Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks

Shahaboddin Shamshirband a,d,*, Nor Badrul Anuar a, Miss Laiha Mat Kiah a, Vala Ali Rohani a, Dalibor Petkovic b, Sanjay Misra c, Abdul Nasir Khan a

a Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaysia, 50603 Kuala Lumpur, Malaysia
b Department of Mechatronics, Faculty of Mechanical Engineering, University of Niš, 18000 Niš, Serbia
c Department of Computer Engineering, Atılım University, 06836 İncek, Ankara, Turkey
d Department of Computer Science, Chalous Branch, Islamic Azad University (IAU), 46615-397 Chalous, Mazandaran, Iran

Article history:
Received 30 August 2013
Received in revised form 26 February 2014
Accepted 17 March 2014
Available online 1 April 2014

Keywords:
Artificial immune system
Cooperative
Fuzzy system
Intrusion detection and prevention systems
Security

ABSTRACT

Due to the distributed nature of Denial-of-Service attacks, it is tremendously challenging to identify such malicious behavior using traditional intrusion detection systems in Wireless Sensor Networks (WSNs). In the current paper, a bio-inspired method is introduced, namely the cooperative-based fuzzy artificial immune system (Co-FAIS). It is a modular-based defense strategy derived from the danger theory of the human immune system. The agents synchronize and work with one another to calculate the abnormality of sensor behavior in terms of context antigen value (CAV) or attackers and update the fuzzy activation threshold for security response. In such a multi-node circumstance, the sniffer module adapts to the sink node to audit data by analyzing the packet components and sending the log file to the next layer. The fuzzy misuse detector module (FMDM) integrates with a danger detector module to identify the sources of danger signals. The infected sources are transmitted to the fuzzy Q-learning vaccination modules (FQVM) in order for particular, required action to enhance system abilities. The Cooperative Decision Making Modules (Co-DMM) incorporates danger detector module with the fuzzy Q-learning vaccination module to produce optimum defense strategies. To evaluate the performance of the proposed model, the Low Energy Adaptive Clustering Hierarchy (LEACH) was simulated using a network simulator. The model was subsequently compared against other existing soft computing methods, such as fuzzy logic controller (FLC), artificial immune system (AIS), and fuzzy Q-learning (FQL), in terms of detection accuracy, counter-defense, network lifetime and energy consumption, to demonstrate its efficiency and viability. The proposed method improves detection accuracy and successful defense rate performance against attacks compared to conventional empirical methods.

1. Introduction

Wireless Sensor Networks provide an ideal schema for gathering data as opposed to sensor nodes and data transmission via wireless networks. These types of networks range in application from the military (Bekmezci and Alagoz, 2009) and health care monitoring (Darwish and Hassanien, 2011) to disaster response (Wagner and Agrawal, 2014). The existing wireless sensor application designs afford greater flexibility in establishing communications and increasing system automation, but lack security and privacy (Abolfazli et al., 2014; Naserian and Tepe, 2009; Sun et al., 2013; Xu, 2010). The core weakness of these sensor nodes lies in the limited-resource devices, i.e. power and processing units (Aslam et al., 2011). For this reason, vulnerability to various security threats is notably high. Meanwhile, adversaries may hold passive and active access to secret information, such as keys stored in a compromised node by eavesdropping (Schaffer et al., 2012) or Denial-of-Services attacks. Thus, the wireless medium becomes overloaded and the probability of packet collisions within the interfering signal's range increases, causing, in both cases, additional sensor node energy consumption (Tan et al., 2013).

In mitigation security attacks, the soft computing (SC) approach incorporates Intelligent Intrusion Detection Systems with Preventions (IIDSs) to detect and impede abnormal traffic patterns that diverge from the modeled, expected, normal traffic behavior (Abraham et al., 2007; Anuar et al., 2013; Arun Raj Kumar and Selvakumar, 2013; Baig et al., 2013; Wong et al., 2012; Shamshirband et al., in press). A simple inspection packet mechanism was proposed by Tsunoda et al. (2008) to avoid stateful
inspection against Distributed Reflective Denial-of-Service (DRDoS) attacks. Muñoz et al. (2013) utilized fuzzy Q-learning for congestion detection to drop packets that differ from normal features. A pulse quarantine strategy was applied to worm propagation (Yao et al., 2012). Quinlan proposed a decision tree approach (Quinlan, 1986). C4.5 builds decision trees from training data sets using the concept of information entropy. That is, it is based on the highest gain of each attribute. After the tree is created by maximizing the gain, the C4.5 model decomposes the data space such that certain decomposed regions become homogeneous. Then, C4.5 performs the final pruning step. This step reduces the classification errors caused by specializations in the training set; thus, it makes the tree more general. While intrusion detection-based soft computing approaches display relatively reasonable performance regarding detection accuracy and minimal resource consumption, they fail to detect “unknown” attacks. Hence, applying soft computing security techniques that protect the wireless sensor network infrastructure by maximizing detection accuracy remains a challenge (Shamshirband et al., 2013). As such, an attempt is made through this research to address the problem of security by implementing an immunity-based mechanism.

From an information security perspective, one vital aspect to be learned from immunology is that a computer security platform should guard a host or entire network from illegitimate intruders, which is equivalent to the immune system’s responsibility of defending the human body from dangers and attacks by unknown pathogens. Ou (2012) proposed a system call damage detection mechanism based on agents that utilize the danger theory. Boukerche et al. (2007) suggested a mobile agent-based artificial immune system detection structure for register signature analysis using both syslog and Log check Unix in the network. Salmon et al. (2013) utilized an artificial immune system inside the sensor node to perform the monitoring of neighborhood behavior and collaborate to detect intrusion. Greensmith et al. (2010) used artificial dendritic cells (DCs) within the artificial immune system context that synchronizes artificial T-cell immune responses. Although the dendritic cells seem superior because they perform high accuracy detection while considering inspection among antigens, they fail to minimize the false alarm rate.

