to accommodate the changes. Also the current implementation of this method was performed implicitly and no implementation on network nodes is available.

In Remote Password Comparison (RPC) Algorithm [13], node duplication which can affect the data flow in WSNs prevents Sybil attack by verifying nodes ID and location. However this algorithm fails when the route failure occurs and requires route repair mechanism to be added [21].

In Neighbor Listening (NL) Algorithm [14], an asynchronous technique for neighbor discovery and configuration is employed for a single node Cogitative Radio Network (CRN). This algorithm provides a way to allow the leader node to inform other nodes about their neighbors, to set channel and configure global common channel, thus avoiding Sybil attack in WSNs. However the multichannel network and availability of channel at different nodes are not considered in this algorithm when detecting Sybil attack [28].

The network layer of the protocol stack of WSN is responsible for routing and data flow control. However, most of the hierarchical detection models have detection service at the sink level that can result in single point of failure if the sink is compromised. There is need of IDS Architecture for countering attacks targeting the data flow control in WSN with fault tolerance, high detection rate, and light-weightiness to overcoming the vulnerabilities of Hierarchical IDS Architectures. Also, learning capability in the system is missing in most of the detection models that can help to detect any modified form of the data anomaly attacks during its detection and will make the system more intelligent. Most of the IDS designs do not focus on the light-weightiness of the system in terms of communication overhead between the nodes that can affect the throughput of the WSNs. This leads to performing a research using immunoengineering approach to develop an immune inspired based Anomaly Detection System (ADS) focusing on the environmental and adaptability issues of WSNs. In addition to a decentralized attack detection design with learning capabilities there is a need for a light-weighted communication model between the nodes in the system to detect new or any modified version of data anomaly.

3. Results and Discussions

The proposed framework is a Cluster Based Hierarchical Architecture with Low Energy Adoptive Clustering Hierarchical (LEACH) protocol used for its routing operations. The proposed detection system is a hybrid Anomaly Based Network Intrusion Detection System (ANIDS) with services distributed at the node, sink, and cluster head level. The proposed work is divided into three main modules/phases as shown in the following:

Phase 1: self-acquisition,

Phase 2: detector production,

Phase 3: detection.

The following assumptions are made for this implemented work:

(i) The nodes are static with no addition of new nodes in the network.

(ii) For routing data packets to the sink node, tree based forwarding mechanism is used.

(iii) Except for making an attack, tampered nodes perform normally.

(iv) There is enough training time before a Sybil attack to start.

Due to finite communication range, sensor node has a certain number of neighbors within its radio range. A node receives messages and observes the behavior of its neighbors using its detection module, as shown in Figure 1.

3.1. Phase 1 (Self-Acquisition). In the training period, beacon packets collected from neighbors for key parameters extraction are processed before storing them in the self-pool as shown in Figure 2. The key parameters extracted are hop count, parent, and an average estimate. The parent field indicates the neighbor's next hop towards the sink node in the beacon packet. Most attacks affect at least one of these fields.

This phase is implemented and operated at the sink level. It is assumed that during this phase no attack or alarm

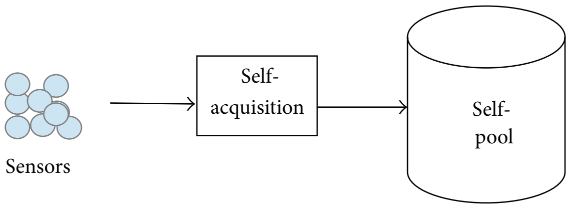


Figure 2: Self-acquisitions—Phase 1.

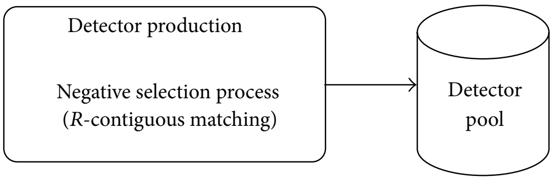


Figure 3: Detector productions—Phase 2.

is triggered. Also the network is trained in the simulation environment in order to generate self-pool termed as self-cell in HIS.

3.2. Phase 2 (Detector Production). The negative selection module starts generating detectors just after the completion of training, the detectors are stored in detector pool as shown in Figure 3. Negative selection (NS) is a process in HIS to defend the body against rising of self-reactive lymphocytes (antibodies). The purpose of detector generation is to distinguish a node having normal behavior from an abnormal behavior.

