Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

C-FPA: A Cloud-Based FPA Novel Approach to Defend Hotspot Issues and Attacks in WSN

J. Vijitha Ananthi[1], S. Shobana[2]

[1]Research Scholar, Department of Biomedical Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India
[2]Technical Analyst, Confyy Pvt. Ltd, Coimbatore, India

E-mail: [1]vijithaananthi@karunya.edu.in, [2]er.shobanadinesh@gmail.com

Abstract

Wireless Sensor Network (WSN) is a distributed network formed by sensor nodes that perform a specific sensing task like temperature, humidity, fire attacks, and so on. Used in all sorts of application like military, medical, industrial, scientific, and so on, WSN's are well known for high performance operations. Till date, power conservation and sensor node lifetime remained as the major drawback in such networks where the development of optimization techniques and routing protocols were proposed to overcome them. Also, attacks like DoS (Denial Of Service), Sybil attack, wormhole attack, HELLO flood attack, and identity replication attack are mostly common in a WSN. At present, Hotspot-based issues and attacks is found as one of the major and performance-degrading factor in wireless sensor network. In this paper, we propose a novel cloud-based FPA scheme or approach to defend and withstand such hotspot-related issues and attacks in WSN. Developed with the principle of Cloud, the simulation results prove that the proposed scheme offer high privacy, and routing stability.

Keywords: Wireless sensor network, hotspot-locating attack, cloud, privacy, fake traffic, routing stability

1. Introduction

Wireless Sensor Network is categorized under wireless network that follows a distributed independent fashion of sensor nodes to sense and monitor environmental & physical conditions. WSN is used in data mining, data processing, analysis, storage, and so on. Apart from the above mentioned applications, a wireless sensor network is used in IoT, agriculture, landslide detection, and medical applications [1]. In WSN, the communication

DOI: https://doi.org/10.36548/jitdw.2022.2.004
Received: 21.05.2022, received in revised form: 25.06.2022, accepted: 09.07.2022, published: 19.07.2022

between sensor nodes is made wireless usually with Wi-Fi or mobile mules. The sensor nodes collects data like temperature, pollution level, fire level, and sends it to the base station or parent node. The parent node or sink sends it later to the destination like alarm or display through a wired connection [2]. WSN can be found in surplus applications unlike forest & weather monitoring, battlefield surveillance, and human tracing. Although applications differ, such WSN's follow Air medium for transmission, and WLAN (Wireless Local Area Network) for data transmission [3]. At present, special WSN types like wireless sensor-actor network (WSAN), underwater wireless sensor network (UWSN), wireless body-sensor network (WBSN), and wireless underground sensor network (WUSN) are also available.

