International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Performance Analysis for IDBAS and LWSEA Cryptography Technique in Generic Bio-Inspired Cybersecurity in SIWC model for WSN

A. V.Vivekia, Dr. N. Kumaratharan
Department of Information Technology, Sri Venkateswara College of EngineeringChennai, Tamil Nadu, India

ABSTRACT

The expeditious advances of Information Technology (IT) and Communication Technology have led in various Cyber-Physical Systems (CPSs) such as smart traffic flow management, healthcare platforms, Internet of Things and computer networks. In current days the Wireless Sensor Networks (WSNs) play a pivotal role in CPSs, particularly for operations such as surveillance and monitoring. However, these WSNs are vulnerable to various types of security attacks known as cyber-attacks. To strengthen cybersecurity in WSN-enabled CPSs, a generic bio-inspired model called Swarm Intelligence is proposed. Swarm Intelligence for WSN Cybersecurity (SIWC) is a system trained by swarm intelligence optimization to automatically determine the optimal critical parameters that are used to detect cyberattacks using SIDS and prevent them by using cryptography LWSEA techniques.

Keywords: Cyber-physical systems (CPSs), Cybersecurity, Cyberattacks, Swarm Intelligence for WSN Cybersecurity (SIWC), Swarm based Intrusion Detection System (SIDS), Light-weight Symmetric Encryption algorithm (LWSEA).

I. INTRODUCTION

A WSN is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

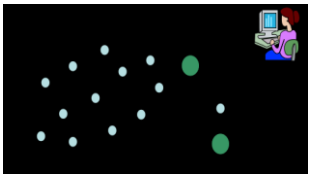

Figure 1. Typical multi-hop Wireless Sensor Network architecture

They usually consist of a processing unit with limited computational power and limited memory, sensor MEMS (Micro-Electro Mechanical Systems) (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. A WSN is a group of specialized transducer with a communications infrastructure for monitoring and recording conditions at diverse locations.

A. Characteristics of WSNs
The main characteristics of a WSN include:

- Ability to cope with node failures (resilience)

- Some mobility of nodes for highly Mobile WSN (MWSNs)
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers, which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. The interference between the different users, access conflicts, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

So the cross-layer can be used to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, Quality of Service (QoS), etc. Sensor nodes can be imagined as small computers which are extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors or Micro-Electro Mechanical Systems (MEMS), a communication device.

B. Applications of WSN

Wireless sensor networks have gained considerable popularity due to their flexibility in solving problems in different application domains and have the potential to change our lives in many different ways. WSNs have been successfully applied in various application domains

- Military applications: WSN are likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.
- Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored. When the sensors detect the event being monitored (heat, pressure etc.,), the event is reported to one of the base stations, which then takes appropriate action.
- Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.
- Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.
- Environmental sensing: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc.
- Industrial monitoring: WSN have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.
- Agricultural sector: Using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.
- Forest fire detection: A network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced.

C. Protocols of WSN

The traditional protocols have several shortcomings when applied to WSNs and the following are the protocols that are used for my system.

- On-demand Routing Protocols

In on-demand trend, routing information is only created to requested destination. Link is also monitored by

periodical Hello messages. If a link in the path is broken, the source needs to rediscovery the path. On-demand strategy causes less overhead and easier to scalability. However, there is more delay because the path is not always ready. The following part will present AODV, DSR, TORA and ABR as characteristic protocols of on-demand trend.

- AODV Routing

Ad hoc on demand distance vector routing (AODV) is the combination of Destination-Sequenced Distance Vector (DSDV) and Dynamic Resource Routing (DSR). In AODV, each node maintains one routing table. Each routing table entry contains Active neighbour list, a list of neighbour nodes that are actively using this route entry. Once the link in the entry is broken, neighbour nodes in this list will be informed. Destination address Next-hop address toward that destination Number of hops to destination Sequence number for choosing route and prevent loop Lifetime time when that entry expires Routing in AODV consists of two phases Route Discovery and Route Maintenance. When a node wants to communicate with a destination, it looks up in the routing table. If the destination is found, node transmits data in the same way as in Destination-Sequence Distance Vector (DSDV). If not, it start Route Discovery mechanism source node broadcast the Route Request packet to its neighbour nodes, which in turns rebroadcast this request to their neighbour nodes until finding possible way to the destination.

When intermediate node receives a Route Request (RREQ), it updates the route to previous node and checks whether it satisfies the two conditions:

- There is an available entry which has the same destination with RREQ
- Its sequence number is greater or equal to sequence number of RREQ.

If no, it rebroadcast RREQ. If yes, it generates a Route Reply (RREP) message to the source node. When RREP is routed back, node in the reverse path updates their routing table with the added next hop information. If a node receives a RREQ that it has seen before it discards the RREQ for preventing loop.

If source node receives more than one RREP, the one with greater sequence number will be chosen. For two RREPs with the same sequence number, the one will less number of hops to destination will be chosen.

II. ALGORITHMS

A. Swarm Intelligence Algorithm

All of the nodes are cluster members. A local voting scheme is performed at each node's neighbourhood 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. 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.

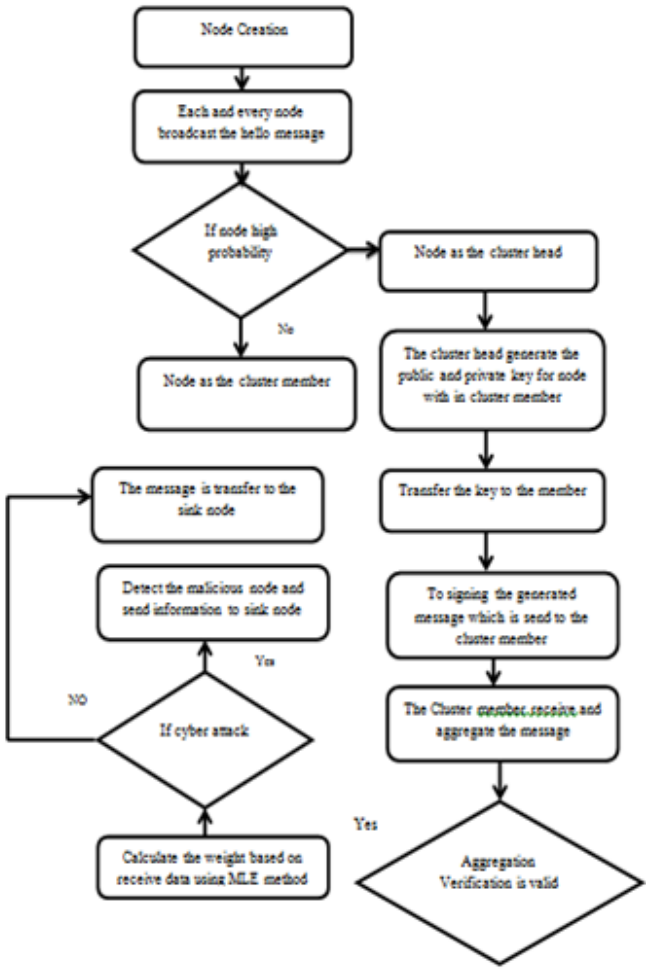

Figure 3. Block Diagram

B. Ant Colony Optimization Algorithm

WSN consisting of nodes with limited power are deployed to gather useful information from the field. In WSNs it is critical to collect the information in an energy efficient manner. ACO, a swarm intelligence based optimization technique, is widely used in network routing. A novel routing approach using an ACO is proposed for WSN consisting of stable nodes.

III. EXISTING SYSTEM

In the existing system, cybersecurity model Swarm Intelligence for WSN Cybersecurity with Enhanced ID-Based Aggregate Signature Scheme of encryption algorithm to detect the cyberattacks and keep data integrity. In our system, each sensor node belongs to one cluster, sends messages and its signatures to their aggregator, and the messages will finally be sent to data control packets to the corresponding protector node (the cluster head) to calculate the probability of an attack. After receiving weighted parameters received from the corresponding sensors. The Maximum Likelihood Estimation MLE method is trained to find the best values, which promote the highest probability of cyberattacks detection. The found probabilistic value is compared to a prefixed threshold, which represents the cyberattacks 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. It verifies the node aggregated signature if valid then forward the information to the base station else it integrate the forgery message then detect the coalition attack in the network. So in proposed the network life time, throughput, energy consumption, packet delivery ratio, end to end delay are increased.

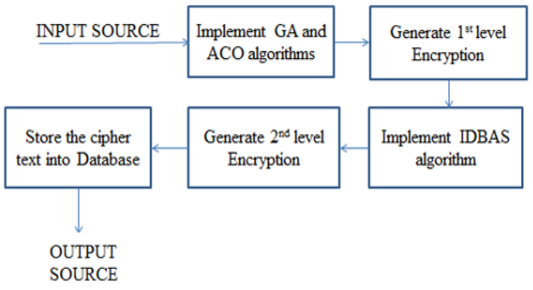

Figure 4. Block diagram

IV. PROPOSED SYSTEM

In the proposed System, the recent years WSNs are vulnerable to various types of security attacks known as cyber-attacks. 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. But the sensor data is easy to be intercepted by attackers. It is necessary to adopt some encryption measurements to protect data of WSNs. The bio-inspired model is used for detection of the cyber-attack like Eavesdropping Attack, DOS attack and the proposed light-level symmetrical encryption algorithm: LWSEA with bio-inspired model. In this mechanism is adopt the minor encryption rounds, shorter data packet and simplified scrambling function. After encryption perform. Finally our evaluation result shows proposed method prevent the network security attack in the WSN and also reduce the encryption and decryption time, a comparison graph is evolved of IDBAS and LWSEA.

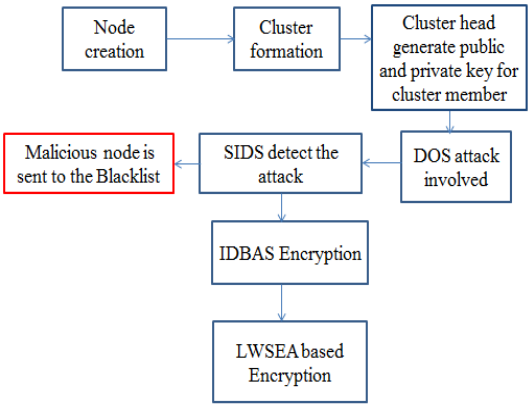

Figure 5. Block diagram of LWSEA

V. METHODOLOGY

When the system will start it will form a network. This network will consist of certain number of nodes. All the nodes will be browsed. In order to search the 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 the system will stop and no further process will be carried out.

A. Network Formation

The network formation module describes about how the nodes configuration setting takes place, how the network topology designed, node creation, and zone based hierarchical link state routing protocol.

1) Node Configuration Setting

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

2) Topology design

In Topology design all the node place particular distance. Without using any cables then fully wireless mobile equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The cluster head is at the centre of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

3) Node Creating

Node Creating is developed to node creation and more than 40 nodes placed particular distance. Mobility node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

4) 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 Symmetric and Asymmetric key encryption technique are introduced while sending and in receiving information between two or more nodes. Prior to sending the data packets, the source primarily examines its intrazone 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 responds with a locality reply encompassing of the zone Identification (ID) of the destination

B. Neighbour Discovery

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

1) Routing Overhead

The ratio of the total packet size of control packets (include RREQ, RREP, RERR, and Hello) to the total packet size of data packets delivered to the destinations. For the control packets sent over multiple hops, each single 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 OLSR protocols include a neighbour list in the RREQ packet and its size is bigger than that of the original AODV.

2) Data Routing

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

COALITION ATTACK

The adversary in our security model has the capability to launch any coalition attacks. If an adversary can use some single signatures including invalid ones to generate a valid aggregate signature, we say that the attack is successful.

VI. EXPRIMENTAL RESULTS AND DISCUSSION

A. NS2

Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an on-going effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS is written in C++, with an OTcl interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios.

B. Network Components

This section talks about the NS components, mostly compound network components. Figure 4.2 shows a partial OTcl class hierarchy of NS, which will help understanding the basic network components. The root of the hierarchy is the Tcl Object class that is the super class of all OTcl library objects (scheduler, network components, timers and the other objects including Network Animator (NAM) related ones). As an ancestor class of Tcl Object, Ns Object class is the super class of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links. The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output DATA paths. The basic network and objects that have only one output DATA path are under the Connector class, and switching objects that have possible multiple output.

C. Benefits

- Low cost:

There is no need to spend time and money to obtain licenses since Linux and much of its software comes with the GNU General Public License. It is able to start working immediately without worrying that your software may stop working anytime because the free trial version expires.

- Stability:

Linux doesn't need to be rebooted periodically to maintain performance levels. It doesn't freeze up or slow down over time due to memory leaks and such. Continuous up-times of hundreds of days (up to a year or more) are not uncommon.

- Performance:

Linux provides persistent high performance on workstations and on networks. It can handle unusually large numbers of users simultaneously, and can make old computers sufficiently responsive to be useful again.

- Flexibility:

Linux can be used for high performance server applications, desktop applications, and embedded systems. You can save disk space by only installing the components needed for a particular use. You can restrict the use of specific computers by installing for example only selected office applications instead of the whole suite.

- Compatibility:

It runs all common UNIX software packages and can process all common file formats.

- Multitasking:

Linux is designed to do many things at the same time e.g., a large printing job in the background won't slow down your other work.

- Security:

Linux is one of the most secure operating systems. "Walls" and flexible file access permission systems prevent access by unwanted visitors or viruses. Linux users have to option to select and safely download software, free of charge, from online repositories containing thousands of high quality packages. No purchase transactions requiring credit card numbers or other sensitive personal information are necessary.

D. Parameter Factors

PARAMETERS	DESCRIPTION
Number of nodes	48
Number of clusters	3
Number of cluster head	3
Routing algorithm	SIWC and ACO
Type of WSN	Mobile WSN
Protocol	On-demand routing and AODC protocols
Initial Energy	100 Joules
MAC type	IEEE 802.11
Idle Power	0.02 Joules
Transceiver Power	1.0 Joules
Receiver Power	0.8 Joules
Simulator	Ns2
Simulation time	31.6 ms

This type of conversation is relatively easy to handle, provided there are no major changes in the system. Each program is tested individually at the time of development using the data and has verified this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. NS2 is the best-known network simulator that supports WSNs, various illustration and representations are made to clearly depict the working.

E. Performance Analysis

1) Performance of PDR

Fig.8, the packet delivery ratio in percentage is close to 90% for most of the stability period. This ensures a smooth operation and reliable network operation.The packet delivery ratio (PDR) is prescribed by the number of packets accepted to that of the number of packets directed towards destination. It is desired that the PDR remains as high as possible. The protocol is designed such that most of the nodes die simultaneously so that they are alive together for most of the time thereby maintaining the prolonged stability zone.

2) PDR = (recv/sends)*100; # pdr [fraction]

3) 2) Performance of Network Lifetime

Fig.6, Network lifetime increases with level of heterogeneity. First node dead of all heterogeneity levels are compared as shown in Fig.6, which shows as level of heterogeneity increases, the period between network creation and first node dead increases.

Network Lifetime = (sumpacket/recvnum)

4) Performance of End to End Delay

Fig.7, End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from round-trip time (RTT).

Average Delay = (Total Delay / count)

5) Performance of Throughput ratio

Fig.4, To measure the total rate of data sent over the network, the rate of data sent from cluster heads to the sink as well as the rate of data sent from the nodes to their cluster heads. The throughput ratio according to the equation is given by

Throughput = (receiver/time)*(8/1000)

6) Performance of Energy consumption

The energy consumption rate for sensors in a wireless sensor network varies greatly based on the protocols the sensors use for communications. Results for energy consumption, transmitted and received power, minimum voltage supply required for operation, effect of transmission power on energy consumption, and different methods for measuring lifetime of a sensor node are presented.

Energy = (Power * time)

F. Screen shots

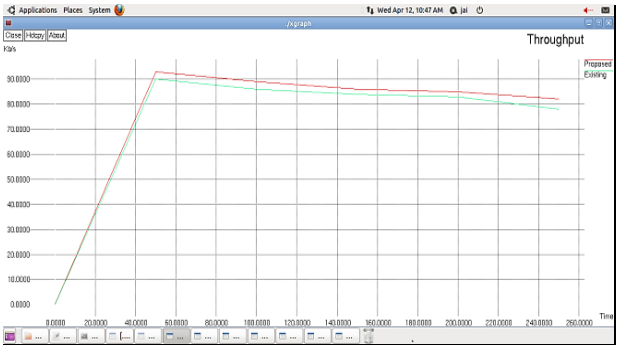

Figure 5. A Throughput Graph between existing and proposed system

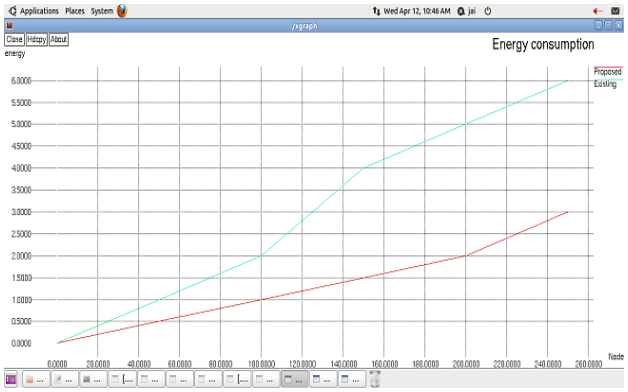

Figure 6. A Energy consumption Graph between existing and proposed system

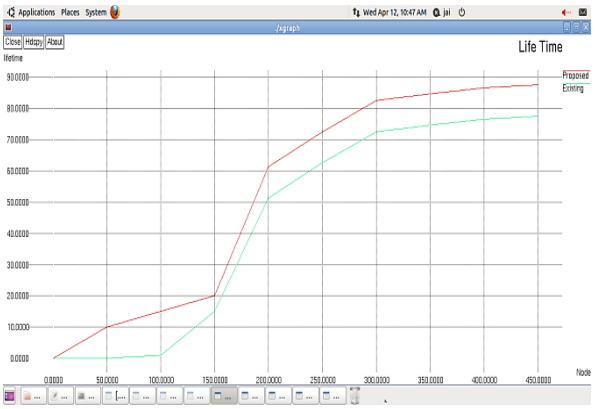

Figure 7. A Network Life time Graph between existing and proposed system

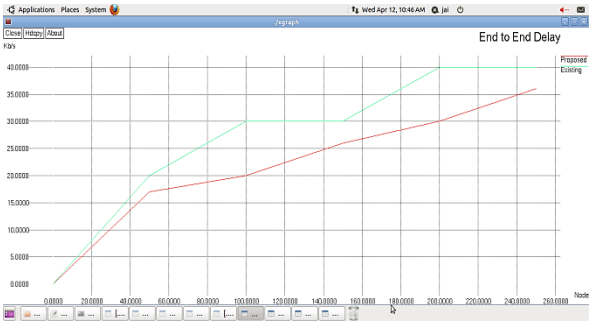

Figure 8. An End to End Delay Graph between existing and proposed system

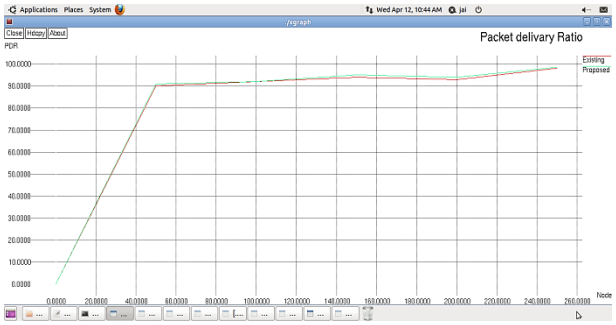

Figure 9. A Packet Delivery Ratio Graph between existing and proposed system

VII. CONCLUSION AND FUTURE ENHANCEMENT

The proposed work is 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 Trust value concept and Enhanced Identity Based encryption algorithm for providing security. SIWC uses key distribution and SIDS technique which are used for swarm intelligence optimization and automatically determine the optimal critical parameters used to detect cyberattacks and the LWSEA prevent them from the cyberattacks.

In future, the most of the current research is in the direction of increasing the number of problems that are successfully solved by Swarm Intelligence algorithms, including real-word, industrial applications. Currently, the great majority of problems attacked by Swarm Intelligence are static and well defined combinatorial optimization problems, that is, problems for which all the necessary information is available and does not change during problem solution. For this kind of problems Swarm Intelligence