The NS process is shown in Figure 4. A mature detector is the one with no match with any random candidate string failing which the string has discarded. The typical matching rule in this proposed technique is r-contiguous bits [10].

In order to make the rule of this Intrusion Detection System unable to trace, detector production with randomization will be required. The detector pool copy will be moved down to the cluster heads at different level from time to time.

Let Z be a universal set which contains all 2^k distinct bit strings of length k. Consider the following:

A bit string $b \in Z$ with $b = b_1, b_2, \ldots, b_l$,

detector $d \in Z$ with $d = d_1, d_2, \ldots, d_l$ match with r-contiguous rule,

if a position p exists where $b_i = d_i$ for $i = p, \ldots, p + r - 1$ and $p < l - r + 1$.

Let the set S contain pairwise distinct bit strings randomly drawn from set Z. In NS process, detectors are to be produced such that no detector matches with any bit string from S. After generation of Detector Set $\mathbf{D}$, bit strings b_i are matched against the bit strings of $\mathbf{D}$ and classified as anomalous if an r-contiguous match occurs (see Algorithm 1).

When the Network Training Period is completed, the system change its state to detection phase. Nodes will extract the behavior (key parameters) by overhearing packets from neighbors. A detector will die and new detector will be generated if the number of matched antigens (count) is less than a predefined threshold in a detector's lifetime. The detector will issue an alarm if the number of matched antigens is greater than the threshold. The process of NSA is also shown in Figure 4.

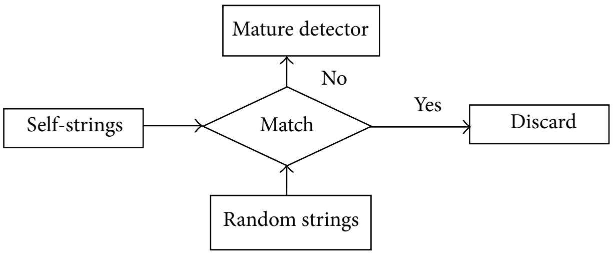


Figure 4: Matching rule (negative selection).

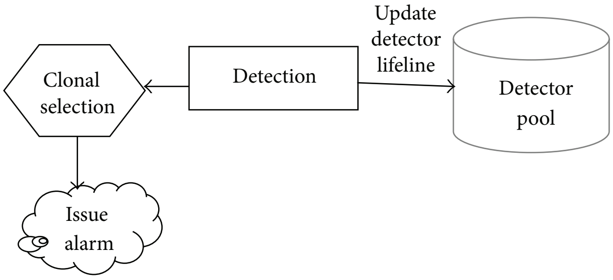


Figure 5: Detection—Phase 3.

3.3. Phase 3 (Detection). The system changes its state into detection phase when training is over as shown in Figure 5. Node hears beacon packets and extracts the information called antigens. The detector expires if the count of the matched antigens is less than the threshold, it will issue an intrusion alarm if it crosses it. A fast detection mechanism has been introduced in this research work to overcome time dely. A detector can trigger an alarm and go to the Clonal Selection service whenever it is activated. The proposed IDS can detect anomalies in a short time with acceleration using discrete r-contiguous bits rule.

The Clonal Selection service evolves detectors to memory detectors. Memory detectors detect anomaly quickly. Whenever the detector is activated, the lifetime of the detector increases and threshold decreases. In order to achieve fast data anomaly detection, this service turns on memory detectors quickly when attack of similar nature happens.

The detectors in the detector pool "$\mathbf{D}$" are categorized as immature, mature, and memory detector. The promotion of a detector from one type to another is based on its performance in terms of matching capability. The pseudocode of the proposed technique is shown in Pseudocode 1.

The proposed technique is simulated in Omnet++ which is an extensible, modular, component-based C++ simulation library and framework. The simulation comprises 100 nodes distributed randomly in a field of 120 × 100 m^2 in a hierarchical clustering model. The radio range of each node is 50 m. The simulation runs 10000 attack cycles each time.

```
Input: $S \subseteq Z$
(1) Begin
(2)         Generate a set D of detectors such that each fails to match any element in $S$
(3)         Monitor data $b_i \subseteq Z$ by continually matching the detector in D against $b_i$ if any detector matches with $b_i$, classify $b_i$ as
             an anomaly otherwise as normal.
(4) End
```

Algorithm 1: Negative selection.

```
IMB_IDS_WSN ()
{
    While (Training)
        If (Receive_Beacon (Msg))
            Phase1_SelfAcq (Msg, Spool)

  Phase2_Det_Production (Detector, Spool)

  //Phase 3 is Detection
    While (TRUE)
        If (Receive_Beacon (Msg))
            If (Match(Detector, Msg))
                Detector.Count++
                If (Detector.Count ≥ Detector.TH)
                    Clonal_Selection (Detector)
                    Trigger_Alarm ( )
                else
                    If (Detector.LTime > 0)
                        Detector.LTime - -
                    else
                        Update_DPool(Detector, Spool)
}
```

Pseudocode 1: Pseudocode of the proposed IDS.

