INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 4, Issue - 6, June – 2020
Monthly, Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.245
Received on : 03/06/2020 Accepted on : 18/06/2020 Publication Date: 30/06/2020

Source- Location Privacy in Energy efficient Based on Routing Techniques using Wireless Sensor Networks in Social Internet of Things (SIoT)

S. Jayasri [1] , Dr. R.Parameswari [2]
[1] Research Scholar, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117
[2] Associate Professor, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117
E-mail:[1] jai.341985@gmail.com, [2]dr.r.parameswari16@gmail.com

Abstract: *Social Internet of Things (SIoT) is a rapidly changing technology that emanates from the Internet of Things (IoT). Recently, SIoT has turned out to be the focus of numerous intelligent research activities although it ensures decentralized networks for trillions of interconnected artifacts and promotes fascinating new applications. Wireless Sensor Network (WSN) is basically a multi-hop, independent network comprising several sensor nodes. Depending on sensor nodes characteristics, Source location privacy (SLP) is considered to be a challenging issue for WSN. This paper aims to address and examine data privacy models of the source-location in a SIoT, related Wireless Sensor Network. This paper emphasizes on the basic routing techniques employed in WSNs.*

Key Words: *SIoT, WSN, SLP, Routing, IoT.*

1. INTRODUCTION :

In recent years, the items linked to the internet are increasing on a continuous basis, thereby providing the IoT downscales with a social structure for IoT visibility and ensuring navigation among objects. Several research attention has been drawn to the application of social interactions with the IoT systems. Existing works emphasize on connections between humans and objects while others find only the relationships between person and person. Although others take advantage of current social networking sites and combine them with IoT.

SIoT system is dealt with numerous challenges that degrade its performance quality. They need to be supported by certain prerequisites for enhancing their applicability and usability across extremely diverse application Domains of SIoT. Improved service provisioning by social Relationships some forms of fundamental social relationships between objects to effectively discover services. It does not therefore accept the complex creation of novel relationships within social objects' network. Since few applications having automated service functions need dynamic objects' selection. Thus, objects must gain the capability to analyze novel interconnection relationships with other objects in network. The Wireless sensor network nodes are very small in nature and capable of sensing, collecting, and spreading information.

2. BRIEF LITERATURE REVIEW:

SLP in WSN is characterized as a source wishing to transmit information to a base station (BS) while maintaining its location's privacy[1]. The location privacy in WSN is a phantom routing proposed by ozturk et al.[2] (enhanced by kamat et al.[3]), wherein the message routing comprises two stages: i.e. in first stage, a directed random walk of h steps follows, and in second stage, the message will be routed to BS through one direction or by flooding.

The classification of privacy problems of WSNs are content-oriented and contextual-oriented problems. Through encryption and authentication, the challenges of Content -oriented can be addressed.

Location privacy requires anonymity the location of a node, which is a contextual problem in WSNs [2].

Yao et al. [4] proposed a method for SLP in WSN, by considering the ring concept, wherein it was assumed that group of nodes are having identical distance to BS. Further, message was passed to a ring first then traveled towards a fixed direction. Then again routed through another random ring and the message finally reach to the base station.

The enhanced MHT-Leach protocol was proposed by emad et al., [9] for transmitting sensor information to BS through an infinite number of levels. The period of every stage was divided into two thereby implying that network life cycle was splitted into rounds. Every round comprised three main phases: namely Initial, Announcement and Routing phase. Furthermore, the clusters were generated in initial phase through the similar method employed in the Leach protocol. Then network's Ch's was selected and remaining sensor nodes were linked to their clusters.