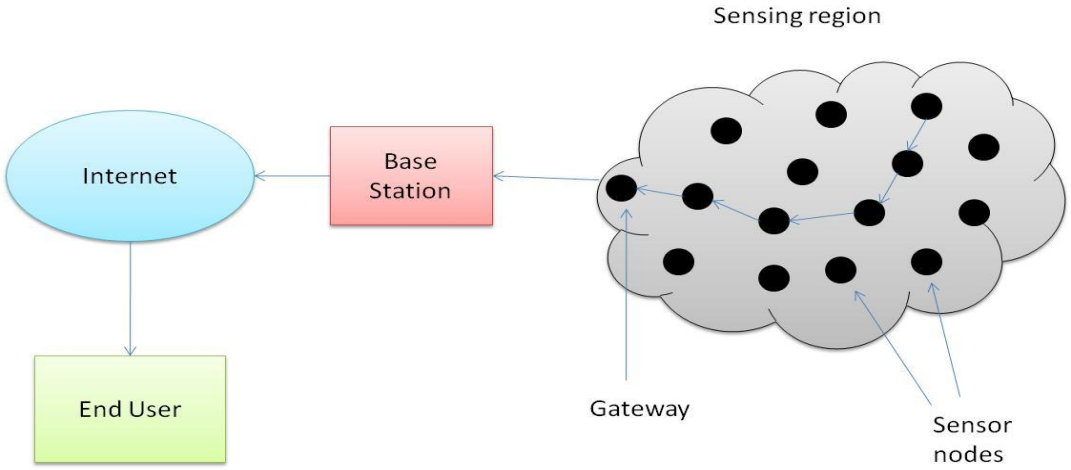

Figure 1. A typical WSN

A typical wireless sensor network is illustrated in Figure.1. It consists of sensor nodes, base station, internet, and a user. The sensor nodes have onboard processor that monitors the environment. A senor node is also called as Motes [4]. They are energy-efficient, multi-functional wireless devices that are present in a network in hundreds or thousands based on the purpose. Every sensor node comprises of a power unit, control, sensing, and processing unit. These nodes are categorized as senor node, relay node, actor node, cluster head, gateway, and radio nodes [5]. A sensor node is just used for data gathering whereas a relay node is used for communicating with the adjacent node in order to enhance the network reliability. Actor nodes are resource-rich motes that take decision based on situations [6]. Cluster head performs the data aggregation task and has high bandwidth. Finally, gateway or radio node is the interface channel between the network and other network. Radio nodes are the powerful motes that send the data to WLAN [7]. The radio node consists of power source, transceiver, memory, and a microcontroller. The sensing region is connected to the BS (Base

station)(i.e. gateway) that acts as the processing unit for the entire system. The BS in turn is connected to the Internet followed by the user to whom the data is to be shared [8].

1.1 Hotspot issue and attack

A wireless sensor network possess major characteristics like fault tolerance, mobility of nodes, dynamic network topology, communication failures, heterogeneity of nodes, scalability, and independency [9]. Although wireless sensor networks are advantageous, sensor networks doesn't fit into regular topology and possess latency, network attacks, unreliability, synchronization, node failure, and topology changes [10]. Among the issues, hot spot problem is a major one and in adversary attack type, hotspot-locating attack is a noticeable one. The representation of hotspot-locating attack is given in Figure 2.

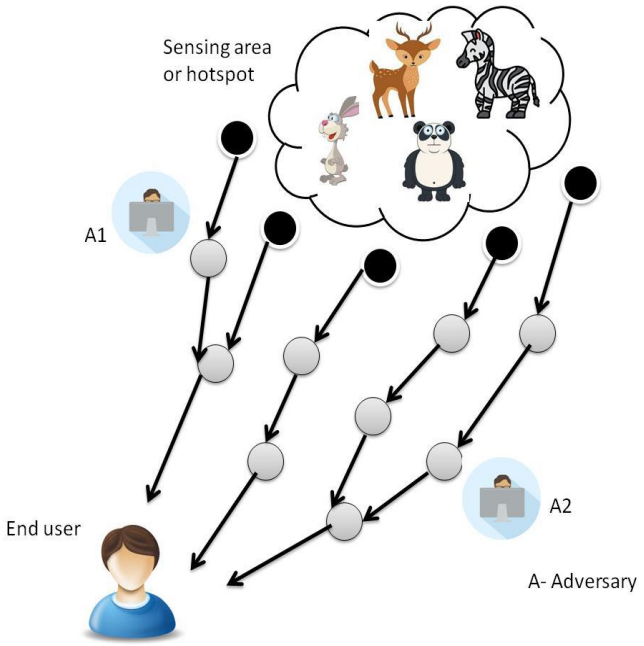

Figure 2. Hotspot-locating attack

- **Hotspot issue**: In a wireless sensor network, sensor nodes cannot send data directly to the base station. Despite, they forward it to Cluster Head (CH) that is in turn forwarded to the BS. By this process, the CH's near BS depletes more energy when compared to CH's far from BS due to heavy traffic. This circumstance results in coverage issues, network disruption, and energy draining of CH. This issue is known as hot spot problem [11].

- **Hotspot-Locating attacks**: Hotspot-locating attack comes under content privacy, and contextual privacy attacks where the adversaries use the traffic info to track or

monitor the sensed data related to objects (endangered animals, birds, monuments), and confidential places. In such attacks, the adversaries make use of traffic analysis techniques to capture the sensed information. Various adversary models or schemes like global adversary and routing are available [12,13].

2. Related Works

It could be to resolve or keep a full stop to the hotspot-related problems in WSN, various research works and algorithms were developed where a few are discussed in brief in this section. The authors in reference [14] have proposed the ZECR (Zone-divided and Energy Clustering Routing Protocol) that proposes the idea of partitioning the available area into countless zones and employing unequal clustering mechanisms. RN for the inter-cluster communication is selected relating to high residual energy and the data is therefore transferred to BS. The simulation results show that ZECR protocol can alleviate the hotspot issue to a significant extent.

Another class of clustering protocol was proposed in [15] termed as EADUC (Energy Aware Distributed Unequal Clustering). This protocol not only elevates the hotspot issue but the energy hole issue as well. Following the principle of CH selection with respect to average residual energy of surrounding sensor nodes, an uneven cluster size is developed that preserves the network energy for intercluster communication. While the above-discussed protocols employ the mechanism of unequal clustering, the HUCL [16] protocol based on both dynamic and equal/unequal clustering is found to be beneficial. In this method, based on the engaged SMS, distance from BS, and residual energy, the CH is chosen. Also, the data transmission stages are divided into major slots, further into minor slots, and those minor slots are given a CM that forwards the data to the CH. This method reduces the overhead in the network, and hotspot issues.

Similarly, to mitigate the hotspot-location tracking attacks in WSN's, Onion Routing [17] was proposed that hides the info related to end users by providing anonymous communication to the internet. Another way to protect the information is by concealing the MAC /network address that can also achieve anonymous communication in ad-hoc or sensor networks [18]. Whereas, Jien et.al [19] has used a different strategy of injecting pack packets of the sink to preserve the location privacy. As both the incoming and outgoing traffic are equally distributed, it becomes difficult for the adversary to trace the location and other info relating to sink or end user. Likewise, to preserve sink's location privacy, each node can send

packets at constant rate followed by a delayed transmission. This scheme has effectively reduced the traffic-related hotspot attack, and preserved privacy [20].

3. Proposed Work

FPA (Flower Pollination Algorithm) is a population-based algorithm used in WSN's that is an inspiration gained from the pollination process taking place in the flowering plant. As per the rules of Levy Flights, pollens are transported by pollinators and such pollination can take place globally or locally. In our proposed system, we have developed a novel scheme called C-FPA that is a diversity-pollen FPA approach with cloud based mechanism to overcome both hotspot issue and attack in a wireless sensor network. In the method of diversity pollen FPA, the overall population is divided into subpopulation and the available fitness resources are shared by the neighbourhood topology. The information regarding the subpopulations is shared among each SP's whenever the communication is triggered so that co-operation is preserved. To make a dynamic diversity and adjust the global and local searching process, dynamic switching probability strategy is introduced. With a stage iteration, the activate schedule is on, and then the small groups starts searching for the target in the sensing area. The switching probability of the FPA algorithm is defined by the below given formula:

$$\rho = \alpha - \beta * \frac{\tau - mod(iter, \tau)}{\tau}$$

In the above equation,

τ& iter= exchanging period and current iteration

ρ= range of [0,1]

α, β = constants in range of [0,1] and α>β

In the proposed system, both Niching technique, and FPA optimization are used. As hotspot issue is created by multihop communications in the network, FPA selects an optimal group of sensors as CH and calculates the optimized parameters to form clusters thus preventing the unbalanced energy consumption. Two characters are considered in the sensing region namely: communicating and small size. To create diversity in local search, small groups are used as they perform better when multimodal, and in constrained problems. Also, they can converge to a local optimum as they search the given area with historical information. Whereas, the communicating character are better-performing ones in the cluster

used for exchanging information and ensuring co-operation among the members. The algorithm of the diversity pollen FPA is as follows:

***Step 1*:** Initialization of pollen as per population size confirmation (n*m). Assign the exchanging period.

***Step 2*:** Evaluation of value of $f(X^{t}_{ij})$pollen in j-th group.

***Step 3*:** Updating the local and global solutions.

***Step 4*:** Replace the k poorer pollen with the best k pollen in the group and update the group for each R iteration.

***Step 5*:** Terminate the process if the best pollen solution is recorded else go to step 2.

In order to elevate the hotspot-locating attack imposed by adversaries and preserving the privacy of the network, the below cloud-based mechanism is implemented along with the above-discussed FPA technique. The scheme is segregated into 3 phases: 1. Predeployment, 2. Fake source nodes assignment, and 3. Event Transmission Phase.

1. **Predeployment Phase**: This phase serves to be the initial phase where each node is loaded with an unique identity ID_A, a key K_a shared with sink, and a secret key d_a that computes the shared key with other sensor nodes.

2. **Fake Source Nodes Assignment**: Here, the Fake source or sink nodes are assigned to confuse the adversary. To assign fake source nodes, a node namely A broadcasts FREQ (Fake Nodes Request Packet)message that adds the information number of hops (h_{max}). As a response, FREP (Fake Nodes Request Reply) packet is sent back to the node A. Node A now categorizes and forms a separate group based on responses and unicasts the FASS (Fake Node Assignment Packets)to intimate the list of fake nodes. The identities of respective nodes are added so that pseudonyms are shared between them in the route.

3. **Event Transmission Phase**: As mixing within a crowd is the best way for confusing the adversary from locating the privacy and information, the source node along with the group forms an irregular shape “cloud”. Although the adversary can find that a packet is being sent from the cloud, the identity of the node cannot be found out. When a key is shared between two nodes, a sequence of pseudonyms is created with a one-way keyed hash function. Such pseudonyms are used in the process of

identification of the sender/receiver nodes and in identifying the routes as well. To avoid the missing of pseudonym, sliding window matching can be used to interpret the expected and received pseudonym.

In this phase, when the source node is about to send data to sink, the fake source node is picked and the event packet is sent. The message M is then encrypted by the source node with the key that is known only to the sink. To improve privacy and fake traffic, fake packets are sent to the cloud.

4. Results and Discussion

To carry out the experiment and analysis, a network with n-node (100, 200) are created in a two-dimensional problem space. As the nodes in a cluster increases, the chances of becoming a CH becomes high. In the experimental model, the number of CH is 10% more than the total node count. To verify and evaluate the effectiveness of the proposed solution in terms of convergence and search rate, the following parameters in Table 1 is quite helpful.

Table 1. Variant N-values to evaluate the convergence and search rate

Number of nodes	Convergence after the generations	CH(%)	Solution search rate (%)
100	185	10.0	97
200	355	10.0	99
300	455	10.0	98
400	645	11.2	96.2