Table 1: Simulation parameters.

R (matching length)	7
Detector pool size	256 bytes
Self-pool size	128 bytes

The number of nodes, radio range of the node, and field size can be varied. At the beginning during the learning period (7200 sec), node cannot issue alarms because of no attack. Adversaries start Sybil attack after the learning period. The attack interval uses only the first 20% of an attack cycle. In the simulation for initial results, 25% of the whole network data flow is malicious packets that are fixed; however the percentage can be varied. The parameters for detection modules fixed in the simulation are given in Table 1.

The value of R (r-contagious value) is fixed to 7 in order to cover more antigens by the detector. The size of the detector pool is fixed to 256 bytes keeping in view the limited storage of the sensors and to the requirement of our application. Also the size is fixed in order to accommodate more detectors and the size remains fixed as the unused detectors lifetime decreases with time and storage space is reused with only those detectors that are promoted to mature detectors. Also size of the self-pool is fixed to 128 bytes and it will reside at the sink level.

Table 2: Comparison of the techniques with Sybil attack detection models.

Evaluation	Proposed technique	DCA	NL	RPC
Detection rate %	98.7	91.2	94.3	86.3
False positive rate %	3.2	4.2	3.5	5.6
False negative rate %	2.9	4.7	3.6	3.5

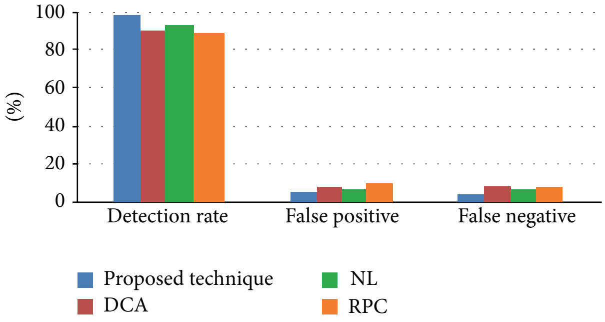


Figure 6: Analysis of the proposed technique with three Sybil attack detection models.

The detection false positive and false negative rates are simulated for evaluating our proposed IDS. In our simulation, Sybil attack is used to evaluate the performance of the proposed Intrusion Detection System. The detection and false positive and false negative rates of this technique are compared with DCA in Figure 6. The drop in the performance of this algorithm as mentioned earlier is due to the missing learning capabilities which has increased the false positive and negative rates. Also, comparison of detection rate and false positive and false negative rates of NL Algorithm with this technique is shown in Figure 6 and the result shows success of proposed work. The effectiveness of our proposed technique for Sybil attack detection is also compared with the RPC Algorithm in Figure 6 which justifies success of the proposed technique with low false positive and false negative rates and high Sybil attack detection rate. It is evident from Table 2 that our implemented work performed well in all respects than DCA, NL, and RPC.

In Table 2, the detection rates of different methods proposed for detection of Sybil attack are compared. It is obvious from Figure 7 that detection rate of our implemented

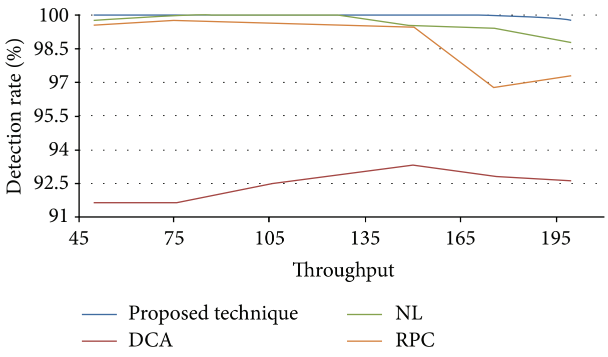


Figure 7: Comparison of detection rate against throughput.

technique is higher while false positive and false negative rate remained low compared to the other Sybil attack detection models. While DCA [21], NL [14], and RPC [13] methods performed well when there is an intermediate number of nodes, their performance in terms of data flow attack detection degrades quickly as the number of nodes increases continuously.