To mitigate the problem of false alarm rate, a multi-agent based immune system is utilized with intrusion detection system (IDS). Agent-based artificial immune systems adapt to the dendritic cells agent to imitate the behaviors of lymphocyte cell management of the human immune system in appraising antigens and corresponding signals to identify whether the antigens are malicious (Ou et al., 2013). This is achievable in the condition that each agent has defined duties and goals, as the multi-agent system is capable of coordinating and collaboration. Sobh and Mostafa (2011) proposed a cooperative immunological approach to detect anomalous behavior in a network. Gu et al. (2012) came up with a dendritic cell algorithm (DCA), which correlates gathered data as antigens and signals, and categorizes antigens as normal or anomalous. DCA accomplishes a mission by creating an anomaly detection mechanism with mature context antigen value (MCAV). The proposed agent-based mechanism influences robustness, flexibility, adaptability and low resource consumption, but the detection accuracy is not satisfied by using a non-sharing strategy and non-fuzzy threshold. Applying cooperative security techniques with bio-inspired agents that protect critical wireless network infrastructure by maximizing detection accuracy remains a challenge, and this research is an attempt to address the security problem in wireless sensor networks.

In this study the aim is to design a cooperative multi-agent based fuzzy artificial immune system (Co-FAIS) to protect against attacks on the wireless sensor node. This is a novel solution for the IDS problem. Co-FAIS is implemented in the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol and simulated in NS-2 to validate its performance in terms of recognition and defense accuracy. The defense strategy is adopted whenever a victim node in the network receives a flooding packet beyond a certain alarm event threshold. In identifying the diversity of adversaries potentially encountered by a node, a Co-FAIS mechanism is applied to reinforce the agent’s self-learning abilities and provide detector players with an incentive function to protect the most vulnerable sensor nodes that represent possible security threats.

The remainder of the manuscript is structured as follows. Section 2 presents related studies. Section 3 describes the proposed model and the methodology. The model integrates a cooperative mechanism with a fuzzy Q-learning based immune system with the scope of detecting Distributed Denial-of-Service attacks in wireless sensor networks. The detection model design is provided in Section 4 by introducing the agent strategies and utility function. Section 5 highlights the fuzzy Q-learning based artificial immune system algorithm, while Section 4 presents the simulation setup and a performance analysis discussion, particularly on detection and defense accuracy, network lifetime as well as energy consumption. Finally, Section 5 concludes the manuscript with suggestions for future research work.

2. Related studies

2.1. Types of possible attacks in wireless sensor Networks

Data transmission within a wireless sensor network necessitates the fulfillment of five requirements associated with security and energy consumption, namely data privacy, authentication, integrity, a distributed denial-of-service attack in terms of flooding, and energy exhaustion (Huang et al., 2013). A multitude of DDoS attacks have been designed, which can be categorized as synchronized packets in transmission control protocol (TCP SYN) flooding, User Datagram Protocol (UDP) flooding, and Internet Control Message Protocol (ICMP) flooding. A flooding attack employs overwhelming volumes of packets to deplete the victim network’s resources, including the processing capability among network terminals. It is assumed that the victim system’s memory stack becomes saturated and the system cannot process any more new demands (Zhou et al., 2010). In a wireless sensor network, flooding is more damaging on account of unstable wireless links, unbalanced usage of network resources, and weaker network devices, in which sensors always have processing and energy capability constraints (Fei yi et al., 2007).

2.2. Wireless sensor network model

From the multitude of network routing protocols proposed in recent years, hierarchical routing protocols are a major factor in a system’s scalability, lifetime, and energy efficiency (Ahmadi et al., 2013; Akkaya and Younis, 2005). Nodes in hierarchical networks are assigned various functions, e.g., cluster heads and cluster members. The nodes at higher levels, namely cluster heads (CHs), handle and gather information from the clustered nodes at lower levels (cluster members). Each cluster head collects information from members of its individual cluster, combines and then sends the data to the sink. All hierarchical routing protocols try to obtain an optimum cluster head and suitably aggregate nodes so as to preserve energy (Lung and Zhou, 2010).

Although hierarchical protocols have innate weaknesses such as requiring time synchronization potentially producing non-optimal routing, and utilizing higher overhead for cluster management, they reveal attractive advantages regarding wireless sensor network constraint management (Cordeschi et al., 2013; Lung and...
Compared with flat protocols, hierarchical protocols are more suitable solutions to handling large-scale networks with enhancements in sharing limited wireless channel bandwidth, balancing node energy consumption and reducing communication expense more optimally (Anisi et al., 2012; Liu, 2012). For instance, BEE-C is a hierarchical routing algorithm for wireless sensor networks that is bio-inspired by bee behavior, which aims to conserve sensor node energy (da Silva Rego et al., 2012). The BEE-C is based on the Low Energy Adaptive Clustering Hierarchy and LEACH-Centered protocols, which are both prominent in wireless sensor networks as identified in literature. BEE-C is applied to sensor networks with continuous data dissemination. The results indicate a number of advantages that BEE-C has over LEACH and LEACH-C. In the search for an efficient approach of generating clusters, the well-understood hierarchical clustering algorithm is adopted in this paper by proposing a distributed hierarchical clustering algorithm (Section 3.1).

2.3. Intrusion detection systems based on soft computing

Several countermeasures (Tapiador and Clark, 2013), such as source-end defense points (Mirkovic and Reiher, 2005), core-end defense techniques (Chen and Hwang, 2006), victim-end defense (Wang et al., 2007) and adaptive probabilistic filter scheduling (Seo et al., 2013) have been developed to mitigate flooding attack damage to routing protocols. Implementing firewalls, rate limitation and access control lists (ACLs) on routers may avert ongoing flooding attacks. End-to-end authentication should be well-designed to ensure that each user is certified prior to access to any network resource or the wireless channel (Das, 2009). Traditional security strategies, e.g., firewall, are alternatives to preventing external intruders and satisfying data confidentiality, authentication, and integrity (Eissa et al., 2011). Conventional strategies are essentially impractical in completely protecting network resources (i.e., energy resources) from increasingly sophisticated internal attacks (Qiu et al., 2013).