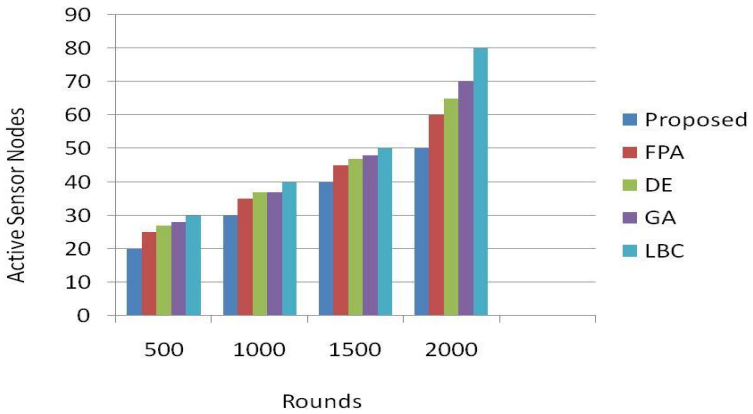

Figure 3. Convergence rate comparison

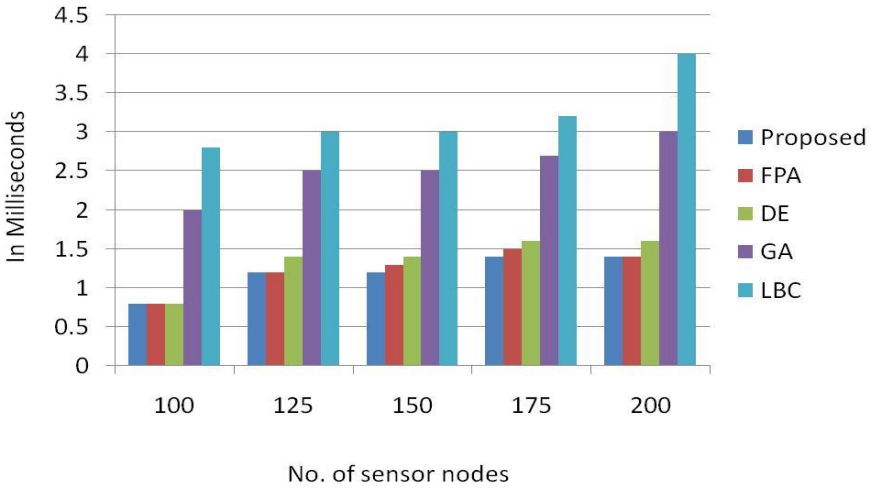

Figure 4. Execution time comparison

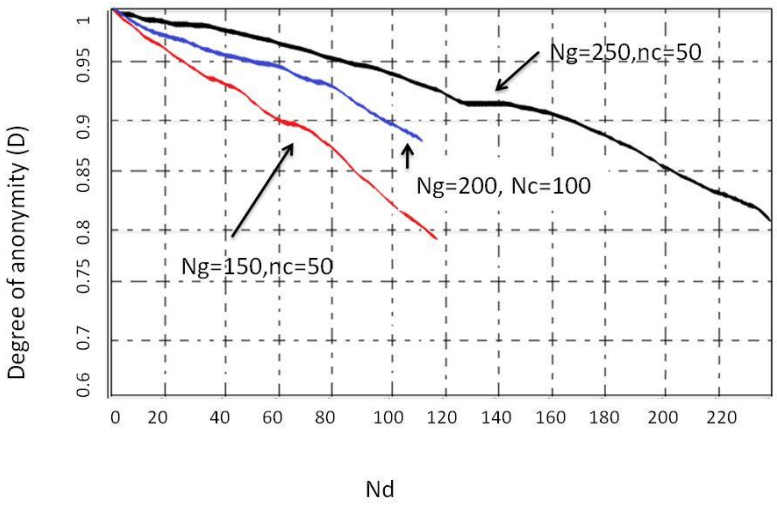

Figure 5. The degree of anonymity of C-FPA

When the proposed system is simulated in the NS3 simulator, it is found to be better when compared to different clustering methods like GA, DE, and LBC methods prevalent in WSN. Figure.3 depicts the comparison approach between various schemes in terms of convergence. Similarly, the execution time of the proposed system is fast as shown in Figure 4. Finally, the degree of anonymity of the proposed C-FPA scheme is depicted in Figure 5.

5. Conclusion

A wireless sensor network is the best distributed network suitable for all sorts of fields for the purpose of continuous monitoring. Amongst the various network issues and attacks evolving in WSN's, this paper has concentrated on the hotspot issue and hotspot-locating attack. Also, we have proposed C-FPA approach that utilizes a diverse Flower Pollination

Algorithm enriched with a Cloud scheme to defend adversaries from grabbing the sensible and confidential information. The experimental results convey that the proposed method offers better load balancing for the equal load of sensor nodes when compared to the other algorithms and protocols that are used to eradicate the hotspot issues in WSN's.