The proposed technique achieves 95% detection rates for all the forms of Sybil attacks with large detector pool and self-set. Reasons for achieving high detection rates by the proposed techniques are as follows: (a) use of discrete r-contiguous bit rule reduces the gray area in detection. (b) Fast detection accuracy is achieved due to memory detectors that learn attack signatures. (c) Each detector has different coverage on the non-self-set and complements its neighbors. Network memory and radio interference cause false positives. Even after the attack is over, these two characteristics make the network still under intrusion. Radio interference has a strong impact on the selection of number of hops to the network and next hop [28]. The simulations show that the proposed anomaly detection has high accuracy and capability of detecting any form of Sybil attacks.

4. Conclusion

This paper has investigated Sybil attack detection which is one of the data flow attacks which causes end-to-end latency in WSNs. Keeping in view the restrictions of WSNs in terms of limited resources and the attacks targeting them, an immunity-based data flow detection technique is presented in this paper. The detection of attack is performed at different level of the hierarchical WSNs in a distributed manner using HIS inspired negative selection process for dataflow anomaly detection. The customization of NS using r-contiguous bit matching is light weighted. The technique is compared and evaluated with three Sybil attack detection models for WSNs. The evaluations have shown high detection rates and low false positive and false negative rates for our proposed technique for Sybil attack detection in WSNs. This proves efficiency and accuracy of our technique in detecting Sybil attacks for WNs compared to other models keeping in view the limited resource constraints challenge. This technique will also be applied to other data flow control attacks at the network layer of WSNs and its efficiency will be evaluated accordingly.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] S. Khan, J. Lloret, and E. M. López, "Bio-inspired mechanisms in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 173419, 2 pages, 2015.

[2] B. Haris, "Wolf routing to detect vampire attacks in wireless sensor networks," *International Journal of Computer Science and Information Technology*, vol. 6, no. 3, pp. 2806–2809, 2015.

[3] E. Karapistoli and A. A. Economides, "ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks," *Eurasip Journal on Information Security*, vol. 2014, article 3, 2014.

[4] S. Shamshiobad, N. B. Anuar, M. L. Kiah et al., "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–117, 2014.

[5] H. Soleman and A. Payandeh, "Self-protection mechanism for wireless sensor networks," *International Journal of Network Security & Its Applications*, vol. 6, no. 3, pp. 85–97, 2014.

[6] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting," *Ad Hoc & Sensor Wireless Networks*, vol. 5, pp. 1–25, 2013.

[7] S. Nishanth, Virudhunagar, and T. Nadu, "Intrusion detection in wireless sensor networks using watchdog based clonal selection algorithm," *International Journal of Research in Engineering & Advanced Technology*, vol. 1, no. 1, pp. 131–143, 2013.

[8] M. R. Ahmadi, "An intrusion prediction technique based on co-evolutionary immune system for network security (CoCo-IDP)," *International Journal of Network Security*, vol. 9, no. 3, pp. 290–300, 2009.

[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[10] O. Aziz, B. Lo, J. Pansiot, L. Atallah, G. Z. Yang, and A. Darzi, "From computers to ubiquitous computing by 2010: health care," *Philosophical Transactions of the Royal Society of London Series A: Mathematical, Physical and Engineering Sciences*, vol. 366, no. 1881, pp. 3805–3811, 2008.

[11] J. Le Boudec and S. Sara Janovic, "An artificial immune system approach to misbehavior detection in mobile ad-hoc networks," in *Proceedings of the 1st International Conference on Biologically Inspired Approaches to Advanced Information Technology (Bio-ADIT '04)*, pp. 96–111, Lausanne, Switzerland, January 2004.

[12] M. Drozda, S. Schaust, and H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: performance and design principles," in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC '07)*, pp. 3719–3726, Singapore, September 2007.

[13] Y. Liu and F. Yu, "Immunity-based intrusion detection for wireless sensor networks," in *Proceedings of the International Joint Conference on Neural Networks (IJCNN '08)*, pp. 439–444, Hong Kong, June 2008.

[14] J. Kim and X. Yash, "Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm," in *Proceedings of the International Conference on Artificial Immune Systems*, pp. 390–403, Oeiras, Portugal, September 2006.

[15] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection in manets: a survey," *Journal of Intrusion Detection*, vol. 3, pp. 1–58, 2009.

[16] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 222–232, 1987.

[17] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pp. 202–212, Oakland, Calif, USA, May 1994.

[18] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05)*, pp. 253–259, Québec, Canada, August 2005.

