A Survey on Various Applications of Swarm Intelligence in Wireless Sensor Networks

[1] S.Sushmitha,[2] G.Mahalakshmi
[1]Student [2] Assistant Professor
[1][2] Department of Computer Science & Engineering,
NPR College of Engineering And Technology, Tamil Nadu

Abstract: **Wireless sensor network is susceptible to to various attacks due to the deployment in aggressive environment. Among various types of security threads, low power sensor nodes are affected by the various types of attacks that cause the random drainage of the energy source of sensors. It leads to the expiry of sensor nodes. The denial of sleep attack is the most important type of attack belongs to this category. In this survey, various aspects of swarm based approach for the detection and prevention of denial of sleep attacks in wireless sensor networks are described.**

Index Terms—**Anomaly detection, denial of sleep attack, Swarm Intelligence**

I. INTRODUCTION

Security of Wireless sensor network (WSN) becomes an important issue because of the fast elaboration of WSN that is uncovered to a wide range of attacks due to the narrow resources and its deployment in the intimidating environment. Intrusion detection system based on Swarm intelligence is one of the main and effective defensive methodologies against the various attacks in WSN. A particular distressing attack is denial of sleep attack (DS attack). It is a particular type of DoS (denial-of-service) attack.

Swarm intelligence (SI) is the cooperative performance of decentralized, self-organized systems, natural or synthetic. Swarm intelligence is the attitude that deals with the natural and artificial systems composed of many individuals that organize using decentralized control and self-organization. In particular, this discipline focused on the collective performances that result from the local interactions of the individuals with each other and with their environment.

Swarm intelligence is an advanced distributed intelligent method for solving optimization problems such as collision avoidance by formerly took its stimulus from the biological samples by swarming, collective phenomena in vertebrates. The basic philosophy of Swarm Intelligence is to observe the performance of social animals and try to imitate those animals on computer systems. Many famous examples of swarm intelligence include bird's flock, fish school and bugs swarm. The social communications among individual agent help them to adapt to the environment more capably since more information are gathered from the whole swarm.

The main concept of swarm intelligence (SI) denotes the combined performance of self-regulating, detached systems. These systems comprises of inhabitants of simple agents with no central control to advise their performance. The simple agents are un-intelligent and mingle locally with each other and environment to yield an intelligent and more complex performance.

Swarm intelligence characterizes the meta-heuristic attitude in order to solve a problem. A number of optimization algorithms have been revealed with incorporating swarm behavior. Some of the well known examples are

- ❖ Ant colony optimization (ACO)
- ❖ Particle swarm optimization (PSO)
- ❖ Gravitational search algorithm (GSA)
- ❖ Intelligent water drops (IWD).

Some of the descriptions of SI algorithms are listed below.

- ❖ ***Ant colony optimization***: Ant colony optimization algorithm is based on the ants' action-mechanism to bargain their food. This algorithm can be functional to the complicated problems such as discovering the optimal path to accomplish the objectives.

- **Particle swarm optimization**: Particle Swarm optimization algorithm is motivated by social attitude of bird flock or fish schooling. It is an essential part centered search algorithm used to discover most excellent solution in an n-dimensional space.

- ***Gravitational search algorithm***: Gravitational search Algorithm is based on the gravitational law and the usage of laws of Newtonian physics. The pursuit universe comprises of commonalities as agents. The gravitational force is accountable for the instants of these agents towards the global weightier bulk which resembles to the greatest universal illumination of aberrant.

- **Intelligent water drops**: This algorithm is nature based and impressionists the technical behavior of water drops and soils of the riverbed. In IWD algorithm, gathering of artificial water drops is used to find the optimal way with lowermost soil. IWD has been used to illuminate the traveling salesman Problem.

This paper is organized as follows. Section 2 describes various SI based Approaches in Wireless sensor networks. Section 3 provides conclusion and future enhancement.