To overcome the problems of detection accuracy and false alarm rate, an intrusion detection systems (IDS) is adopted to identify illegal and unauthorized use, as well as misuse and abuse of any computer system by intruders (Patel et al., 2013). Soft computing techniques (i.e., fuzzy set, neural network and genetic algorithm) adapt to an intrusion detection system to capture the network’s traffic activity via sensors, and analyze it (Shamshirband et al., 2013). For instance, the artificial immune system mimics a natural immune structure to process all malicious events perceived by the sensor and implements intrusion detection techniques (Dasgupta et al., 2011; Greensmith et al., 2010; Igawa and Ohashi, 2009; Laurentys et al., 2010). These have been developed around the negative selection algorithm (Mahapatra et al., 2013) and clonal selection algorithm (Haktanir Ulutas and Kulturel-Konak, 2011). Although both algorithms exhibit good performance with regards to detection accuracy, they fail to improve the false alarm rate. As such, the danger theory is implemented to perform an action.

2.4. The danger theory (DT)

The danger theory suggests that antigen-presenting cells (APCs), particularly dendritic cells, function with danger signal receptors (DSRs) that are able to recognize signals from damaged cells. Such signals trigger the human-like immune system to act toward the responses. Antigen-presenting cells are stimulated by danger signals, and in this condition of stimulation they are capable of affording crucial signals to helper T-cells that direct and control the adaptive immune response (Aickelin et al., 2003). Danger signals are produced by regular body cells that have been damaged by pathogen attacks. These signals are sensed by dendritic cells, constituting a fundamental connection between the body’s immune system and the environment.
innate and adaptive immune systems and presenting the initial steps toward pathogenic attack detection. An antigen-presenting cell seizes antigen protein from the surrounding environment, then ingests and digests the antigens. Dendritic cells are also part of the innate immune system; once triggered, they travel to the lymphoid tissues where they interact with T-cells, while B-cells initiate the adaptive immune response. In this way, adaptive lymphoid tissues where they interact with T-cells, while B-cells of the innate immune system; once triggered, they travel to the then ingests and digests the antigens. Dendritic cells are also part cell seizes antigen protein from the surrounding environment, peptide–MHC molecules on dendritic cell surfaces. The stimulated T-cells proliferate and their clones differentiate into other cells, such as helper T-cells and cytotoxic T-cells (Shortman and Sathe, 2013). More recently, the multi-agent based artificial immunology IDS has been employed in wireless sensor networks to alleviate DDoS attacks through a cooperative agent scheme.

2.5. Multi-agent based artificial immune systems

Any software system part, that can perceive and analyze is known as an agent. The agent self-learns, solves problems, modifies according to the environment, and makes independent decisions for users (Ou et al., 2013). From a functional standpoint it is much like immunological cells. The implementation of multi-agent based artificial immune systems (MAIS) is one means of being management and communication instruments for the latter. AIS flexibility may assist with agents’ learning processes. Immune system responses, e.g., specificity, diversity, memory and self/

Table 1

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UF</td>
<td>Is a utility function</td>
</tr>
<tr>
<td>ρ</td>
<td>Symbolizes the weight of effective prediction, q = 0.75</td>
</tr>
<tr>
<td>SP</td>
<td>Characterizes the true confidence rate of attack patterns.</td>
</tr>
<tr>
<td>β</td>
<td>Signifies the weight of failed estimates (attack but no defense), b = 1</td>
</tr>
<tr>
<td>FN</td>
<td>Represents false negative of attack patterns – there are attacks but no defense</td>
</tr>
<tr>
<td>θ</td>
<td>Denotes the weight of failed predictions (defense but no attack), h = 1</td>
</tr>
<tr>
<td>FP</td>
<td>Represents false positive of attack patterns – there is defense but no attack</td>
</tr>
</tbody>
</table>

Figure 1 provides an assessment with reference to artificial immune and multi-agent systems. Artificial immune system, which is derived from the human immune system, also inherits properties such as learning, generating diversity, self-tolerance, memory, coordination, and self-maintenance.

In this research the agents’ features are classified in two main categories: (1) artificial immune systems, and (2) multi-agent systems. The inputs shown in the figure are as follows: for the properties marked “Yes” for both MAS and AIS (e.g., coordination and communication), the agent mechanism can be applied to the artificial immune system; these properties remain obscure and undefined in immunology. In contrast, for the properties marked “No” for multi-agent systems but “Yes” to artificial immune systems, the related theory of the latter is applicable to the multi-agent system. One instance is the “Learning” property, whereby the artificial immune system learning mechanism is an option for the multi-agent system. In our proposed scheme, the cooperative artificial immune system is implemented into IDS to

nonself recognition are vital to a good learning mechanism. They could help improve agent reaction to intruders. Moreover, biological immune system elements such as content-addressable memory and adaptation can be implemented by intelligent agents.

Significant agent features, for instance “non-adaptability,” are challenging for multi-agent systems in relations with their surroundings. Three key multi-agent based artificial immune phases motivated by the clonal selection theory are diversity generation, self-maintenance and memory of non-self (Chan and Lau, 2011), with the final two signifying multi-agent system (MAS) adaptability. Agents distributed throughout the multi-agent system perform these steps.

- Diversity generation:
  - Results in the constant adaptability of MAIS. Mutations produce various agents with distinctive receptor and effector specificities.
- Self-maintenance:
  - Agents are tuned to become insensitive to known patterns (self) in the developmental stage. The negative selection theory is fundamental to self-maintenance.
- Memory of nonself:
  - Agents are adjusted to be more sensitive to unknown patterns (nonself) during the working phase.
generate the benefits of a fuzzy Q-learning algorithm with a value function to mitigate the flooding attack issue in a wireless sensor network with respect to detection and defense accuracy. Resource loss, accuracy of attack detection via sensors, and service inaccessibility at critical times are among the challenges posed, and through this research, an effort is made to confront the security setbacks by applying the cooperative game-based fuzzy system and reinforcement learning mechanism.

2.6. Utility function

To appraise the efficacy of the associations determined by the Co-FAIS and to establish the rule's applicability at every point in time, Eq. (1) was utilized in this work as suggested by Huang et al. (2013). Table 1 lists the utility function parameters.

\[ U_F = \frac{\rho SP}{C_0} - \frac{\beta FN}{C_0} - \frac{\theta FP}{\left(1\right)} \]

The artificial immune system-based fuzzy Q-learning principle approach entails detection accuracy with low time complexity, which only subsequently begins to formulate a shield policy. The major drawback of the artificial immune system theory is that if attacks recur over a short interval, a substantial amount of time is consumed in the detection phase, thus weakening the defense. It can be said that detection precision may be low and false alert rate high. To diminish the flaw of artificial immune system-based fuzzy Q-learning, we utilized cooperative fuzzy Q-learning proposed by Shamshirband et al. (2013). Its principal contribution is identifying the probability of future attacks aimed at a wireless sensor node. For frequent attacks occurring over a short time, multi-agent based fuzzy Q-learning was adopted to deal with the excessive time spent on detection. The aim of the proposed Co-FAI is to obtain high detection accuracy with a low false alarm rate.

3. Proposed model

3.1. Wireless sensor network model

In the present research study and according to Fig. 1 the distributed network with hierarchical routing comprises clusters (C), their coordinators, or cluster heads (CHs), as well as member sensor nodes (S). In the current scheme, the cluster head is assumed to be a sink node (SN) in each cluster. The sink node monitors the behavior of sensor nodes by collecting data from the member sensor nodes and transmitting the critical status – the sensor nodes’ attack information, to a base station (BS). Each cluster is mapped into distributed system formation while the set of sensor nodes is charted into each cluster grouping. Although
only one base station is shown in Fig. 2, several could practically be implemented in a real, operational wireless sensor network. The route from a sensor node to a base station is deemed a distributed-hierarchical path that creates a hierarchical system with numerous routes as the main feature of cluster-based wireless sensor networks. Sensor nodes function independently to avoid their collective collapse in case a single one fails. The sensor node redundancy approach increases the overall reliability in distributed hierarchical systems. Figure 2 illustrates the way sensor nodes send data collected from a sink node to a base station via other adjacent sink nodes, and the base station receives data only if all sensor nodes within the routing formation are actively functioning. Hence, a set of clusters on a route counts as a set of independent, distributed-connected elements. Attacks in this scenario can target the wireless sensor in multiple ways, with DDoS attacks potentially originating either from the Internet or neighboring wireless sensor sources.

3.2. Methodologies and techniques employed

The bio-inspired based detection and defense mechanism operates to detect DDoS attacks, where the sink node and base station select the best strategy of discovering an impending attack and responding to it. Regardless of whether attacks are carried out on a regular basis or not, the IDS can adjust its learning parameters to identify future attacks. According to deficiencies observed by Ou et al. (2013), Sobh and Mostafa (2011), Yang et al. (2009), an improvement in IDS based on cooperative fuzzy Q-learning based AIS algorithm is introduced. In our scheme, Co-FAIS is used to detect danger signals emitted by sensor nodes. These danger signals are based on antigen or attack patterns, which are defined by traffic generated in response to a flooding attack dataset.

The system runs and distinguishes attacks in real-time mode. It continuously sniffs data from the network and inspects the sensor's behavior. The attack dataset contains profiles of normal system resource usage (Excessive CPU usage, memory load on the host, bandwidth saturation, and high number of connection at the host) collected from the trace file of the NS-2 simulator. This database is meant to create a base to assist with classifying normal from abnormal usage. Figure 3 demonstrates the proposed Co-FAIS architecture and data flow in six modules.

To highlight the proposed Co-FAIS, the sink node and base station are allocated a corresponding reward/incentive functional value retained by the Fuzzy Q-learning IDS. As such, a node's evolving fuzzy state may be recorded and quantified through the fuzzy reward function. When a node encounters an attack or receives an anonymous message, the sink node sends the related severity of alarm event evidence and messages to the base station, who then analyzes the critical data to adjust the artificial immune FQL parameters. Based on the sink node information, the base station decides which nodes are under attack or at risk and elects whether to safeguard them or not. The base station had previously set a severity alarm event threshold rate, v. Once the severity alarm value acquired by a node exceeds v, the Co-FAIS deems the node under attack or at risk, and strengthens its defenses to secure the cluster area in which the node is detected at the associated base station.

3.2.1. Module 1: Sniffer Module

The Sniffer Module (SM) section seizes packets from the network traffic and examines every packet constituent. The data is sniffed online and is transmitted to the detection module for potential attack examination. The sniffed data is fed to the offline system in case of high traffic volumes, and the outcome is saved in a log file. A fuzzy rule-based packet analyzer served as a detection module in the present work, to pre-process packet features.

3.2.2. Module 2: Fuzzy Misuse Detector Module

This module computes the match (affinity) between packets among a set of self-packets and then reports the highest matching value. Consequently, the highest matching value is contrasted with a matching threshold to identify whether the recently caught packet is recognized by the system or intruder. From a security domain viewpoint, this is considered the misuse detection unit. To fully examine suspicious behavior, the fuzzy system utilizes

#### Table 2

Fuzzy linguistics and abbreviations of variables for each parameter.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Inputs linguistic variables</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy usage (Eu): Joule</td>
<td>Low (L), Medium (M), High (H)</td>
<td>0–100 (J)</td>
</tr>
<tr>
<td>Buffer size (Bs): kb</td>
<td>Low (L), Medium (M), High (H)</td>
<td>4–7068 (Kb)</td>
</tr>
<tr>
<td>Time response (Tr): ms</td>
<td>0–120 (ms)</td>
<td></td>
</tr>
<tr>
<td>Count (Co): ms</td>
<td>1–3 (%)</td>
<td></td>
</tr>
<tr>
<td>Pattern (P)</td>
<td>Outputs linguistic variables</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bad, average, good, excellent (N, A)</td>
<td></td>
</tr>
</tbody>
</table>

![Fig. 4](Image) The architecture of the proposed Fuzzy Misuse Detector Module.
fuzzy rules from the Fuzzy Misuse Detector Module (FMDM) to identify the anomaly conditions received from the traffic. The proposed FMDM consists of the following components: capturing traffic, feature extractor, fuzzification, the fuzzy inference engine, knowledge base, and the expert analyzer. Figure 4 shows the components of the proposed fuzzy-based misuse detection system architecture of Co-FAIS.

3.2.2.1. The feature extractor. The feature extractor obtains elements on the “network traffic” caught by the traffic capture component. Under the network and system environments, several traffic features may be employed for attack detection and analysis.

Definition 1. Threat profile

One of the problems with IDS has to do with defining a “baseline” to identify network packet anomalies. A threat profile (TP) baseline for instance can help IDSs with decision making on the sorts of suspicious network packet attacks. In line with network detection, these aspects are signal attribute functions (CPU_usage, memory_load, bandwidth_saturation, connection_numbers). In our scheme, the threat profile is defined as a 4-tuple TP=\{Eu, Bs, Tr, Co\} according to vulnerability scanning information, where Eu denotes the sensor node’s energy consumption; Tr is the variance of time difference between two connections during a specific time window; Bs denotes the length of the packet from source to destination; Co is the number of connections to the same host as the current connection in the last two seconds.

3.2.2.2. Fuzzification. Each input variable ought to first be fuzzified into linguistic values prior to the fuzzy decision dealing with it according to the rule base. A typical fuzzy set function is allocated values between 0 and 1, denoting membership degree of an element in a particular set. Table 2 displays the input and output fuzzy linguistic variables and Figure 5 indicates the membership functions for attack source evaluation by verifying energy usage, buffer size, time response, and count.

3.2.2.3. The fuzzy inference engine and knowledge base. The knowledge base stores the fuzzy rules used by the fuzzy inference engine to obtain a new fact.

![Fig. 5.](image-url) (a–d) Input membership functions of linguistic variables of the threat profile. (a) Energy usage (Eu) membership function, (b) Buffer size (Bs), (c) Time response (Tr), (d) Count (Co) and (e) Output membership functions of linguistic variables (pattern).
3.2.2.4. The expert analyzer. The expert analyzer decides the influence result from defuzzification, as to whether inspected packets are attacked or not. If the crisp value is not equal to the threshold value of the detection attack rule, then it assumes an attack has occurred. The process of manually extracting rules can be time-consuming and the rules may be approximate (Shamshirband et al., 2010). Because these methods are off-line in nature, if a very large data set is involved, it can become expensive and impractical. Thus, it fails to detect new attacks in real-time. To overcome this problem, a hybrid soft computing method of identifying DDoS attacks is proposed in this work.

3.2.3. Module 3: Danger Detector Module
The main responsibility of the Danger Detector Module (DDM) is to contrast the usage profile of the current system against that of the normal system saved in the profile database, and check for possible deviations and measure their degree. This phenomenon can create a security domain definition based on the anomaly detection module that can recognize new attacks through analyzing changes in the system’s normal behavior. This systematic model plays a part in modifying the self-database mentioned below, as it detects sources with the potential to cause the release of danger signals.

3.2.4. Module 4: Fuzzy Q-learning Vaccination Module
The human activity most similar to this model is vaccination. The models’ principal responsibility is to update information regarding the system in terms of thresholds, profiled resources, etc., by examining the behavior of a real attack in a monitored environment and checking the system’s ability to react and defend itself. To prevail over the required complex detection and defense time as well as detection precision issues in our artificial immune system method, the fuzzy Q-learning algorithm proposed by Shamshirband et al. (2013) is applied in the current work to predict probable future points of attack. To optimize Q-learning algorithm performance from the action selection method and reward function perspectives, the fuzzy min–max methods were employed. In the proposed scheme, the fuzzy min–max action selection and reward function with conventional Q-learning in terms of Fuzzy Q-learning Vaccination Module (FQVM) works to identify attack behavior. Fuzzy Q-learning served to reinforce the learning capability of the artificial immune system. Figure 6 depicts the FQL optimization system as a block diagram.

The fuzzy Q-learning vaccination module is a fuzzy-based Q-learning strategy for attack detection. The design of the anomaly-based fuzzy Q-learning incorporates a fuzzy logic controller, which converts the continuous inputs into fuzzy sets. Four fuzzy sets have been defined for the fuzzy Q-learning input to represent four different situations as a Q-learning state space. This supplements more dynamic behavior to the system and enables the early detection of new attacks. The fuzzy Q-learning inputs, given by Energy usage (Eu), Time response (Tr), Buffer size (Bs), and Count (Co), correspond to the network’s fuzzy state in the following equation:

$$S(t) = \text{[Energy usage (Eu), \times Time Response (Tr), Buffer size (Bs), Count (Co)]}$$ (2)

The FQL output, given by the abnormality, represents the action of agent, $$A(t)$$. The linguistic variables Eu, Tr, Bs, and Co act as inputs while the abnormality functions act as output, all of which are used in the experiments (Table 2). A small number of rules (Table 3) accelerate Q-learning algorithm convergence since fewer states are visited during the exploration phase. Therefore, the

<table>
<thead>
<tr>
<th>State</th>
<th>Objective</th>
<th>Number of states</th>
<th>Energy usage (Eu)</th>
<th>Time response (Tr)</th>
<th>Buffer size (Bs)</th>
<th>Count (Co)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>Start=good</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>a2</td>
<td>N=good</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>a3</td>
<td>N=average</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>a4</td>
<td>N=average</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>a5</td>
<td>N=average</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>a6</td>
<td>N=average</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>a7</td>
<td>N=average</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>a8</td>
<td>Goal (G)</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>a9</td>
<td>Goal (G)</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>a10</td>
<td>Goal (G)</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

Table 3: Fuzzy states proposed by the rules.

Fig. 6. Block diagram of the FQL optimization system.
fuzzy states of optimized Q-learning are based on 14 rules. The fuzzy states (S) are \(s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}\) and \(s_{14}\), as seen in Table 3.

Regarding Table 3, ten fuzzy states are considered in modeling the detected attack behavior. Each state is defined by fuzzy energy usage, fuzzy time response, fuzzy buffer size and fuzzy count. The range of these fuzzy states adopts the fuzzy membership function to represent the Q-learning function. Figure 7 illustrates the state diagram of fuzzy Q-learning attack detection for an agent.

Considering that the FQL agent is in the starting state \((s_1)\) it is defined as “Energy usage is low, Time response is low, Buffer size is low and Count is low.” FQL moves toward the goal state \((s_{10})\) with “Eu is high, Tr is high, Bs is high and Co is high.” The fuzzy Q-learning adopts an action based on min–max weighted fuzzy for all subsequent states. In order to find the optimal action, the reinforcement signal \(r(t)\) is used in Eq. (3). The FQL agent assigns a weight to all possible next states based on fuzzy logic controller (FLC). Through association to the threshold value, optimal cost measurement is achieved. Thus, the FLC actions that result in Abnormality greater than \(A_{th}\) should be rewarded with a positive value, while those producing Abnormality lower than \(A_{th}\) should be penalized with a negative value. The reinforcement signal used in this work is formally defined as

\[
r(t + 1) = \begin{cases} 
100, & \text{if } a^k_{\text{measured}}(t) < A_{th} \\
-100, & \text{otherwise}
\end{cases} 
\]

where \(r(t + 1)\) is the reinforcement signal for the Kth iteration \(t + 1\). The value of \(a^k_{\text{measured}}(t)\) is calculated as the min–max weighted average:

\[
\text{Abnormality} = \text{output } (C_j) = \left( \sum_{i=1}^{N} c_i a_i \right) / \left( \sum_{j=1}^{N} c_j \right) 
\]

where \(a_i = [\mu_i(x_0)\mu_j(y_0)]\), \(N\) is the number of rules, \(\alpha_j\) is the degree of truth for rule \(j\), and \(C_j\) is the selected output constant value for the same rule. The rule outputs can be defuzzified using discrete centroid computation based on Eq. (4). The Fuzzy Q-learning algorithm adapts to an artificial immune system, as seen in Algorithm 1.

**Algorithm 1.** FQL algorithm for attack detection.

**Step 1:** Let \(t = 0\), \(Q^0(s, a) = 0\) for all \(s \in A\) and \(a \in A\)

**Step 2:** Initialize action based on fuzzy min–max action = \(\left( \sum_{i=1}^{N} c_i a_i \right) / \left( \sum_{j=1}^{N} c_j \right)\)

\(a_i = [\mu_i(x_0)\mu_j(y_0)]\)

**Step 3:** \(Q(s(t), a) = \sum_{i=1}^{N} c_i(s)q[i, a_i]\)

where \(c_i(s)\) is the degree of truth for the rule

**Step 4:** \(V_i(s(t + 1)) = \sum_{i=1}^{N} \gamma(s(t + 1))\max_a Q[S(t), a]\)

where \(Q(s(t), a)\) is the value of the Q-function for the state \(s(t)\) in iteration \(t\) and the action \(a\).

**Step 5:** Take action and leave the system to evolve to the next state, \(s(t + 1)\).

**Step 6:** Observe the reinforcement signal, \(r(t + 1)\), and compute the value of the new state denoted by \(V_i(s(t + 1))\)

**Step 7:** Calculate the error signal:

\(\Delta Q = r(t + 1) + \gamma \times V_i(s(t + 1)) - Q(s(t), a)\), where \(\gamma\) is a discount factor

**Step 8:** \(q[i, a_i] = q[i, a_i] + \eta \Delta Q \cdot a_i(s(t))\), where \(\eta\) is a learning rate.

**Step 9:** Repeat the above-described process starting from step 2 for the new current state until the convergence is achieved.

**Fig. 7.** State diagram for FQL detection agent, where S is the starting point and G is the goal.

**Fig. 8.** Simulated WSN environment.
The execution of steps 2 through 9 corresponds to the fuzzy Q-learning optimization process. These steps are reiterated until convergence is achieved. In the first step, continuous states and actions are generated through a fuzzy structure. In step 2, the agent uses a min–max action value function that calculates the expected utility of performing a specification in a discrete state.

3.2.5. Module 5: Cooperative Decision Making Module

The Fuzzy Q-learning based artificial immune system principle approach entails detection accuracy through low time complexity, and only afterward begins to formulate a shield policy. The major drawback in the FQL-based AIS theory occurs in cases when attacks are repeated over a short period and significant amounts of time are consumed in the detection phase; thus, defense fails. It can be said that detection precision may be low while the false alert rate could be high. This problem is a worst-case scenario, but it is addressable using a cooperative-detection mechanism (Shamshirband et al., 2013). In this paper, the cooperative decision making module (cooperative-DMM) is employed, combining the outcome from the FMDM and FQVM detectors. A consolidated result is obtained, along with analysis of attack source that portrays what the real cause of the attack may be and the name of the attack if it is known by the system. In this module, cooperation between the two detection modules is vital. They not only collaborate in making the final decision but also in updating each other. For frequent attacks occurring over a short time, a multijoint-based fuzzy Q-learning artificial immune system was implemented to cope with excessive time spent on detection.

3.2.6. Module 6: Response Module

The Response Module (RM) is the task of the acting policy. The action policy updates databases or modifies hosts in the network. For instance, to mimic the natural immune system’s skill of more rapid response to recurring attacks, the response module produces an attack signature and eliminates it from the safe list. Finally, response to the same attack will be faster in a repeat case. The response module functions as a prevention system by taking online action to break the attack instantaneously; however, such system performance incurs additional operating cost.

4. Simulation and analysis

4.1. Simulation setup

To evaluate performance and check the link between Co-FAIS and the routing protocol, NS-2 is simulated. In this work only Distributed Denial-of-Service attacks are considered. A DDoS, also called a flooding attack, is characterized by the presence of an attacker. Flooding attacks cause noise in wireless communication due to sending flooding packets, and also exhaust energy (Ghosal and Halder, 2013). The noise disrupts communication between nodes in the network, preventing them from entering ‘sleep mode’ as a result of the medium getting flooded with messages.

The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was utilized in the simulation, as it most closely reflects wireless sensor networks in practice and is also applicable to dealing with related energy consumption concerns. The simulations were run for 1000 s with LEACH as the routing protocol, the initial access point energy was 100 J, the effective transmission range of the wireless radio for the access point was 100 m, the sink node transmission range was 100 m, the common node transmission range was 50 m and the transport protocol is given in Fig. 8. In addition, the cooperative immune system-based IDS with fuzzy Q-learning, was employed to hasten the simulation.

Table 4 presents the wireless sensor network configuration along with the set of parameters applied in NS-2. However, in practical WSN security operation, minimizing energy usage to conserve energy and maximize detection accuracy as much as possible is vital when designing and running Co-FAIS within efficient IDS. The results obtained from the proposed algorithm are compared with those from the fuzzy logic controller, artificial immune system, and fuzzy Q-learning.

4.2. Generating and analyzing the flood attack strategy (artificial attack dataset)

The purpose of this section is to create artificial attack data and analyze the quantitative behavior of attacks in the UDP protocol layer. In the present experiments, normal UDP traffic was initially considered, after which the attack intensity under flooding attack with UDP traffic was explored. Subsequently, the total energy consumed before and after attack was examined. To generate a flooding attack, we initially developed an attack algorithm. After generating an attack (online), the log file or dataset (attack dataset) was collected in the base station and finally, Co-FAIS was applied to this offline dataset. However, the dataset used is not the same as in literature. Algorithm 2 displays the attack strategy.

Algorithm 2. Attack strategy.

1. Start
2. Min(r)=% Initial round simulation (Max(r)=n)
3. While (r<n)
   4. Decide r round’s cluster head randomly
   5. Cluster head advertises schedule time to all its common nodes
   6. Generate attack node randomly
   7. Attack node receives schedule time message from its cluster head
   8. Attack node starts to compromise victims
   8.1. Attack node sends flooding packets to its cluster head in this round
   8.2. Victim (cluster head) receives data more quickly than normal state, so its energy will decrease rapidly
9. End.

In the experiment, an attack with UDP attack intensity was implemented. Figure 9 indicates flooding attack intensity per packet length. Greater attack intensity percentage obviously occurred between 200 and 300 s, at which time packet length also reached elevated values. In Fig. 10 it appears that UDP attack intensity affected the wireless sensor network’s energy, besides the fact that energy was consumed proportionate to attack
intensity. For example, the most energy was consumed at attack intensities between 100 and 150 s.

While a cluster behaves with high severity but low certainty and short attacking time, it is difficult to determine if this is a malicious attack or not. In this case, we consider the threat profile vector TP (1)=[Eu, Bs, Tr, Co]=[0.6, 0.7, 0.5, 0.1] for the Co-FAIS evaluation. Therefore, the threat profile faces an average of 70% intrusion. In other words, it corresponds to 70% of antigens created in the attack algorithm. The dataset contains 12215 samples belonging to the sensor with attacks (attack class) while the remaining 3785 samples are of the sensor with no attacks (normal class). The class information contained in the dataset signifies 0 for healthy sensors and 1 for infected sensors. In the present research work, three experiment sets were conducted to examine the effects of attack detection accuracy and defense rate against attacks based on the fuzzy logic controller, artificial immune system, and fuzzy Q-learning. The cost function was calculated according to Eq. (1).

4.3. Analysis of the CO-FAIS IDS in terms of detection accuracy

The proposed cooperative-based fuzzy artificial immune system (Co-FAIS) algorithm with the utility function UF = ρ SP − β FN − θ FP was compared with existing soft computing methods (C4.5, dendritic cell algorithm (DCA), artificial immune recognition system (ARIS), clonal selection algorithm (CLONALG), fuzzy logic controller (FLC), artificial immune system (AIS), and fuzzy Q-learning (FQL)) with respect to the attack detection precision of modeled Denial-of-Service (flooding) attacks. An evaluation between the average utility function and Co-FAIS with cost maximization indicates that the latter yielded an improvement over the fuzzy Q-learning algorithm (Table 5).

It is evident that a fuzzy Q-learning based artificial immune system with a cooperative mechanism attained the utmost detection accuracy gain. It can also be inferred from Fig. 11 that detection accuracy per attack percentage is greater with the Co-FAIS algorithm than the other methods.

In Fig. 11, the X-axis represents the percentage of malicious nodes in an attack, and the Y-axis indicates the accuracy rate. At higher attack frequencies, the proposed method (cooperative-based FAIS) displays greater accuracy scores.

4.4. Analysis of cooperative-based FAIS IDS in terms of defense rate

The proposed Co-FAIS method was weighed against that of Huang et al. (2013), who used the Markovian IDS with an attack-pattern-mining algorithm. According to Huang et al. (2013) empirical results, the defense rate effectiveness of non-cooperative-based Markovian IDS with an attack-pattern mining algorithm for 60% of malicious nodes in a network and two sink nodes ranged between 78% and 98% (Fig. 12). With the proposed cooperative-based FAIS IDS, the successful defense rate was between 80% and 99% (Fig. 12). It can be concluded that integrating the cooperative artificial immune system with the fuzzy Q-learning algorithm outperforms individual defense schemes.

Figure 12 points out that the successful defense rate values for Huang et al.’s (2013) model and the proposed method decreased from 100% to 87% once anomaly percentage increased. However, the proposed method gained the advantage of successful defense rate owing to the higher percentage of malicious nodes detected compared to Huang’s lower success rate. It can thus be deduced that by integrating the cooperative artificial immune theory with the fuzzy Q-learning method, performance surpasses that of any other individual defense approach.

4.5. Analysis of cooperative-based FAIS IDS in terms of number of live nodes

An experiment was conducted to evaluate the performance of the Co-FAIS algorithm with regard to the number of live nodes during
simulation runtime. In the current scheme, the number of sensor nodes was 250. Figure 13 displays the number of live nodes for different algorithms throughout the simulation runtime. The simulation outcomes indicate the number of live nodes at the end of the simulation time (1000 s), according to which, the number of live sensor nodes in the proposed Co-FAIS method is significantly greater than existing algorithms. Co-FAIS maintains 53 live nodes against an attack in comparison to 42, 32, and 21 by FQL, ARIS, and FLC, respectively.

