Bio-Inspired Cybersecurity for Wireless Sensor Networks

Salim Bitam, Sherali Zeadally, and Abdelhamid Mellouk

The authors present a careful review of different bio-inspired techniques developed for improving cybersecurity of CPS using WSNs. Additionally, they propose a generic bio-inspired model called Swarm Intelligence for WSN Cybersecurity (SIWC) that addresses drawbacks of prior bio-inspired approaches.

ABSTRACT

Rapid advances in information and communication technologies have led to the emergence of cyber-physical systems (CPSs). Wireless sensor networks (WSNs) play a pivotal role in CPSs, particularly for operations such as surveillance and monitoring. However, these WSNs are subject to various types of cyberattacks that can cause damage, theft, or destruction of sensitive data, in addition to disruption of services provided by CPSs. To strengthen cybersecurity in WSN-enabled CPSs, various researchers have proposed a new category of efficient algorithms, inspired by biological phenomena. We present a careful review of different bio-inspired techniques developed for improving cybersecurity of CPSs using WSNs. Additionally, we propose a generic bio-inspired model called Swarm Intelligence for WSN Cybersecurity (SIWC) that addresses drawbacks of prior bio-inspired approaches.

INTRODUCTION

The widespread deployment of information technology (IT) in various cyber-physical systems (CPSs) such as smart grids, healthcare platforms, and computer networks has made them vulnerable to various types of security attacks known as cyberattacks. Such attacks are becoming increasingly sophisticated and dangerous, attempting to gain unauthorized access to a service or data, or trying to compromise a computational system's confidentiality, availability, or integrity. The last few years have brought a tremendous increase in the number of cyberattacks, along with the emergence of various types of cybercriminals who constantly develop new attack techniques.

According to the Ponemon Institute [1], the average consolidated total cost of a data breach, based on a recent 2015 study of 350 companies spanning 11 countries, is $3.8 million worldwide, up from $3.5 million a year ago. The same study found that the cost of a data breach is $154 per stolen record containing sensitive information, up from $145 in 2014. Due to the increasing cost of cyberattacks and our heavy reliance on computer systems and technologies, cybersecurity has emerged as an important research field to control and prevent such access.

TRENDS IN CYBERSECURITY WITH WIRELESS SENSOR NETWORKS (WSNS)

CPSs adopt and deploy technologies extensively, such as wireless sensor networks (WSNs) for many application domains. In particular, WSNs contribute to ensure the cybersecurity of CPSs, where sensors may dynamically collect physical information through a cooperative process that helps detect and mitigate potential future cyberattacks (as shown in Fig. 1).

In the literature, WSNs have been heavily used to support various surveillance and security functions. For example, sensor networks have been deployed to support surveillance capabilities such as threat-presence detection within security-sensitive and hostile regions such as a militarized area, border protection, etc. To support surveillance, a WSN has been proposed in [2] to detect and determine the direction of movement of intruding personnel and vehicles (i.e. target tracking) in the sensitive zone. For many of the surveillance functions, deployed sensors cooperate with each other to detect an imminent approaching mobile threat and are able to self-organize to provide a relevant, timely, and concise net-centric view of the surveillance field. This information helps to enhance decision-making abilities for command and control, intelligence, surveillance, and reconnaissance tactical mission planning. To enhance these decision-making abilities, sensor nodes should be able to forward threat information to a gateway node called the sink node. In such an environment, sensor nodes may be compromised by intruders to disrupt sensed and transmitted data by injecting false data reports.

Medical monitoring can also be cited as a healthcare service provided by wearable and implantable body sensors connected in the well-known body sensor network (BSN). A typical BSN is composed of a number of miniature, lightweight, low-power sensing devices and wireless transceivers. These sensor networks are used to capture large amounts of data containing information about the patient's health status, which is then stored in some database. Health status data commonly includes information such as blood pressure, heart rate, distance traveled through walking/running, playing activ-

Salim Bitam is with the University of Biskra, Algeria; Sherali Zeadally is with the University of Kentucky; Abdelhamid Mellouk is with the University of Paris-Est.

0163-6804/16/$25.00 © 2016 IEEE

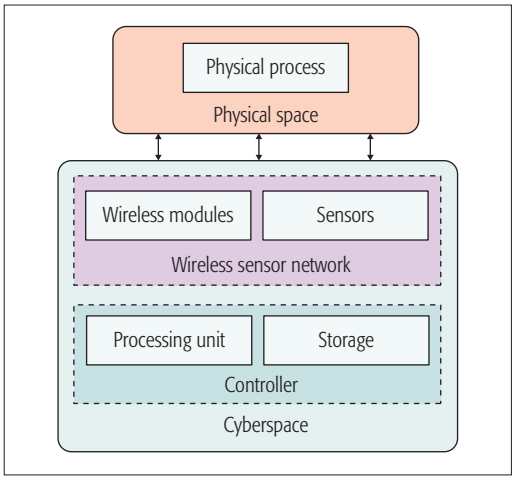

Figure 1. WSN-enabled cyber-physical systems.

ities, and surroundings (e.g. room temperature). This collected information helps the early detection of emergency conditions, diseases in at-risk patients, as well as the monitoring of chronic disease, elderly people, postoperative rehabilitation patients, and persons with special disabilities [4]. However, in this case a BSN may be exposed to a malicious party who can exploit various serious security threats to compromise the healthcare service and prevent patients from reaching available healthcare facilities.

Earlier discussions about the application domains (surveillance of sensitive regions and healthcare) demonstrate that WSNs are critical to provide vital solutions and cybersecurity that protect countries', organizations', and individuals' digital equipment resources and services from unintended or unauthorized access/change, disruption, or destruction. Attacks on WSNs can potentially affect the infrastructure's/application's entire operation (along with data confidentiality, integrity, and availability) given the integral role they currently play.

Motivations for Using Bio-Inspired Approaches for Cybersecurity

In the literature, several traditional approaches were proposed [3] to cope with WSNs' cybersecurity. However, these traditional security algorithms are not very effective for WSNs for the following reasons:

- In previously proposed traditional security approaches, compromised nodes are hard to detect because these algorithms typically consider one centralized node (i.e. a base station) responsible for detecting cyberattacks for large-scale networks. This situation leads to a heavyweight security process performed by the base station, which could potentially miss several attacks.
- Conventional security solutions do not scale well with the rapid increase in information or processing required by the massive influx of large amounts of data. Furthermore, the computational complexity of cyberattacks requires security solutions that are more scalable, robust, and flexible than traditional security methods can offer [5].

Therefore, recently a new category of methods has emerged that is inspired by biological phenomena such as biological evolution, biological immune system, and swarm intelligence. Bio-inspired techniques for WSN cybersecurity are initially motivated by the successful adaptive defense process of insects, such as ants against threats where they can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. Bio-inspired approaches are highly scalable, use lightweight architectures, and are less resource-constrained compared to traditional security solutions.

Bio-Inspired Methods and Their Application to Cybersecurity

Here, we briefly review three bio-inspired approaches aimed at improving cybersecurity (although not specifically for WSNs).

Genetic Algorithm (GA)

GA was proposed in [7] to create a moving target defense where the computer configurations (operating system and/or applications) are directly manipulated to find diverse, secure configurations that are placed in service at varying periods of time. The motivation behind this idea is that alternative configurations found by GA can disrupt the attacker's knowledge about the system. Therefore, the attacker acts on false or constantly changing information that may expend more resources, thereby increasing the risk of detection. This study encodes computer system configurations as chromosomes, and the security associated with each configuration is considered as its fitness. A series of selection, crossover, and mutation processes are performed to discover secure configurations. The fitness is decayed based on the period of time it was made active. Hence, less recently used configurations will be considered less secure, which will potentially pave the way for newly discovered configurations.

Ant Colony Optimization (ACO)

The authors of [8] proposed an ant-based model (called AraTRM) to address the problem of trust and reputation management and ensure the security of data forwarding in networks. In contrast to traditional approaches, the ant-based model is considered an effective way to detect an adversary node that exists in the selected path leading to the service provider. As in nature, when ants move, they leave a secreted pheromone substance to inform their nest mates of possible food discovery. Similarly, if the consumer is satisfied, he increases a score from source to destination (i.e. pheromone) on the global path from its location to the service provider, thereby rewarding this path as secured so that other consumers might use this path. On the other hand, pheromone values along the path to the malicious service provider will be punished by a victim client. As a result, the malicious service provider would be less likely to be selected as the next nodes by other consumers, because the incremented digital value (i.e. pheromone) on the edges linked to the malicious service provider is relatively small.

Bio-inspired techniques for WSN cybersecurity are initially motivated by the successful adaptive defense process of insects, such as ants against threats where they can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped.

The DAF utilizes lightweight agents that use stigmergic (pheromone-based) communications to create useful emergent colony behaviors that ensure the protected enclave's security. Application of the DAF to energy delivery systems incorporates data from both information technology and energy delivery systems.

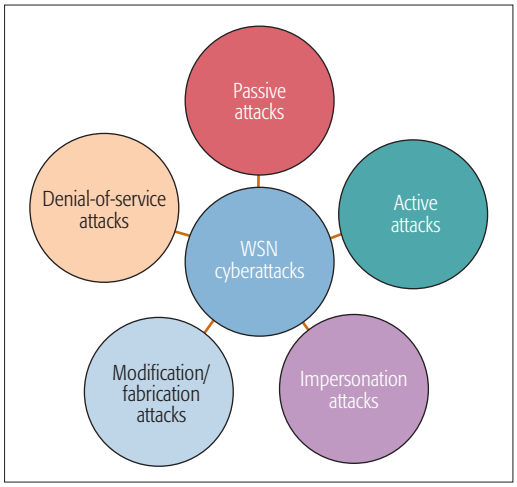

Figure 2. The five types of well-known WSN cyberattacks.

Artificial Immune System (AIS)

The authors of [9] used artificial immune system (AIS) modeling to study distributed system security issues such as identification, access level, authentication, and authorization in grid computing infrastructures. These grid systems aim to provide a safe and secure environment for anyone using recorded logs (i.e. all operations that occurred in the grid system). These logs, though, cannot ensure secure communications within the grids. To deal with this deficiency, four different groups of AIS agents were proposed: presenter, helper, memory, and killer agents. The presenter agent plays the role of an antigen that moves randomly between the network's nodes and is responsible for finding (auditing) faults, failures, or defected nodes caused by a cyberattack. If a defect occurs, the presenter agent solicits a helper agent to determine a specific killer agent for eliminating the defect's causes. The elimination operation follows a learning pattern generated and communicated to the killer by the memory agent, playing the role of lymphocytes that are known as natural killer cells (a type of white blood cells).

Next we present various WSN cyberattacks, followed by a discussion of different cybersecurity bio-inspired methods that can be applied to cope with these attacks.

WSN Cyberattacks

There are five types of well-known cyberattacks against a WSN (as shown in Fig. 2).

Passive Attack (or Eavesdropping Attack): Here, an attacker compromises and intercepts an aggregator node in the network, inspects it, listens, and reads useful data in it, trying to learn which nodes have more value within the topology (e.g. sink node or base station). Under the attacker's control, the new compromised node can be used to launch new malicious attacks. To protect nodes, WSNs should be able to conceal messages from unauthorized access (**confidentiality**).

Active Attack: In this scenario, an attacker intends to disrupt the network's functionality (**availability**). The active attacks jam communications by making changes to data already stored in the WSN in addition to modifying configuration parameters of the WSN's components (i.e. sensors). Thus, the sensors become unavailable and the expected WSN services are suspended.

Impersonation (or Sybil) Attack: In this attack, an adversary can directly replace a node's media access control (MAC) or IP address. The victim node is masqueraded as another node, which receives false data packets and compromises the trustworthiness of the information relayed.

Modification/Fabrication Attack: This attack involves unauthorized access to the WSN to modify the transmitted data packets or generate bogus data (affecting the **integrity** of the information) that is forwarded to the network nodes and to the base station. A sinkhole (blackhole) attack is a type of modification/fabrication attack that occurs when a malicious node attracts data packets sent by a sensor to a base station. A wormhole attack is another modification/fabrication attack in which the attacker records the packets at one location in the network and tunnels them to another location.

Denial-of-Service (DoS) Attack: This involves stopping the aggregation and forwarding of data in the network produced by the unintentional failure of nodes or as a result of malicious actions. DoS attacks prevent the base station from getting information from several sensors and nodes in the network.

Any of the aforementioned attacks that can potentially disrupt or destroy a network, or diminish a network's capability to provide a service, are considered a DoS attack.

Bio-Inspired Cybersecurity Solutions for WSNs

Now we review bio-inspired methods proposed for WSN cybersecurity. We classify these methods according to their biological inspiration.