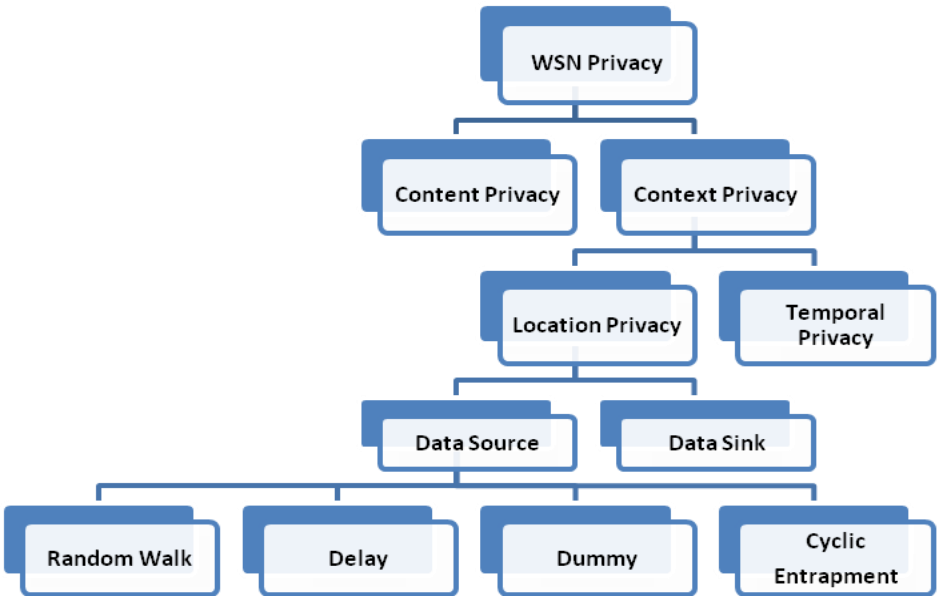

Fig.1 Privacy in WSN

In this paper, we strategize to extend the WSN life and boost its performance. Hence a novel general strategy will be introduced to transmit sensor nodes deployed around BS to stages. Furthermore, it will be assumed that every cluster around Ch will be splitted into two levels [9]. ACO consists of a group of smart algorithms to model an Ant Colony's Foraging behavior. Ants leave a material called a Pheromone on the feeding path which can be detected by other ants and affect their crawling path.

The motive of the primary ACO technique was to select the optimal path depending on ants actions in the path search process between their Food Source and Colony. Since then, the original aim of solving a broader variety of numerical problems has been diversified, resulting in several problems, depending on several aspects of ants behavior [10].

3. WSN ARCHITECTURE:

The WSN comprises numerous sensors. Sensor nodes are accountable for transmitting and gathering relevant information to sink node, receiving and delivering the information collected by the network to the End user

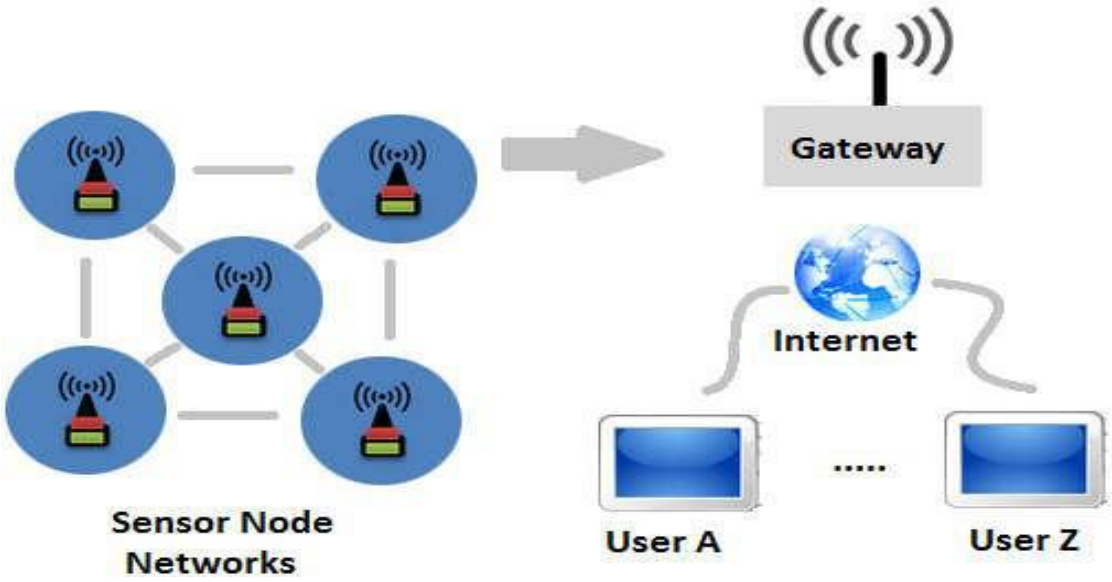

Fig.2 WSN [14]

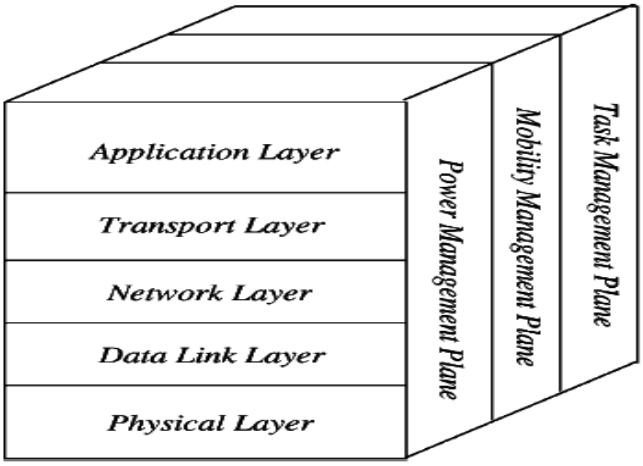

Fig.3 WSN Architecture

A. **Application Layer**

This layer deals with Traffic Management and offers tools for determining positive data for the several applications that transform information in a proper manner. Moreover, sensor networks are organized for diverse applications in distinct fields like military, agriculture, medical, environmental, etc.