[19] I. Onat and A. Miri, "A real-time node-based traffic anomaly detection algorithm for wireless sensor networks," in *Proceedings of the International Conference on Systems Communications*, pp. 422–427, IEEE, Ockland, Calif, USA, August 2005.

[20] J. Timmis, P. Andrews, N. Owens, and E. Clark, "An interdisciplinary perspective on artificial immune systems," *Evolutionary Intelligence*, vol. 1, no. 1, pp. 5–26, 2008.

[21] L. Hong and J. Yang, "Danger theory of immune systems and intrusion detection systems," in *Proceedings of the International Conference on Industrial Mechatronics and Automation (ICIMA '09)*, pp. 208–211, IEEE, Chengdu, China, May 2009.

[22] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection," in *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS '05)*, pp. 153–167, Dehli, India, August 2005.

[23] S. Sara Janovic and J. Le Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal and memory detectors," in *Proceedings of the 3rd International Conference on Artificial Immune Systems*, pp. 342–356, Catania, Italy, 2004.

[24] C. Wallenta, J. Kim, P. J. Bentley, and S. Hailes, "Detecting interest cache poisoning in sensor networks using an artificial immune algorithm," *Applied Intelligence*, vol. 32, no. 1, pp. 1–26, 2010.

[25] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, pp. 46–57, ACM, Urbana-Champaign, Ill, USA, May 2005.

[26] M. Zamani, M. Movahedi, M. Ebadzadeh, and H. Pedram, "A DDoS-aware IDS model based on danger theory and mobile agents," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '09)*, pp. 516–520, Beijing, China, December 2009.

[27] J. Greensmith and F. S. Resdak, "Detecting danger: applying a novel immunological concept to intrusion detection systems," in *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS '05)*, pp. 112–119, Paris, France, August 2005.

[28] R. Amuthavalli and R. S. Bhuvaneswaran, "Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method," *Journal of Theoretical and Applied Information Technology*, vol. 67, no. 1, pp. 236–246, 2014.

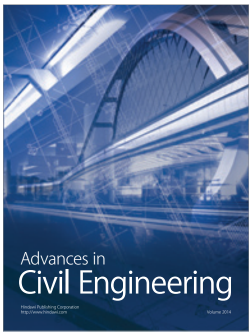
Journal of
Engineering

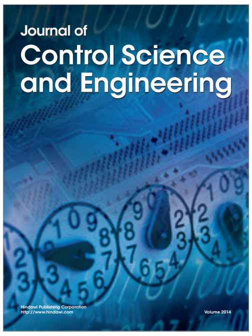
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

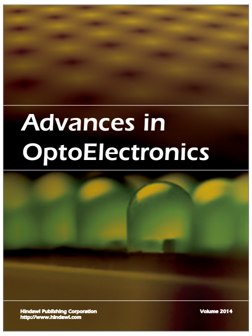
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

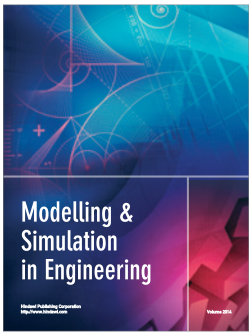
Journal of
Robotics

Journal of
Electrical and Computer Engineering

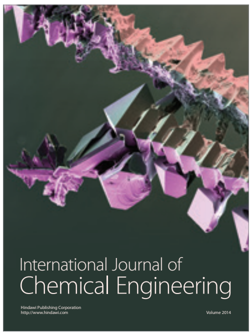

Advances in
OptoElectronics

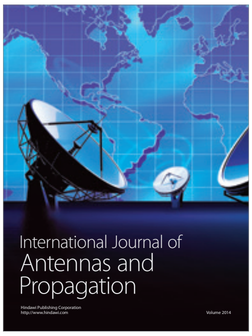
VLSI Design

International Journal of
Navigation and Observation

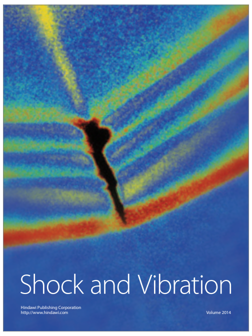

Modelling & Simulation in Engineering

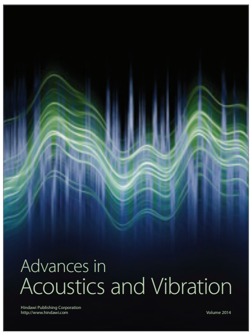
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration