International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1952140

Expressive and Deployable Swarm Intelligence Based Cybersecurity for Wireless Sensor Network

I. Govindharajn[1] ,P. Jeeva[2] , M. Kanimozhi[2], S.Kodieswari[2] , A. Narmadha[2]

[1]Associate Professor, Department of Computer Science & Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, Tamil Nadu, India

[2]UG Student, Department of Computer Science & Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, Tamil Nadu, India

ABSTRACT

Wireless sensor networks (WSNs) play a pivotal role in Cyber Physical Systems (CPSs), particularly for operations such as observing the location and monitoring it. To enhance the cyber security in WSN-enabled CPSs, various researchers have proposed a various category of algorithms, inspired by biological phenomena. These algorithm works on the basis of mobility of head node (Mobile Anchor Node). However, these WSNs mobile anchor node are subject to various types of optimization like Grey wolf optimizer (GWO) and Whale optimization Algorithm (WOA). Complexity is one of the limitation of these algorithm and also it is vulnerable to damage, theft, or destruction of sensitive data, in addition to that interference in services also occur in CPSs. To prevent these cyber-attack, we proposed generic bio-inspired model ie., enhanced Grey wolf optimizer path planning called Swarm Intelligence for WSN Cyber security that addresses drawbacks of prior bio-inspired approaches. In this model WSN enabled Cyber Physical Systems use ID-Based Aggregate Signature Scheme to detect the cyber-attack and keep data integrity.

Keywords: Wireless Sensor Network, Cyber Physical Systems, Enhanced Grey Wolf Optimization, Swarm Intelligence, Aggregate Signature

I. INTRODUCTION

Wireless networks are a promising new technology to enable economically viable solutions to a variety of applications, for example pollution sensing, structural integrity monitoring, and traffic monitoring. A large subset of wireless network applications requires security, especially if the wireless network protects or monitors critical infrastructures. Security in wireless networks is complicated by the broad- cast nature of the wireless communication and the lack of tamper-resistant hardware (to keep per-node costs low). In addition, wireless nodes have limited storage and computational resources, rendering public key Cryptography impractical. In this section, we investigate the Sybil attack, a particularly harmful attack in wireless networks. In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by imitating other nodes or by claiming false identities. In the worst case, an attacker may generate an random number of additional node identities, using only one physical device.

The proposed system systematically analyzes the Sybil attack and its defenses in wireless networks. This paper makes the following contributions. We introduce a taxonomy of the different forms of the Sybil attack as it applies to wireless networks. We

analyze how an attacker can use the different types of the Sybil attack to perturb or compromise several wireless network protocols. We propose several new defenses against the Sybil attack, including radio resource testing, key validation for random key pre distribution, position verification, and registration. Through quantitative analysis, we show that the radio resource testing method is very elective given the assumption that a malicious node cannot send on multiple channels simultaneously. We also present a quantitative evaluation for the random key pre distribution approach showing that it is robust to compromised nodes. In particular, we show that in the multi-space pair wise scheme storing more than 50 keys at each node, the attacker would have to compromise more than 50 nodes before having even a 5% chance of being able to forge new identities for the Sybil attack.

PRIVACY protection of wireless ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, one has to get access to wired cables so as to eavesdrop communications. In contrast, the attacker needs an appropriate transceiver to receive wireless signal without being detected. In wired networks, devices like desktops are always static and do not move from one place to another place. Hence in wired networks there is no need to protect the user's mobility behavior or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments. Otherwise, an adversary is able to profile users corresponding to their behaviors, and endanger or harm users based on such information. Lastly, providing privacy protection for ad hoc networks with low-power wireless devices and low-bandwidth network connection is a very difficult task. With regard to privacy-related notions in communication networks, we follow the terminologies on anonymity, unlinkability, and unobservability. These notions are defined with regard to item of interest (IOI, including senders, receivers, messages, etc.) as follows:

- AnAnonymity is the state of being not identifiable within a set of subjects, the anonymity set.
- AnUnlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view.
- AnUnobservability of an IOI is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

In above definitions, the related and unrelated subjects refers to subjects involved or not involved in network operations like routing or message forwarding. Privacy protection in routing of WIRELESS NETWORK has interested a lot of research efforts. A number of privacy-preserving routing schemes had been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in WIRELESS NETWORK, most of them exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to an incomplete content protection. The Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which breaks the unlinkability and may lead to source trace back attacks. Meanwhile, an unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to attain complete unlinkability and unobservability. Unfortunately, unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to the attackers. Then the passive attacker can mount traffic analysis based on packet

type. In this case, it is preferable to make traffic content completely unobservable to outside attackers so that the passive attacker only overhears some random noises. However, this is far from an easy task because it is extremely difficult to hide information on packet type and also node identity. Furthermore, a hint on using which key for decryption should be provided in each of the encrypted packet, which demands careful design to remove linkability. Another drawback of most previous schemes is that they rely heavily on public key cryptography, and thus it incur a very high computation overhead. Among these requirements an unobservability is the strongest one in that it implies not only anonymity but also unlinkability.

To achieve unobservability. To achieve unobservability, a routing scheme should provide unobservability for both content and the traffic pattern. Hence we further refine unobservability into two types:

1. Content Unobservability, referring to no useful information can be extracted from content of any message;
2. Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

Unlinkability: Let us consider the three types of packets defined in Section III-B2. In these packets, they are identified by pseudonyms which are generated from random ones and secret session keys. The n onces are only used once and never reused, and so are the pseudonyms. Except the random nonce and the pseudonym, the remaining part of message, including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for the global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key. He even has no idea of the type of the packet being transmitted in the network, and he cannot relate different packets in terms of packet type.

Unobservability. In RSSI, RREQ, RREP and data packets are indistinguishable from dummy packets to a global outside adversary. Meanwhile, the nodes involved in the routing procedure are anonymous to other valid nodes. Consequently, RSSI provides unobservability as defined for ad hoc networks. First of all, a global adversary cannot distinguish different packet types, and neither can he distinguish a meaningful cipher text from random noise. Moreover, a node chooses the nonce randomly and never reuses it. The nonce is updated each time after it is used, so there is no linkage between the pseudonyms which are computed from nonces. Only those wireless nodes with valid session keys can recognize valid pseudonyms and decrypt the corresponding cipher texts to obtain meaningful plaintexts from them. Secondly, a node and its next-hop node or previous-hop node on route establishes a session key anonymously, hence no one is able to know real identities of its next-hop node or previous-hop node. Even source and destination node do not know real identities of the intermediate nodes on route.

Node Compromise. Node compromise is easy for the adversary and highly possible in ad hoc networks, hence it is crucial for a privacy-preserving routing protocol to withstand security attacks due to node capture. In this case, the privacy information leakage is unavoidable due to secret exposure, while our routing protocol can protect user privacy against serious node compromise. Suppose a node is compromised by an attacker, then his private signing key and ID-based encryption key are disclosed to the attacker. The attacker now is able to establish keys with neighboring nodes, but only the following information can be obtained by the attacker: i) the

type of a received packet; ii) data/RREP packets sent to/via the compromised node; iii) headers of packets relayed by the compromised node; iv) RREQ packets sent from the compromised node's neighbors. The attacker is not able to obtain more beyond this information. From this information, attacker cannot infer: 1) the location of the source/destination node; 2) real identities of source/destination node of the relaying packets; 3) source/destination node of the RREQ packets. That is, the privacy leakage due to node compromise is limited within the compromised node's neighborhood, and privacy information like identity and location is still well protected by RSSI. Even if the global attack exploits the compromised node's secret credential for a global attack, RSSI's resilience against privacy leakage can still offer satisfactory protection, due to its per-hop protection of packets. As described, RREP and data packets are encrypted hop-by-hop, and one time nonces and pseudonyms are used to provide unlinkability and unobservability. Only if RREP or data packets pass through the compromised node can the attacker know the packet type. Even if the compromised node happens to be on route, as an intermediate node, the attacker has no clue on where the source node or the destination node is. If the attacker tries to imitate as the source node to request a route to a specific node, the attacker is still not certain where the destination node is in any case.

Collision Attacks. For the colluding outsiders, privacy information is perfectly protected with RSSI. As the attacker is unable to distinguish a meaningful packet from a dummy packet, RSSI can provide complete protection for privacy with an appropriate traffic padding scheme. Even if a target node is surrounded by more than one attack node, given the assumption that no node is totally surrounded by compromised nodes, the attacker is unable to perceive anything except some random dummy packets. If appropriate dummy traffic is injected into network, the colluding outsiders cannot gain any privacy information about the network at all. For the colluding insiders, RSSI still offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by RSSI. The attackers are able to know: i) a target node is involved in a route discovery procedure since it is broadcasting a RREQ packet; ii) a target node is the previous hop or next hop on the path. However, the colluding insiders are not able to know an identity of the target node or other intermediate nodes on route. According to the design of RSSI, authentication and key establishment is achieved by group signature, which perfectly protects user identity from disclosure. Consequently, unobservability is guaranteed by RSSI under colluding insider attacks according to the definition of unobservability.

Sybil Attacks. In Sybil attack a single node presents multiple fake identities to other nodes in the network. The Sybil attacks pose a great threat to decentralized systems like peer-to-peer networks and geographic routing protocols. Thus, it is impossible for adversary to obtain other valid identities except the compromised ones. Nevertheless, the anonymity feature of RSSI allows the adversary to launch Sybil attacks which are similar to collusion attacks discussed above. As discussed in the collusion attack part, RSSI is able to count such attacks effectively.

The Sybil attacker can cause damage to the ad hoc networks in several ways. For example, the Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, the Sybil attacker can change the

whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, the Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, the Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic. Therefore, the Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect the Sybil attacks and eliminate them from the network. The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or a trusted certification. However, this approach is not suitable for the mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered as one of the most promising solutions for wireless ad hoc networks.

II. RELATED WORK

STRUCTURAL HEALTH MONITORING SYSTEMS

Usage of wireless sensor networks in structural health monitoring systems has gained more interest because of its reduced installation cost and maintenance cost. SHM system is used to keep a periodic check on critical infrastructure like bridges and stadiums to ensure public safety. Scalability, sensor placement, data processing issues are addressed in this paper.

ENERGY EFFICIENT ALWadHA ALGORITHM

Efficient working of WSN is based on the positioning of sensor nodes called localization. Many localization algorithm are developed yet in this paper energy efficient localization is proposed.it uses ALWadHA (An efficient Localization algorithm for Wireless ad hoc sensor networks with High Accuracy).

Impacts of three approach is revised in this paper.at first single estimation approach is used, in this a node is allowed to calculate its position only one. Second dynamic power control is used, in this, Based on the distance the node is allowed to broadcast the location request to its neighboring nodes. Last incremental and exponential requesting approach is used to control the frequency rate.

REVIEW ON CLUSTERING

To explore the oceanic source of energy underwater Wireless Sensor Network (UWSN) is used in underwater acoustic Sensor Networks limited availability of energy inaccessability of some employed sensor. To rectify these issues several techniques emerged. One such technique is clustering. Clustering is used to increase scalability and to reduce the cost. It also covers the area of coverage and connectivity.

III. EXISTING SYSTEM

We gathered some of the data about optimization algorithm for cyber security. Some of the algorithms used are Particle swarm optimization (PSO), Genetic Algorithm (GA), Ant Colony Optimization (ACO), Grey Wolf Optimization (GWO), Whale Optimization Algorithm (WOA). These are computational method that optimizes a problem by iteratively trying need not to improve a candidate solution with regard to a given measure of quality. This methods are optimized a problem by having a population of candidate solutions and moving these nodes around in the search-space according to simple mathematical formulae over the node's position and velocity. Each node's movement is influenced by its local best known position but, is also guided toward the best known positions in the search-space, which are updated as better positions are found by other nodes. Particle swarm optimization– which identifies the cluster head. Cluster head is responsible for collecting the

data across its network area and transmit the data to base station. Cluster head is selected on the basis of node having higher probability obtained from the PSO result. Genetic Algorithm (GA)-is a search heuristic that is inspired by Charles Darwin's theory of natural evolution, used to find the efficient cluster members. Ant Colony Optimization (ACO) – which is used to find the optimized path through graph. This algorithm is inspired by the food-seeking behavior of real ants, the ant system is a cooperative population-based search algorithm. As each ant construct a route from nest to food by stochastically following the quantities of pheromone level, the intensity of laying pheromone will bias the path-choosing decision-make of subsequent ants. Grey Wolf optimization (GWO) - is a meta-heuristic technique inspired by grey wolves (Canis lupus). The GWO algorithm imitates the dominant hierarchy and hunting mechanism of grey wolves. Four types of grey wolves such as alpha(α), beta(β), delta(δ), and omega(ω) in which each of these higher level subgroup will lead its lower level subgroups. In addition, the three main steps of hunting includes searching for prey, encircling prey, and attacking prey are implemented. Based on the candidate solution the best solution is identified. In WSN, this technique is employed to find the attacker and finally Whale Optimization Algorithm (WOA)- is algorithm inspired by humpback whales hunting mechanism. It includes three operations to simulate the search for prey, encircling prey, and bubble-net foraging behavior. In WSN, this technique is employed to increase the transmission rate between nodes.

DISADVANTAGES

1) It resolves the economic dispatch problem for considering complex problems to be tackled.
2) It has many complex optimization problems.

IV. PROPOSED SYSTEM

OBJECTIVES:

- The main objective of this project is to strengthen cyber security in WSN-enabled CPSs.
- To overcome the high computational problem in the existing system.
- To accurately detect the cyber-attack like Denial-of-service Attacks, passive attack, active attack, Impersonation Attacks, Modification/ fabrication attacks.
- It can keep data integrity, and also reduce bandwidth and storage cost for wireless sensor networks.

MODULES INVOLVED:

The flow of the proposed system is explained. Whenever the system starts it will form a network. The network consist of certain number of nodes. All the nodes will be browsed. In order to search the sink node, a heuristic searching algorithm will be applied. If the required node is present then statistical traffic analysis will be performed in it. Then the probability distribution will discover the traffic pattern. However, if the required node is not found then no further process will be carried out and the system will terminate.

1. NETWORK FORMATION

NODE CONFIGURATION SETTING

The sensor nodes are designed and configured dynamically, which are employed across the network. The nodes are set according to the X, Y, Z dimension, so that the nodes can have direct transmission range to all other nodes.

TOPOLOGY DESIGN

This module is developed to design the Topology of all nodes that are placed at particular distance. Without using any cables, the data packets are

transmitted and received using wireless mobile equipment. The cluster head is at the center of the circular network area. It is the intermediate between sender and receiver of its sensing area.

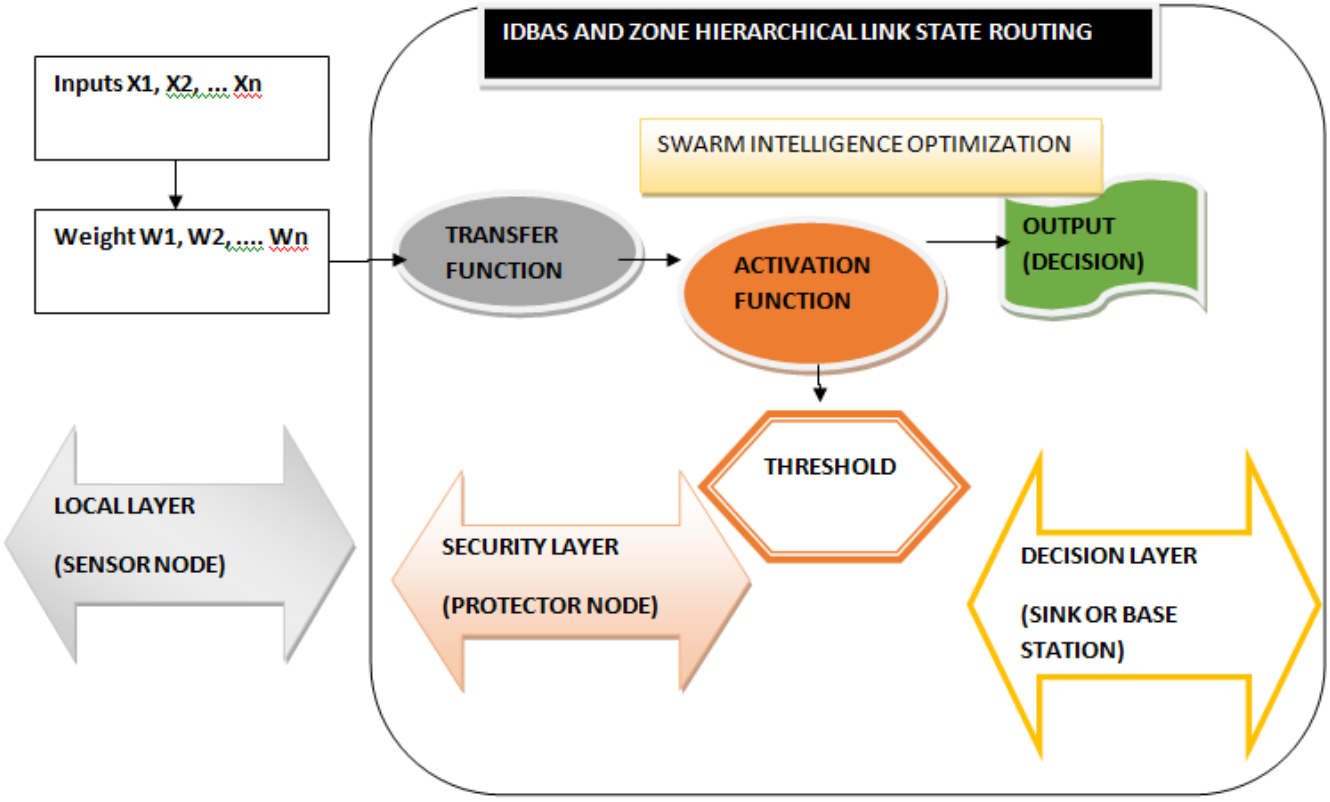
NODE CREATIING

This module is developed to node creation and more than 30 nodes placed particular distance. Mobility node placed at intermediate area. Each node knows its location in relative to the sink node. The access point has to receive the transmitted packets then send acknowledge to the transmitter.

Zone Based Hierarchical Link State Routing Protocol

Zone Based Hierarchical Link State Routing Protocol (ZHLS) is one of the hybrid routing protocols in the Mobile ad-hoc network, which is vulnerable to a large number of security threats that come from internal malicious nodes. It is observed from the recent survey that not much work has been done in the hybrid routing protocol in a way to provide security to the information that is passed between the nodes. In this proposed methodology, the author concentrates on providing security to the hybrid routing protocol i.e. the Zone Based Hierarchal Link State Routing Protocol by employing traditional Digital Signature technique. The Symmetric and Asymmetric key encryption technique are introduced while sending and in receiving information between two or more nodes. The detailed procedure of proving security to the information packets.

Prior to sending the data packets, the source primarily examines its intra zone routing table. The routing information exist in the system, if the destination node and source node is in the same zone. Otherwise, the source node initiates a locality request to remaining zone with the help of gateway nodes. Then, a gateway node of the zone where the destination node exist, attains the locality appeal and



ARCHITECTURE DIAGRAM

responds with a locality reply encompassing of the zone ID of the destination. The zone ID and the node ID of the destination node are given in the header of the data packets initiated from the source node. At the time of packet progressing technique, intermediary nodes excluding nodes in the destination zone make use of inter-zone routing table, and an inter-zone routing table is employed when the packet reaches destination.

2. NEIGHBOR DISCOVERY PHASE

This phase is neighbor discovery phase, each source node identifies its neighbor nodes through broadcasting hello packets, through this process each node detects its neighbor nodes corresponding to location and distance. Based on the neighbor discovery phase each node forms a stable path to destination.

3. ROUTING OVERHEAD:

The ratio of the total size of control packets (include RREQ, RREP, RERR, and Hello) to the total size of data packets delivered to the destinations. For the control packets sent over multiple hops, each hop is counted as one transmission. To preserve fairness, we use the size of RREQ packets instead of the number of RREQ packets, because the DPR and OLSRprotocols include a neighbor list in the RREQ packet size is bigger than that of the original AODV.

Source node route the packets through more stable node to transfer packets to destination. The performance is analyzed.

4. DATA ROUTING

Source node route the packets through more stable node to transfer packets to destination.

The performance is analyzed through graphical result.

The list of attacks involved in this phase as follows:

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 send new malicious attacks. To protect nodes, WSNs should be able to conceal messages from unauthorized access (**confidentiality**).

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.

5. GRAPH EXAMINATION

The performance analysis of our proposed work is examined through graphical analysis.

ADVANTAGES:

1. **Scalability:** Scalability of routing protocols which used in wireless sensor networks is a critical issue due to high node numbers and relatively high node density. A good routing protocol has to be scalable and adaptive to changes in the network topology. Thus protocols must perform well as the network grows larger or as workload increases. In this paper, we provide scalability to overcome this issue.