B. **Transport Layer**

The layer provides traffic flow prevention and provides reliability wherein multiple Protocols are either upstream realistic to offer this characteristic. Nevertheless both protocols employ similar methods for detecting losses and restoring losses. Moreover, this layer is precisely required when system is employed to access other networks.
Offering energy efficient recovery of reliable losses is considered to be the prominent factor that describes why TCP is unsuitable for WSNs. Also this layer can typically be splitted into Packet-driven, Event-based layers. This layer includes few practical scenarios such as STCP (sensor transmission control protocol), PORT (price-oriented reliable transport protocol) and PSFQ (pump slow fetch quick).

C. **Network Layer**

The significant function of this layer is routing, it has a multitude of application dependent tasks, however in reality, the prime responsibilities are partial memory, power conservation, sensors and buffers that must be self-arranged and do not contain Universal- ID.

The basic idea of protocol is to describe a Redundant Lane and Secure Lanes, depending on persuasive scale known as Metric that differs from protocol to protocol. However, existing protocols in this layer, are categorized into Flat routing and Hierarchical routing, or they can be divided into Time-driven, Query-driven and Event-based.

D. **Data Link Layer**

This layer deals with Data Frame Detection multiplexing, data streams & Error management, Point-Point (or) Point Reliability multi-point Confirmation.

E. **Physical Layer**

This layer has the benefit of passing bit streams over the physical medium. Furthermore, it is accountable for Carrier Frequency Generation, Frequency Selection, Modulation, Signal Detection and Data Encryption.

4. SOURCE LOCATION PRIVACY MODELS:

SLP models are often employed for confirming the sensor node privacy on the communication networks. Random walk scheme was proposed by ozturk et al for handling SLP, wherein, on detecting an event by sensor node, event message will be created and sampling chooses a neighbor and passes a message. The neighbor also forwards the message in the same way.

The Directed random walk Approach (EDROW) was introduced by Tan et al. In this method, the root node that is near the base station forwards the packet using different paths to give better privacy to the source location, more of the root node to be created in the path.

The Phantom one-path routing was developed by Luo et al., In this method, the phantom node was initialized and designed to simulate.

The Greedy Random walk approach (GROW) was recommended by Xi et al.,. In this method, the sink was first initialized and the next source node generate and forward the packet in the same pattern. GROW method is monitored by Bloom filter to avoid the repeating cycles.

Another common mechanism used to provide the SLP is dummy data Source which has the limitation of

difficulty in identifying the real and fake congestion.

The Ring Based Routing (RBR) was suggested by Long et.al., In this method, the ring paths confuse the adversary with the location. Furthermore, network energy efficiency is balanced through this method without affecting system lifespan. This method is not suitable for rapid transmission of the network [5].

Solutions for providing SLP

It can be classified into distinct categories namely Geographic Routing, Random Walk, Location anonymization, Network coding, using dummy/fake Data sources, Delay, Separate path routing, Cyclic Entrapment, Cross-layer routing, limiting node detect ability, etc.

5. ROUTING METHODS IN WSNS:

There are numerous routing procedures available for WSNs and are categorized into Flat and Data Centric routing, Hierarchical Routing (HR), Location- based routing (LBR).

Flat and Data Centric routing*:*

WSNs comprise an enormous bunch of sink nodes, so it's hard to keep the Ids for each node. Data Centric and Flat routing method is developed to overcome these issues. In this approach the nodes operate on the basis of the query, which means that the node satisfies the query will be taken for forward or drop of a packets. The query message is initiated by the sink [6].

Flooding, Gossiping and Direct diffusion are the most common routing techniques used in flat and data centric method.

- **Flooding and Gossiping**

  Two traditional methods exist for relaying information in sensor nodes, that does not employ complex routing schemes and topology management. As the Flooding reveals in Figure 3. Each node that receives a packet will transmit the same to its neighbor nodes without checking node capabilities. Till the packet is reached or till the maximum count of hops is reached by packet, this process will be repeated.