Ant Colony Systems for WSN Cybersecurity

McKinnon *et al.* [6] proposed a complex-adaptive control system as a scalable approach inspired by ants' communication behavior to deal with the security risks associated with the large-scale deployments of smart grids. As with any complex system, this approach is based on inter-agent communication and the collective application of simple rules. Similar to ants, these lightweight agents move in the network and communicate using digital pheromones to alert each other about possible cybersecurity attacks. Both communication and coordination are local and decentralized, thereby allowing the framework to scale across the large number of devices that exist in the smart grid environment. This solution employs the digital ants framework (DAF), which applies lessons learned from ant foraging behaviors to address distributed cybersecurity problems. The DAF utilizes lightweight agents that use stigmergic (pheromone-based) communications to create useful emergent colony behaviors that ensure the protected enclave's security. Application of the DAF to energy delivery systems incorporates data from both information technology and energy delivery systems.

Marmol and Perez [10] proposed a bio-inspired trust and reputation model called Bio-inspired Trust and Reputation Model for WSNs (BTRM-WSN). This proposal is based on ant colony systems that select the most trustworthy node through the most reputable path, offering a certain WSN service. In particular, ants build paths fulfilling certain conditions in a graph. These ants leave some pheromone traces that help the next ants find and follow those routes.

Evolutionary Algorithms for WSN Cybersecurity

There are a few studies on WSN cybersecurity that use evolutionary algorithms because of their tradeoffs between required functional (such as accuracy) and non-functional (such as power usage and bandwidth) properties of any security solution. One such study is the reduced-complexity genetic algorithm for intrusion detection in sensor networks [11]. In this study, the authors proposed an evaluation process for sensor node attributes by measuring the perceived threat and its suitability to host the local monitoring node (LMN) that acts as a trusted proxy agent for the sink and is capable of securely monitoring its neighbors. These security attributes, in conjunction with a genetic algorithm, optimize the placement of LMNs by dynamically evaluating a node's fitness based on network integrity, residual battery power, and coverage. As a supervisor node, the sink is responsible for detecting various network misbehaviors, determining the list of sensor nodes affected, and then estimating the attack regions. This research effort [11] has shown a rapid detection of compromised nodes (with an improvement of almost 50 percent) due to the optimal placement of LMNs. Moreover, the accurate analysis of perceived threats by the sink has led to a substantial reduction in false positives and false negatives. Nevertheless, the major drawback of this genetic algorithm is its exponential computation cost for large-scale deployment of WSNs.

Particle Swarm Optimization for WSN Cybersecurity

In [12] the authors proposed a Secure Reputation Update Target Localization (SRUTL) algorithm based on PSO that addresses malicious node attacks such as Sybil attacks using target localization. SRUTL uses three phases. First, the sensor network is constructed following a uniform distribution where nodes are placed in a regular manner in the studied area, and then a stability factor (an inter-device noise) is verified at each node. This prevents malicious attacks at the node level; these nodes are considered as cluster members. A local voting scheme is performed at each node's neighborhood to elect cluster decoders (CDs) after verifying its identity. The CD with the highest reputation is selected as the cluster head (CH). Finally, a PSO algorithm is run at the CH level to detect malicious nodes in the cluster. To do that, the CH estimates the target's location and then sends an update packet to the cluster members. Once the update packet is received, each node (including the CH) computes its reputation based on its contribution for the target's location estimation and increases a local score using the signal strength at every node, as well as environmental and inter-device noise. During the next packet forwarding, the CH verifies its score with those of its cluster members. If a mismatch is found, the CH deduces that this member is a malicious node that should be ignored in any further reputation computation in the network. We note that this scheme did not address the special cases of nodes failing at the CH level, which could affect WSN security.

Artificial Immune Systems for WSN Cybersecurity

An artificial immune system called a cooperative-based fuzzy artificial immune system (Co-FAIS) was proposed in [13] to mitigate WSN DoS attacks. It is a modular-based defense system that consists of a set of agents working together to calculate the abnormality of sensor behavior or to detect the attackers. A sniffer module adapts to the sink node to audit data by analyzing the packet contents and sending the log file to the next layer called the fuzzy misuse detector module (FMDM), responsible for detecting misused nodes. The FMDM works with a danger detector module to identify danger signals' sources. The infected sources are transmitted to the fuzzy Q-learning vaccination module (FQVM) used to identify attack behavior following a reinforcement learning capability. The cooperative decision-making module (Co-DMM) incorporates the danger detector module with the FQVM to produce optimum defense strategies. An evaluation of the proposed system has shown that it improves attack-detection accuracy and yields a successful defense-rate performance against attacks after comparisons with attack-detection techniques based on a fuzzy logic controller, a fuzzy Q-learning system, and an AIS. However, a major drawback of Co-FAIS is that it needs more training time than traditional methods.

Neural Networks for WSN Cybersecurity

To detect DoS attacks at the media access control (MAC) layer of a WSN when monitoring real-time systems, the authors of [14] focus on a neural network (NN) considered as a low storage and computational time security scheme. To detect DoS attacks caused by adversaries that flood the network with packets, thereby causing collisions, two parameters were defined: the collision rate (Rc), which is the number of collisions per second detected by a node; and the arrival rate (Rr), which is the number of ready-to-send packets per second that are successfully received by a node forwarded as MAC control packets to start a data transmission. Rc and Rr are used to detect the probability of a DoS attack. Both Rc and Rr are used as inputs to the NN, and the corresponding probability of attack is represented as the targets to the multilayer perceptron (MLP). At each node, the MLP is implemented with pre-defined weights and biases, which are obtained from a trained phase. Every period, each node passes its computed values of Rc and Rr to its MLP, which produces an output that is the calculated probability of attack at that particular node. If the MLP's output (the calculated probability of attack at that particular node) is greater than a preset threshold value STH, then the node temporarily shuts itself down, and reac-

The accurate analysis of perceived threats by the sink has led to a substantial reduction in false positives and false negatives. Nevertheless, the major drawback of this genetic algorithm is its exponential computation cost for large-scale deployment of WSNs.

Study	Inspiration	Explicit introduction of user parameters	High complexity
[6]	Ant colony	Yes	–
[10] (BTRM-WSN)	Ant colony	Yes	–
[11] (LMN)	Genetic system	Yes	Yes
[12] (PSO-BASED)	Swarm intelligence	Yes	Yes
[13] (CO-FAIS)	Immune system	–	Yes
[14]	Neural network	–	Yes

Table 1. Comparison between bio-inspired methods for WSN cybersecurity.

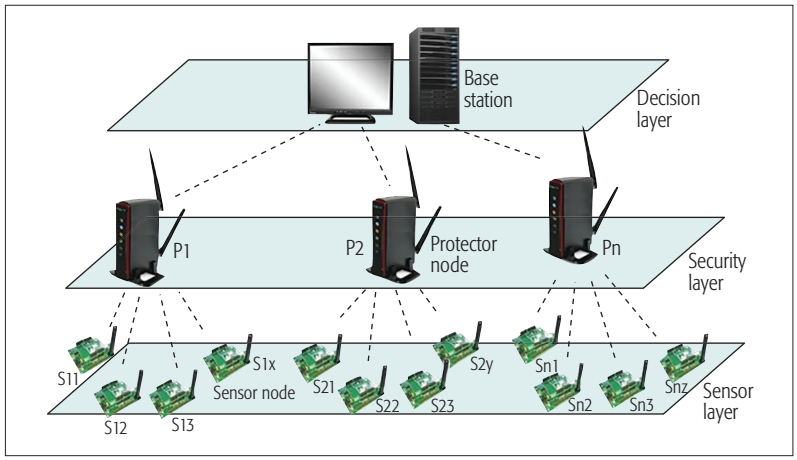

Figure 3. Our swarm intelligence for WSN cybersecurity (SIWC) model.

tivates subsequently when the attack is over. The choice of STH value is chosen depending on the extent of traffic variation in the normal operation of the WSN. Despite the good results given by this scheme in terms of the power saving due to shutting down the attacked nodes, this security mechanism might trigger a false alarm and cause the node to shut down in normal conditions without any attacks.

Discussion of Bio-Inspired Methods for WSN Cybersecurity

As Table 1 shows, the majority of the bio-inspired methods proposed for WSN cybersecurity require that the user input explicitly different parameters and variables (such as the population size for GA or pheromone value for ant systems) used by the method. In this case, because the user can choose inappropriate values, an automated process for choosing the parameter values is preferred. Moreover, some of these bio-inspired methods are of high computational complexity to be executed, especially in the case of a dense WSN. To address these major drawbacks, we propose a machine learning-based model to determine the optimal parameters for detecting more attacks without user involvement. To reduce computational complexity, this model is trained with a swarm intelligence algorithm, as we explain next.

Our Proposed Model: SIWC

We propose here a unified cybersecurity model called Swarm Intelligence for WSN Cybersecurity (SIWC). Considered as a machine learning-based approach, SIWC is an NN system trained by a swarm intelligence algorithm such as a genetic algorithm, ant colony system, particle swarm system, or some other algorithm. In contrast to traditional neural networks where general rules are given explicitly as learning rules to discover a prospective attack, SIWC is trained automatically by the swarm intelligence algorithm without requiring an explicit training process. Specifically, based on its interaction with its dynamic environment (i.e. several sources of information about prior cyberattacks), the swarm intelligence trainer can discover, formulate, and inform the NN about certain future cyberattacks. Various types of cyberattacks could be detected including active attack, passive attack, sybil attack, or DoS attack, where each one is expressed in a specific objective function established by swarm intelligence. Moreover, our approach makes use of an automatic lightweight security process (with reduced computation complexity and resource requirements) that is executed by cooperative agents. It is worth noting that the combination of swarm intelligence with neural networks has been used in the literature to solve other problems in different contexts such as data classification [15]. The architecture and functions of SIWC are explained in the following section.

SIWC Architecture

As Fig. 3 shows, SIWC consists of three layers: the sensor layer, the security layer, and the decision layer. The sensor layer is formed by different sensors (s_{11}, …, s_{1x}, s_{21}, …, s_{2y}, …, s_{n1}, …, s_{nz}) that are responsible for sensing and collecting data transmitted to the security layer (i.e. the second layer). The security layer is a set of protector nodes (p_1, p_2, …, p_n) responsible for detecting abnormal security behaviors and attacks of a cluster of sensors. The protector node represents the head of a cluster of sensors previously formed. For example, the protector node p_n is responsible for detecting misbehaviors of its cluster composed by sensors (s_{n1}, …, s_{nz}). In order to estimate the model parameters, the Maximum-Likelihood Estimation (MLE) approach is proposed. MLE is implemented on each protector node to ensure the cybersecurity of the protector node cluster. When a threat is detected, it is sent to the decision layer, which is the WSN base station, in order to take a relevant decision, such as mitigating the attack or switching off the attacked node.

SIWC Functionality

As mentioned earlier, each sensor node periodically calculates a set of critical parameters (x_i) (e.g. collision rate or arrival rate) in its sensing range. These critical parameters are forwarded as control packets to the corresponding protector node (the cluster head) to calculate the probability of an attack (as shown in Fig. 4). These parameters are weighted according to the importance of each parameter used to define an attack

among the sum of all parameters (e.g. the weight x_i for parameter x_i).

Each protector node possesses its own MLE trained using a swarm intelligence optimization algorithm after introducing the weighted parameters received from the corresponding sensors. The MLE method is trained to find the best values, which promote the highest probability of cyberattack detection. The found probabilistic value is compared to a prefixed threshold, which represents the cyberattack risk and which is determined by the swarm intelligence approach, based on previously detected attacks. Hence, the protector node informs the base station to take the appropriate action, such as shutting down a malicious node.

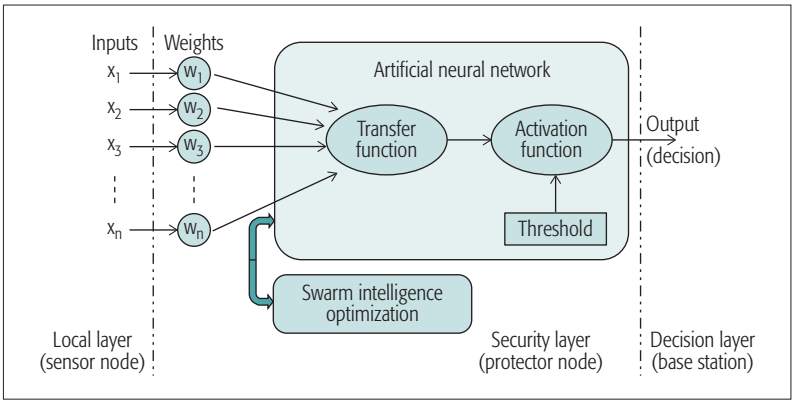

Figure 4. SIWC functionality.

Analytical Discussion of SIWC Model

In this section, an analytical discussion of our proposed model is given. To ensure the cybersecurity of wireless sensor networks that are often deployed to control cyber physical systems, we defined a set of requirements. We discuss below how our proposed model deals with each of these requirements to provide an efficient and secure solution.

Decentralized Authentication and Integration Mechanisms: Cybersecurity solutions should use lightweight, secure authentication mechanisms and key management schemes. Key management operations must be automated. A sensor node frequently needs to communicate with its base station to report data. As a result, secure communication protocols that preserve the integrity of the data should be used to detect any unauthorized access or modification to the data without any centralized coordination.

Our proposed SIWC model is a neural network-based technique that aims to ensure authentication and integration at a local level without any centralized administration. In fact, each cluster is independently protected by its own protector node that is responsible for its management. This protector node handles all cryptographic operations such as the generation of public and private keys, digital signatures, and cryptographic hash functions.

As for authentication, the protector node locally checks all connections among WSN nodes to detect any unauthorized intrusion. To achieve this, a maximum likelihood neural network is devoted to constantly monitor the network connections. This neural network is trained by a swarm intelligence algorithm in order to obtain sufficient learning experience to detect unusual variations when an attack occurs.

Automated Connection Lock: Cybersecurity for WSNs requires the timely processing of the transmitted messages so that they are received within a pre-defined time window, otherwise anomalous delays will be logged. Also, long network delays will cause termination of the network connection automatically after a predefined period of inactivity, as well as locking a connection session after a predefined number of consecutive invalid attempts. Based on the MLE, the proposed SIWC can estimate with high accuracy different delay parameters to detect various abnormal transmissions involving various delays, inactivity periods, etc. Indeed, the MLE gives the average value of the estimated parameter (taken from several random samples) which is theoretically exactly equal or close to the population value.

Distinction between Failure Situations and Cyberattacks: WSN devices are subject to eventual failures. In order to provide safe and secure operation, the cybersecurity system should distinguish between usual failure detection and unexpected cyberattacks by performing efficient local self-scan and self-test during the occurrence of any suspected event. To achieve this goal, the swarm intelligence algorithm defines a specific objective function that evaluates different nodes' states in order to distinguish a node under attack from a node failing or malfunctioning. Consequently, a set of parameters describing an attacked node is sent to the neural network, which can trigger periodically and automatically a test and scan routine to detect any attacked node.

Minimizing Computational Complexity of Cybersecurity Solutions: Another important requirement is to minimize the computational complexity of cybersecurity solutions. Considered as a biologically-inspired approach, swarm intelligence optimization is the most promising approach that reduces computational complexity because biological metaphors are an essential part of cyber concepts such as viruses, worms, etc. Bio-inspired approaches can detect a cyberattack in the WSN with very low complexity due to the probabilistic (none-exhaustive) tracking process that intelligently explores the network, and due to the best configuration (i.e. best values of neural network parameters) suggested by the swarm intelligence algorithm, which helps to quickly and efficiently detect any cyberattack.

Conclusion

Cyberattacks continue to become more sophisticated and occur with greater frequency. In this work, we focused on WSN cybersecurity, which is an integral part of many CPSs. In reviewing various bio-inspired approaches to enhance the cybersecurity of CPSs, we found that there is a need to address several of the drawbacks of recently proposed bio-inspired methods. These methods suffer from high computational complexity and require users to choose various input parameters. To address these drawbacks, we proposed SIWC, a generic bio-inspired model that uses a machine learning-based approach. SIWC is an NN sys-

These methods suffer from high computational complexity and require users to choose various input parameters. To address these drawbacks, we proposed SIWC, a generic bio-inspired model that uses a machine learning-based approach. SIWC is an NN system trained by swarm intelligence optimization to automatically determine the optimal critical parameters used to detect cyberattacks.

tem trained by swarm intelligence optimization to automatically determine the optimal critical parameters used to detect cyberattacks.

Acknowledgments

We thank the anonymous reviewers for their valuable suggestions and comments, which helped improve the quality and presentation of this article.

References

[1] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of Cyber Risk: An Empirical Analysis," *The Geneva Papers on Risk and Insurance–Issues and Practice*, vol. 40, no. 1, 2015, pp. 131–58.
[2] D. S. Ghataoura, J. E. Mitchell, and G. E. Matich, "Networking and Application Interface Technology for Wireless Sensor Network Surveillance and Monitoring," *IEEE Commun. Mag.*, vol. 49, no. 10, 2011, pp. 90–97.
[3] A. Oracevic *et al.*, "Secure Target Detection and Tracking in Mission Critical Wireless Sensor Networks," *Proc. IEEE Int'l. Conf. in Anti-Counterfeiting, Security, and Identification*, 2014, pp. 1–5.
[4] A. Darwish and A. E. Hassanien, "Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring," *Sensors*, vol. 11, no. 6, 2011, pp. 5561–95.
[5] D. J. John *et al.*, "Evolutionary Based Moving Target Cyber Defense," *Proc. ACM Conf. Genetic and Evolutionary Computation Conf. (GECCO), Wksp. Genetic and Evolutionary Computation in Defense, Security and risk management (SecDef)*, 2014, pp. 1261–68.
[6] S. R. Thompson *et al.*, "Bio-Inspired Cyber Security for Smart Grid Deployments," *Proc. IEEE Innovative Smart Grid Technologies*, 2013, pp. 1–6.
[7] E. W. Fulp *et al.*, "An Evolutionary Strategy for Resilient Cyber Defense," *Proc. IEEE Globecom*, 2015, pp. 1–6.
[8] W. Hao and Z. Yuqing, "AraTRM: Attack Resistible Ant-based Trust and Reputation Model," *Proc. IEEE Int'l. Conf. Computer and Information Technology*, 2014, pp. 652–57.
[9] E. B. Noeparast and T. Banirostam, "A Cognitive Model of Immune System for Increasing Security in Distributed Systems," *Proc. IEEE Int'l. Conf. Comput. Modelling and Simulation*, 2012, pp. 181–86.
[10] F. G Mármol and G. M. Pérez, "Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique," *Telecommunication Systems*, vol. 46, no. 2, 2011, pp. 163–80.
[11] R. Khanna, H. Liu, and H. H. Chen, "Reduced Complexity Intrusion Detection in Sensor Networks Using Genetic Algorithm," *Proc. IEEE ICC*, 2009, pp. 1–5.
[12] R. Tanuja *et al.*, "Secure Reputation Update for Target Localization in Wireless Sensor Networks," *Wireless Networks and Computational Intelligence*, Springer, 2012, pp. 109–18.
[13] S. Shamshirband *et al.*, "Co-FAIS: Cooperative Fuzzy Artificial Immune System for Detecting Intrusion in Wireless Sensor Networks," *J. Network and Computer Applications*, vol. 42, 2014, pp. 102–17.
[14] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural Network based Secure Media Access Control Protocol for Wireless Sensor Networks," *Proc. IEEE Int'l. Joint Conf. Neural Networks*, 2009, pp. 1680–87.
[15] W. A. H. Ghanem and A. Jantan, "Swarm Intelligence and Neural Network for Data Classification," *Proc. IEEE Int'l. Conf. Control System, Computing and Engineering*, 2014, pp. 196-201.

Biographies

Salim Bitam (salimbitam@gmail.com) is an associate professor in the Computer Science Department at the University of Biskra, Algeria, as well as a senior member of the LESIA Laboratory at the University of Biskra, and an associate member of the LiSSi Laboratory at the University of Paris-Est Créteil VdM (UPEC), France. He received an Engineer degree in computer science from the University of Constantine, Algeria, his Master's and Ph.D. in computer science from the University of Biskra, and a Doctorate of Sciences (Habilitation) diploma from the Higher School of Computer Science – ESI, Algiers, Algeria. His main research interests are vehicular ad hoc networks, cloud computing, and bio-inspired methods for routing and optimization. He has to his credit more than 30 publications in journals, books, and conferences, for which he has received two best paper awards. He has served as an editorial board member and a reviewer of several journals for IEEE, Elsevier, Wiley, and Springer, and on the technical program committees of several international conferences (IEEE GLOBECOM, IEEE ICC, IEEE/RSJ IROS, and others).

Sherali Zeadally (szeadally@uky.edu) is an associate professor in the College of Communication and Information at the University of Kentucky. He received his Bachelor degree in computer science from the University of Cambridge, England, and his doctoral degree in computer science from the University of Buckingham, England. His research interests focus on computer networks, including wired/wireless networks; network/system/cyber-security; mobile computing; energy-efficient networking; multimedia; and performance evaluation of systems and networks. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, England.

Abdelhamid Mellouk (mellouk@u-pec.fr) is a full professor at the University of Paris-Est Créteil VdM (Paris-12 University UPEC), Networks & Telecommunications Department and LiSSi Laboratory, IUT Creteil/Vitry, France. He graduated in computer network engineering from the Computer Science High Engineering School, University Oran-EsSenia, Algeria, and the University of Paris Sud Orsay (Paris-11 University). He received his Ph.D. in computer science from the same university, and a Doctorate of Sciences (Habilitation) diploma from UPEC. He is the founder of the Network Control Research activity with extensive international academic and industrial collaborations. His general area of research focus is on computer networks, including adaptive real-time bio-inspired control mechanisms for high-speed new generation dynamic wired/wireless networking in order to maintain acceptable quality of service/experience for added value services. He has held several national and international offices, including leadership positions in IEEE Communications Society Technical Committees.