2. **Security:** The secured link between the sink and the sending node in the WSN is a vital factor in

many applicable fields. In this, the different threats are analyzed and rectified by swarm intelligence technique which is a machine learning approach.

3. It also avoids the malicious nodes while transmission process.

V. EXPECTED OUTCOME

This project is mainly focus that to strengthen cyber security in WSN-enabled CPSs in bio-inspired methods. This will be an high computational complexity which contribute several input parameters and these can be a generic bio-inspired model that uses a machine learning-based approach.

- To overcome the high computational problem
- Accurate and faster detection of cyber-attack
- It can keep data integrity, and also can reduce bandwidth and storage cost for Swarm Intelligence Technique.

VI. CONCLUSION

As the cyber-attacks continue to become more sophisticated and occur with greater frequency. In this work, we focused on WSN cyber security, which is an integral part of many CPSs. In reviewing various bio-inspired approaches to enhance the cyber security 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- tem trained by swarm intelligence optimization to automatically determine the optimal critical parameters used to detect cyber-attacks.

VII. REFERENCES

[1]. Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems," IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 550–586, Firstquarter 2017.

[2]. L. M. Borges, F. J. Velez, and A. S. Lebres, "Survey on the characterization and classification of wireless sensor network applications," IEEE Communications Surveys Tutorials, vol. 16, no. 4,pp. 1860–1890, Fourthquarter 2014.

[3]. H. Karl and A. Willig, Protocols and architectures for wireless sensor networks. Hoboken, NJ: Wiley, May 2005.

[4]. A. B. Noel, A. Abdaoui, T. Elfouly, M. H. Ahmed, A. Badawy, and M. S. Shehata, "Structural health monitoring using wireless sensor networks: A comprehensive survey," IEEE Communications Surveys Tutorials, vol. 19, no. 3, pp. 1403–1423, third quarter 2017.

[5]. D. N. Sandeep and V. Kumar, "Review on clustering, coverage and connectivity in underwater wireless sensor networks: A communication techniques perspective," IEEE Access, vol. 5, pp. 11 176–11 199, 2017.

[6]. A. M. Abu-Mahfouz and G. P. Hancke, "Alwadha localization algorithm: Yet more energy efficient," IEEE Access, vol. 5, pp. 6661–6667, 2017.

[7]. Y. S. Chen, D. J. Deng, and C. C. Teng, "Range-based localization algorithm for next generation wireless networks using radical centers," IEEE Access, vol. 4, pp. 2139–2153, 2016.

[8]. A. Alomari, W. Phillips, N. Aslam, and F. Comeau, "Dynamic fuzzy-logic based path planning for mobility-assisted localization in wireless sensor networks," Sensors, vol. 17, no. 8, 2017.

[9]. S. Halder and A. Ghosal, "A survey on mobile anchor assisted localization techniques in wireless sensor networks," Wireless Networks, vol. 22, no. 7, pp. 2317–2336, 2016

[10]. N. A. Alrajeh, M. Bashir, and B. Shams, "Localization techniques in wireless sensor networks," International Journal of DistributedSensor Networks, vol. 9, no. 6, p. 304628, 2013.

[11]. G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani, and G. K. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2220–2243, thirdquarter 2016.

[12]. S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," Advances in Engineering Software, vol. 69, pp. 46 – 61, 2014.

[13]. S. Mirjalili and A. Lewis, "The whale optimization algorithm," Advances in Engineering Software, vol. 95, pp. 51 – 67, 2016.

[14]. A. Alomari, F. Comeau, W. Phillips, and N. Aslam, "New path planning model for mobile anchor-assisted localization in wireless sensor networks," Wireless Networks, pp. 1–19, 2017.

[15]. D. Koutsonikolas, S. M. Das, and Y. C. Hu, "Path planning of mobile landmarks for localization in wireless sensor networks," Comput. Commun., vol. 30, no. 13, pp. 2577–2592, Sep. 2007.

Cite this Article

I. Govindharajn, P. Jeeva, M. Kanimozhi, S. Kodieswari, A. Narmadha, "Expressive and Deployable Swarm Intelligence Based Cybersecurity for Wireless Sensor Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 761-770, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT1952140

Journal URL : http://ijsrcseit.com/CSEIT1952140