The procedure of adjusting rules according to FLC-based DDoS attacks is more time-consuming, and the attacker defeats a high efficiency of an agent in optimizing the cost function further increases and the fuzzy IDS may crash. In this experiment, the energy consumed by the cooperative-based FAIS method enhances energy efficiency by means of optimization.

4.6. Analysis of cooperative-based FAIS IDS in terms of energy consumption over time

In this experiment, the energy consumed by the cooperative-based FAIS algorithm during DDoS attacks on sensor nodes compared to C4.5, DCA, CLONALG, Q-learning, FLC, ARIS, and FQL is studied. Figure 14 provides the comparison between the mentioned algorithms in terms of total energy consumed by sensor nodes.

In existing detection, the detector agent (sink node) and defense player (base station) partake in activities such as local sensing and data reporting, which consume additional energy. The overhead of energy consumption may be extensive if the number of cooperating players or the amount of sensing results in the report is very large. Thus, energy efficiency should be taken into consideration in cooperative schemes. Accordingly, the cooperative-based FAIS method enhances energy efficiency by means of optimization.

4.7. Analysis of the energy consumed by different nodes deployed in the cooperative-based FAIS IDS

The impact of number of deployed sensor nodes on energy consumption is shown in Fig. 15. Clearly, with increasing percentage of deployed nodes, the proposed Co-FAIS is able to consume the energy in contrast to FQL, ARIS, FLC, Q-learning, CLONALG, DCA, and C4.5.
Finally, Fig. 15 depicts the total energy consumed with varying numbers of sensor nodes deployed in the network. The experiment was run for 50, 90, 130, 170, and 250 nodes. As expected, when more nodes are present in the network, the energy consumption rate is lower than with other comparable methods. This is attributed to the fact that the proposed cooperative-based FAIS prefers to maximize its own utility function through the cooperating learning algorithm to avoid energy consumption by sensors from each cluster.

4.8. Analysis of cooperative-based FAIS IDS in terms of time complexity

Pre-processing time entails the time spent for feature extraction and normalization. Training time depends on the number of times the Co-FAIS required training, which in turn depends on the mean square error between iterations reaching the intended minimum. Testing time is the time spent on testing unlabeled instances by weighting. Table 6 shows the comparison of Co-FAIS performance in terms of time consumed during the experiments. It can be deduced that the training time for Co-FAIS was similar to fuzzy Q-learning, but Co-FAIS consumed more testing time than the FLC, artificial immune system, and FQL. The time complexity was calculated using Intel(R) Core (TM) i5-2400, 3.10GHz, 4GB memory (RAM).

The training time for the proposed Co-FAIS method was large (3.22 s) due to ensemble output combination methods such as fuzzy Q-learning, artificial immune recognition system, Q-learning, fuzzy logic controller, clonal selection algorithm, dendritic cell algorithm and C4.5, but better testing time was achieved in Co-FAIS. The speed of Co-FAIS improved when a hybrid classifier was executed, revealing that all modules can be processed in a parallel processor by different engines, to considerably reduce the overall processing time.
Fig. 13. Number of live sensor nodes during simulation runtime.

Fig. 14. Total energy consumption versus number of sensor nodes under malicious attack in time of simulation.

Fig. 15. Total energy consumption versus different numbers of sensor nodes deployed in a network.
5. Conclusion

In this paper, the interaction between attackers, sink nodes and base station was studied, after which an immunology-based FAIS, cooperative fuzzy Q-learning artificial immune (cooperative-FAIS) theoretic defense mechanism was proposed. This system combines the cooperative-based artificial immune theory with fuzzy Q-learning algorithmic elements. As such, the cooperation between the detector sink node agent and response base station players is reinforced to defend against an incoming DDoS attack that may cause congestion and downtime in wireless sensor network communication as a result of flooding packets. The cooperative-FAIS model is an artificial immune strategy construed as multiagent, providing defense against a single attacker. It adds confidence and establishes a reputation as extremely apt in tracking an attacker and protecting the system. This strategy-based cooperative-immune system adapts to continuous self-learning from past attacks and the behavior in the fuzzy Q-learning decision making process to overcome the attacker. By defining incentives for cooperation and disincentives for fraudulent behavior, it has been determined that repeated interaction sustains cooperation, builds confidence and enhances reputation as supplements offered by Co-FAIS. Cooperative theory-based fuzzy Q-learning artificial immune system, as a mechanism in IDS, is an invaluable tool for increasingly securing next-generation complex heterogeneous computing and networking environments against sophisticated attacks and attackers, beyond what is encountered today. A future initiative should be to extend the proposed Co-FAIS mechanism by incorporating data from various attack types and sources to further enhance its decision making capabilities in order to thwart existing or new attacks. Also as part of future research work on complementing cooperative-FAIS, studying a network evolution ary algorithm, such as the imperialist competitive algorithm, is considered of utmost importance.

Acknowledgment

This paper is financially supported by the Malaysian Ministry of Education under the University of Malaya High Impact Research Grants UM.C/625/1/HIR/MoE/PCSIT/12 and UM.C/625/1/HIR/MOHE/SC/13/3.

References

Chen Y, Hwang K. Shielding wireless sensor network using cooperative-FAIS. Cooperative theory-based fuzzy Q-learning artiﬁcial immune system (Co-FAIS) in network and computing environments against sophisticated attacks and attackers, beyond what is encountered today. A future initiative should be to extend the proposed Co-FAIS mechanism by incorporating data from various attack types and sources to further enhance its decision making capabilities in order to thwart existing or new attacks. Also as part of future research work on complementing cooperative-FAIS, studying a network evolution ary algorithm, such as the imperialist competitive algorithm, is considered of utmost importance.

Acknowledgment

This paper is financially supported by the Malaysian Ministry of Education under the University of Malaya High Impact Research Grants UM.C/625/1/HIR/MoE/PCSIT/12 and UM.C/625/1/HIR/MOHE/SC/13/3.

References