References

[1] Aiswariya, S., Rani, V. J., & Suseela, S. (2018). Challenges Technologies and Components of Wireless Sensor Networks. IJERT.

[2] Pandian, M. D. (2019). Enhanced network performance and mobility management of IoT multi networks. Journal of trends in Computer Science and Smart technology (TCSST), 1(02), 95-105.

[3] Nguyen, T. T., Pan, J. S., Dao, T. K., & Chu, S. C. (2018). Load balancing for mitigating hotspot problem in wireless sensor network based on enhanced diversity pollen. Journal of Information and Telecommunication, 2(1), 91-106.

[4] Bhalaji, N. (2019). QOS and defense enhancement using block chain for fly wireless networks. Journal of trends in Computer Science and Smart technology (TCSST), 1(01), 1-13.

[5] M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards statistically strong source anonymity for sensor networks", Proc. Of IEEE INFOCOM'08, pp. 51– 59, Phoenix, Az, USA, April 2008.

[6] Sungheetha, A., & Sharma, R. (2020). Real time monitoring and fire detection using internet of things and cloud based drones. Journal of Soft Computing Paradigm (JSCP), 2(03), 168-174.

[7] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks", Proc. Of ACM WiSec, pp. 77–88, Alexandria, Virginia, USA, April 2008.

[8] Raj, J. S., & Smys, S. (2019). Virtual structure for sustainable wireless networks in cloud services and enterprise information system. Journal of ISMAC, 1(03), 188-205.

[9] Y. Zou, H. Zhang, and X. Jia, "Zone-divided and energy-balanced clustering routing protocol for wireless sensor networks", in 2011 4th IEEE International Conference on Broad-band Network and Multimedia Technology, Shenzhen, China, 2011.

[10] Bashar, A. (2020). Sensor cloud based architecture with efficient data computation and security implantation for Internet of Things application. Journal of ISMAC, 2(02), 96-105.

[11] J. Yu, Y. Qi, G. Wang, Q. Guo, and X. Gu, "An energy-awaredistributed unequal clustering protocol for wireless sensor net-works," International Journal of Distributed Sensor Networks,vol. 7, no. 1, Article ID 202145, 2011.

[12] Raj, J. S. (2019). Efficient information maintenance using computational intelligence in the multi-cloud architecture. Journal of Soft Computing Paradigm (JSCP), 1(02), 113-124.

[13] L. Malathi, R. K. Gnanamurthy, and K. Chandrasekaran,"Energy efficient data collection through hybrid unequal clustering for wireless sensor networks,"Computers and ElectricalEngineering, vol. 48, pp. 358–370, 2015.

[14] Haoxiang, W., & Smys, S. (2020). MC-SVM based work flow preparation in cloud with named entity identification. Journal of Soft Computing Paradigm (JSCP), 2(02), 130-139.

[15] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing", IEEE Journal on Selected Areas of Communications, vol. 16, no. 4, pp 482-494, May 1998.

[16] Kumar, D., & Smys, S. (2020). An efficient packet delivery scheme using trust routing in G. 9959 protocol in a wireless sensor network. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 2(03), 118-125.

[17] M. Mahmoud and X. Shen, "Lightweight privacy-preserving routing and incentive protocol for hybrid ad hoc wireless networks", Proc. of IEEE INFOCOM, International Workshop on Security in Com-puters, Networking and Communications (SCNC), Shanghi, China, April 10-15, 2011.

[18] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 7, no. 10, pp. 3769-3779, October 2008.

[19] Chen, J. I. Z., & Lai, K. L. (2020). Machine learning based energy management at internet of things network nodes. Journal: Journal of Trends in Computer Science and Smart Technology September, 2020(3), 127-133.

[20] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks", Proc. of IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), pp. 113–126, Athens, Greece, September 5 - 9, 2005.