II SWARM BASED APPROACHES IN WIRELESS SENSOR NETWORKS

2.1 Swarm Intelligence based Detection of Malicious Beacon odes

Swarm Intelligence based detection scheme [1] assumes same base model as in (D. Liu et al., 2005) & (A. Srinivasan et al., 2006). However integrating SI, the detection technique can be made more excitingly consider the environmental issue. Formerly various elucidations were projected to either tolerate the occurrence of malevolent nodes or to distinguish and displace them. Also discrete solutions have been anticipated against the specific attacks. IWD algorithm centered approach can accomplish well even in low-grade environmental circumstances because algorithm is based on the relative comparison of errors. The distance-error values of neighbor beacons were evaluated in order to find the probability of reliability or goodness of a node. IWD algorithm incorporates the scheme of natural water drops to choose the next location. Speed of an IWD growths inversely to soil between its current and next location so the drop will gain velocity on the path with low soil. IWD favors the path with low soil, so the possibility of choosing a path with low soil is higher. The probabilistic nature of sensor nodes was noticed by the AMC model. In this approach, denial of sleep attack is discovered by considering the predictable expiry time of sensor network under communal scenario. This system appraises the attitude of negotiated sensor nodes depending on the Markov chain with an absorbing state. The Absorbing Markov Chain was used to model the performance of each and every sensor node, rather than engaged on single.

2.2 Two Tier Data Dissemination Approach

Two Tier Data Dissemination Approach [2] was based on watching the various events happening in a computer system or network and analyzing them for signs of possible instances, which were abuses or imminent the intimidations of defilement of computer security policies, conventional use policies, or typical security practice. Systems that were designed to achieve all the procedures relevant to intrusion detection were termed as Intrusion Detection Systems (IDS). In IDS, a step known as training involves a number of records that is previously collected from the sensing components of the system was applied to the analysis engine. Subsequently in the training step, the IDS go online to secure the system in real time.

A classification or clustering algorithm was the functional component to classify the behavior into normal or abnormal. So, it means, the intrusion detection problem was shortened to a classification or clustering problem .The exceptional physiognomies of SI make it ultimate for this purpose. More precisely, SI techniques target at solving complex problems by the commitment of multiple but simple agents without the necessity of any form of supervision to exist. Every agent cooperates with others in order to discover the optimal solution.

These proceed through the direct or indirect communications while the agents determinedly travel in the search space. For this purpose, the agents can be used for several difficult responsibilities like discriminating the classification rules for misusing recognition decide clusters for abnormality detection, keep track of interloper marks etc. Certainly, these self-organizing and detached attributes are highly noticeable by proposing the means to break a difficult IDS problem into multiple simple ones allocated to agents. This makes the IDS becomes self-governing, highly adaptive, parallel, and self-organizing and cost effective in nature.

2.3 Particle Swarm Optimization (PSO) Algorithm

Particle Swarm Optimization (PSO) Algorithm[3] was based on multidimensional optimization technique, used to treat various optimization problems in WSNs. Working of PSO chooses the parameters and their ranges with junction acceleration to discrete values to overcome the node position problems and perform position the localized node, elect cluster head, localize the node, position the base station to minimize the cost of the sensor, maximize the efficiency and coverage, minimize the localization error and improve the life time of the node.

Data-aggregation needs frequent distributed optimization which was provided by PSO and static deployment, localization and clustering problem at base station could also be addressed by this PSO algorithm.

2.4 PSO Approach for Cluster head selection

This PSO (Particle swarm optimization) approach[4] was used to find out the heads in the cluster nodes (CHs) and the LEACH protocol was used as a basis for transmitting data from the sensor node. The algorithm works as Particle Initialization as the first step moves on with Fitness evaluation, Update Local and Global Best; Finally the Reselect mechanism and Velocity and Position Update were made.

This approach was carried out in homogeneous environment where all the sensor nodes have the same initial energy level and the global optimum solution in a complex search space. The proposed framework was cluster based technique in which respective cluster heads were chosen according to particle swarm algorithm based on the re-selection mechanism used to improve the election process and efficiency of the cluster nodes in WSN.

2.5 Ant Colony Optimization Attack Detection (ACO-AD) Algorithm for Sink Hole Attack

Ant Colony Optimization Attack Detection algorithm [5] was used to identify the sink whole attacks based on the node ids in the Wireless Sensor Networks. The nodes generating an alert on identifying a sink-hole attack were grouped together and were eliminated for better performance. A voting scheme was proposed in order to identify the intruder in the cluster. An ACO Boolean Expression Evolver Sign Generation algorithm was used to distribute the keys to the alerted nodes in the group for signing the suspect list to agree on the intruder. They were moved by applying a stochastic local decision policy based on two parameters named as the trails and attractiveness.

These nodes were sorted and matched based on the table information for detecting the intruders. The pheromone deposition of the ant agent represents the position of the node id and they were compared with the sender field of the route update packet which helps in intrusion elimination to make the node secure and also make the secure WSN.

2.6 Swarm based Defense Approach

A swarm based defense approach [6] was used for the development of an abnormality detection model in order to define the affected traffic between the nodes. Based on this, frequency hopping methodology was originated. Ant agents of swarm intelligence were then functional to collect the frequency hopping time and communication frequency. The faulty channel was recognized based on the frequency hopping time and when the administer node gets this data, it eliminate the defective channel. The simulation results showed that this approach was efficient in faulty channel detection. Less energy was distributed as the data about all the attackers can be acknowledged by employing ants. A framework for preventing denial of sleep attack consists of four key components such as the strong link-layer authentication, anti replay protection, jamming identification and mitigation and broadcast attack defense. Strong link-layer authentication was the greatest important and first component of denial-of-sleep protection and must be involved into any WSN that might be visible to attack.

2.7Swarm based intrusion detection system

Swarm based intrusion detection and defense technique[7] was used for finding malicious attacks in mobile ad hoc networks. In this technique, the nodes with maximum trust value, residual bandwidth and residual energy were designated as active nodes using swarm intelligence centered ant colony optimization. Each active node observers its neighbor nodes and assess the trust value of the neighbor node. If the active node discover any node lower a lowest trust threshold, then the node was marked as malicious and an alert message was directed to the source node. When the source node tries to forward the data packet to target, it omits the malicious nodes in that path and passes the data through other nodes in substitute path. It also accomplishes the certificate overturning process for the malicious nodes.

2.8 Swarm based defense technique for jamming attack

A swarm based defense technique [8] was used to detect the jamming attacks in WSN. Swarm intelligence algorithm is capable adequate to adapt modification in network topology and traffic. By using the channel hoping technique, the sender and receiver alter channels in order to remain away from the jammer. The jammers persist on a single channel, trusting to disorder any fragment that may be transferred in the pulse jamming technique. Using the swarm intelligence procedure, the onward ants either unicast or broadcast at each node dependent on the accessibility of the channel information for end of the channel. If the channel information was accessible, the ants randomly pick the next hop. As the backward ants reaches the source, the composed data was authenticated which channel there was occurrence of attacker long time, and those were misplaced.

Instantaneously the forward ants were absorbed through other channels which were not supposed before for attacks. This system helps to reduce the overhead of channel maintenance.

2.9 Swarm based routing protocol

A Swarm Intelligence based routing protocols[9] were used to remove several problems in the wireless sensor network such as battery life, scalability, maintainability, survivability, adaptability etc. This approach can also improve the routing factors such as latency, fault tolerance, energy with improves the performance of WSN. Energy-efficient ant-based routing algorithm which was based on the ant colony optimization where the routing table stores the information of the nodes and if any ant identification was found, the ant was eliminated and choose different path for routing.

Backward ant was directed to send the data in chosen path. The ant colony optimization based routing scheme has been inspired by operating principles of ants foraging which could improve ant colony function in WSN which could maximize the scalability of the ant node in ant colony.

2.10 Energy consumption based routing using swarm intelligence

An evolutionary algorithm [10] based on swarm intelligence, was used to broadcast the messages with minimum energy. This swarm algorithm was also used for solving communication routing problem. Swarm intelligence was the collective performance from a cluster of social creatures, namely ant, birds, etc., where the agents (ants) interconnect in the system either directly or indirectly using a dispersed problem solving attitude. This attitude extends hand in an optimized routing design, prevents the concentration of the network nodes. Routing in wireless network was never heavy. Therefore this intellectual sensor attitude affords a illumination to dynamic and dispersed optimization difficulties. Thus creating the network more dynamic, flexible, decentralized, intelligible and self-organized

Swarm agents were randomly employed over the network. These ant agents have three features such as Pheromone Level, Transition Probability. Real life ants deposit a chemical element called pheromone, which assists as a trace for the other ants to track. The ant organism caricaturists this pheromone deposition by arranging pheromones based on both energy level at the sensor node and the space from one node to another (Pheromone Level)

TABLE 1:
VARIOUS TECHNIQUES USING SWARM INTELLIGENCE

Authors	Year and reference	Technique	Performance
S. Qureshi, A. Asar.	2011[1]	Swarm Intelligence based Detection of Malicious Beacon odes	Detect the malicious beacon nodes based on Swarm of intelligent water drops
Nidhi, Mrs. Pooja Mittal	2012 [2]	Two tier Data Dissemination Approach (TTDD)	Swarm Based Intelligent approach to perform the reliable packet delivery over the network.
Raghavendra V. Kulkarni Ganesh Kumar Venayagamoorthy	2010 [3]	Particle swarm optimization (PSO) Algorithm .	Applied to address WSN optimal deployment, node localization, clustering and data-aggregation.
Tripti Sharma, G.S. Tomar, Brijesh Kumar, Ishaan Berry	2014 [4]	PSO approach for cluster head selection	Receives large amount of data at end nodes using FND approach
N.K. Sreelaja, G.A. Vijayalakshmi Pai	2014 [5]	Swarm Ant Colony Optimization Attack Detection (ACO-AD) algorithm	Ant Colony Optimization Attack Detection (ACO-AD) algorithm is proposed to identify the sinkhole attacks based on the node id's defined in the rule set
Periyanayagi and Sumathy	2013[6]	Swarm based defense approach	Uses ant agents of swarm intelligence
G.Indrani,K.selva kumar	2012[7]	Swarm based intrusion detection system	Proactive secrete sharing technique to find the active node using highest trust value
Periyanayagi and Sumathy	2011 [8]	Swarm based defense technique for jamming attack	Proposed swarm based detection algorithm to overcome the jamming Attacks
Fatih Celik, Ahmet Zengin and Sinan Tuncel	2010 [9]	Swarm based routing protocol	Used to address routing issues such as survivability and scalability in WSN
Rajani Muraleedharan and Lisa Ann Osadciw	2003[10]	Energy consumption based routing using swarm intelligence.	Transferring message with minimum energy consumption using swarm algorithm

III CONCLUSION

The paper comprises the survey results in application of swarm intelligence in various aspects of wireless sensor networks. This survey describes various methods and techniques such as Particle swarm optimization (PSO) Algorithm, Swarm Ant Colony Optimization Attack Detection (ACO-AD) algorithm, Swarm based routing protocol, Energy consumption based routing, intrusion detection algorithm, Secure localization algorithm. The results of the survey shows that the swarm based intelligence provides an optimal solution to the generic problems in WSN.As a future work, the prevention of denial of sleep attacks can be performed with minimal cost and resource utilization using swarm intelligence.

REFERENCES

[1] S. Qureshi, A. Asar, A. Rehman, and A. Baseer, 2011"Swarm Intelligence based Detection of Malicious Beacon Node for Secure Localization in Wireless Sensor Networks", Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS) 2 (4): 664-672 (ISSN: 2141-7016).