algorithms must competes with very well established algorithms, often specialized for the given problem. Also, very often the role played by local search is extremely important to obtain good results. Although rather successful on these problems, we believe that Swarm Intelligence algorithms will really evidentate their strength when they will be systematically applied to "ill-structured" problems for which it is not clear how to apply local search, or to highly dynamic domains with only local information available.

VIII. REFERENCES

[1]. R. V. Kulkarni and G. K. Venayagamoorthy (2009) 'Neural Network based Secure Media Access Control Protocol for Wireless Sensor Networks', Neural Networks, Vol.10 , pp. 7-11.

[2]. S Markovich – Golan (2011) 'Distributed Multiple Constraints Generalized Side lobe Canceler for Fully Connected Wireless Acoustic Sensor Networks', Wireless sensor networks, Vol.12 , pp. 1847-1864.

[3]. J Yang - (2013) 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks', Vol.13 , pp. 7-13

[4]. C. Karlof and D. Wagner, (2003) 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures', Workshop Sensor Network Protocols and Applications, Vol.11, pp. 237-354

[5]. H. Zhang and H. Shen, June (2016) 'Bio-Inspired Cybersecurity for Wireless Sensor Networks', IEEE Communication Magazine, Vol. 19 pp. 340-347

[6]. W. A. H. Ghanem and A. Jantan, (2014) 'Swarm Intelligence and Neural Network for Data Classification', Proc. IEEE Int'l.Conf. Control System, Computing and Engineering, Vol. pp. 1969-2015.

[7]. C. Biener, M. Eling, and J. H. Wirfs, (2015) 'Insurability of Cyber Risk: An Empirical Analysis', The Geneva Papers on Risk and Insurance–Issues and Practice, vol. pp. 131–58.

[8]. D. S. Ghataoura, J. E. Mitchell, and G. E. Matich, (2011) 'Networking and Application Interface Technology for Wireless Sensor Network Surveillance and Monitoring', Vol. pp. 90–97.

[9]. A. Oracevic, (2014) 'Secure Tasrget Detection and Tracking in Mission Critical Wireless Sensor Networks', Vol. pp. 1–5.

[10]. D. J. John et al., (2014) 'Evolutionary Based Moving Target Cyber Defense', Proc. ACM Conf. Genetic and Evolutionary Computation, Vol. pp. 1261–68.

[11]. Sohrabi K, Gao J, Ailawadhi V & Pottie GJ (2000) 'Protocols for self-organization of a wireless sensor network', IEEE Pers Communication, Vol.7, pp. 16-27.