[2] Nidhi, Mrs. Pooja Mittal 2012. "A Swarm Based Approach to Detect Hole In Wireless Sensor Network", IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012.

[3] Rhavendra V.Kulkarni Ganesh Kumar, Venayagamoorthy,2010" Particle Swarm Optimization in Wireless Sensor Networks: A Brief Survey" IEEE transaction on Systems.

[4] Tripti Sharma, G.S. Tomar, Brijesh Kumar, Ishaan Berry,2014," Particle Swarm Optimization based Cluster Head Election Approach for Wireless Sensor Network" International Journal of Smart Device and Appliance Vol.2, No.2 (2014)

[5] N.K. Sreelaja, G.A. Vijayalakshmi Pai,2014" Swarm intelligence based approach for sinkhole attack detection inwireless sensor networks" ,ELSEVIER

[6] S. Periyanayagi and V. Sumathy, "Swarm Based Defense Technique for Denial-of-Sleep Attacks in Wireless Sensor Networks," International Review on Computers & Software, vol. 8, 2013.

[7] G.Indrani,K.selva kumar" Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks" International Journal of Computer Applications (0975 – 8887),Volume 50– No.19, July 2012

[8] Periyanayagi and Sumathy,2011" A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks", International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011

[9] Fatih Çelik, Ahmet Zengin and Sinan Tuncel,2010" A survey on swarm intelligence based routing protocols in wireless sensor networks" International Journal of the Physical Sciences Vol. 5(14), pp. 2118-2126, 4 November, 2010.

[10] Rajani Muraleedharan and Lisa Ann Osadciw,2003," Sensor Communication Network Using Swarm Intelligence",IEEE_2003.

[11] C. Kolias , G. Kambourakis,2011" Swarm intelligence in intrusion detection: A survey" ,ELSEVIER Sevinc E, Cosar A. An Evolutionary Genetic Algorithm for optimization of Distributed Database Queries, The Computer Journal, 2011;vol.54,Issue 5, pp. 717-725.

[12] Dokeroglu T, Tosun U, Cosar A. Parallel Mutation Operator for the Quadratic Assignment Problem, Proceedings of WIVACE, 2012; Italian Workshop on Artificial Life and Evolutionary Computation.

[13] Sureyya Mutlu, and Guray Yilmaz, " A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs", The Seventh International Conference on Networking and Services(ICNS), pp 292 to 298, 2011

[14] A. Kavoukis and S. Aljareh, "Efficient time synchronized one-time password scheme to provide secure wake-up authentication on wireless sensor networks," *arXiv preprint arXiv:1302.1756*, 2013

[15] P. Sharma, N. Sharma, and R. Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network," International Journal of Computer Applications, vol. 41, pp. 16-21, 2012

[16] T. Bhattasali and R. Chaki, "Lightweight hierarchical model for HWSNET," *Networking and Internet Architecture*, pp. 1-14, 2011

[17] S. Fouchal, D. Mansouri, L. Mokdad, and M. Ioualalen, "Recursive -clustering -based approach for denial of service (DoS) attacks in wireless sensors networks," *International Journal of Communication Systems*, 2013

[18] Abadeh MS, Habibi J. A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection. The ISC International Journal of Information Security 2010; 2(1):33e46

[19] S.Venkatasubramanian, and N.P.Gopalan, "A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET", International

Journal of Computer Applications (IJCA), pp 7-11, 2011.

[20] HyoJin Kim, Ramachandra Bhargav Chitti, and JooSeok Song,"Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile AdHoc Networks", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[21] Rizwan Khan, and A. K. Vatsa, "Detection and Control of DDOS Attacks over Reputation and Score Based MANET", Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 11, October 2011.

[22] Quan Jia, Kun Sun, and Angelos Stavrou, " Cap Man: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET", Proceedings of 20th international conference on computer communications and networks (ICCCN), pp 1 – 6, 2011

[23] Vinay Rishiwal, S. Verma, and S. K. Bajpai, "QoS Based Power Aware Routing in MANETs", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009.