  However, this strategy faces few pitfalls such as: impulse, duplication, and ignorance of capital. In Gossiping, rather than transmitting every packet to its adjacent components, packets will be randomly transmitted to an individual neighborhood selected from a neighboring table after all node capabilities have been tested.

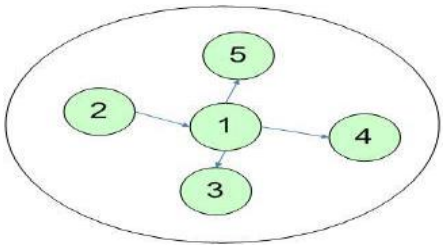

Fig.4 Flooding in WSN

Hierarchical Rrouting(HR)

WSN of sensors using hierarchical model is split into different multiple clusters; one of it's nodes in each clusters will serve as a head-cluster. It helps to decrease the overhead routing of normal nodes. The cluster node is accountable for transmission to base station. Leach (Low energy adaptive clustering hierarchy) Routing protocol, Pegasis (Power efficient gathering in sensor information system) Routing protocol, Teen and Apteen are some of the widely used HR protocols.

.

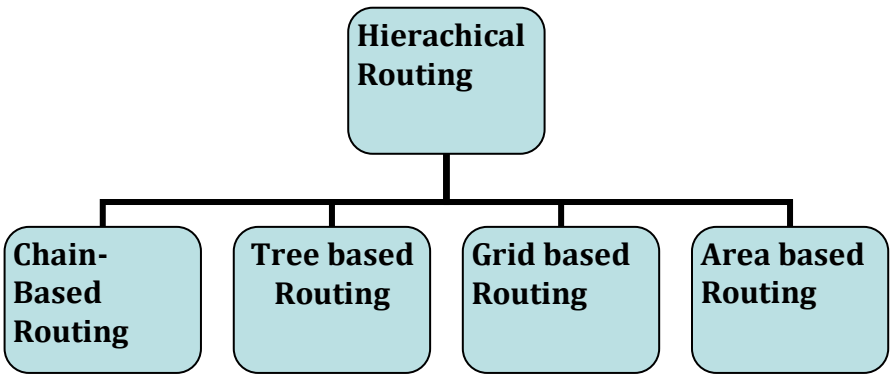

Fig.5 Classification of HR

In chain-dependent routing, network nodes will be connected through rings for transmitting information. Within chain a representative will be selected for performing data collection task, like a drain. Information will be sent through chain, and finally to main node. The information will be aggregated during transmission process [12].

All of the sensor nodes construct a logical tree in tree-based routing. Data is strongly transferred from the nodes on the leaf to their relatives. The root nodes send the information obtained to the root nodes of their parent nodes during impact. Data aggregation can be performed in every node [12].

In Grid dependent topology, network is categorized into distinct grids through geography process. Generally Grid-dependent routing is location-aware routing. Here routing will be performed without the need of routing table that inturn is considered to be the prominent feature of this routing technique. All routing functions will be performed after the source reaches the destination location [12].

Moreover, Area-dependent topology is a state-of-the-art system in which those sensor networks are formed and act as high-level nodes in a given area. In general, these nodes facilitate the process of gathering data from ONs and transferring signals into the node. Furthermore, depending on load balancing needs, area density will be adjusted This topology is continuously used during handheld WSNs[12].

Location Based Routing (LBR)

WSN that uses location-based contact routing, which is often called Geographic Routing or condition-based protocols. By using these protocol it decreases energy usage and increases the service life of the network.

Geographical and energy aware routing (GEAR),Geographic adaptive fidelity (GAF),and Minimum energy communication network (MECN) are some of the common Routing methods in LBR [7].

Gear is a protocol which is considered to be energy-conscious that chooses the neighborhood to route the queries to the destination. It forwards the signal to the destination region instead of a single node. Gear utilizes localization system or GIS (Global information system) for determining the information pertaining to the places. Gear minimizes delay and allows life longer[13].

Each node maintains its network nodes with intelligence about location, remaining resources, position and energy level. Each node uses two forms of costs to enter the cluster through its nearest neighbors, i.e. estimated costs and realized costs. The approximate cost depends on the two variables: range from location and excess energy [13]. Throughout two stages, it works.Next, route packets to the region of destination.Second, distribute information in the field.

Table 1. WSNs Routing protocols – A Comparison [8]

The following table shows the model depending on geography reduces the energy usage and tends to increase network time.

S.No.	Routing Protocol	Classification	Data Delivery Model	Scalability	Power Usage
1.	Flooding	Flat and Data Centric	Neighborhood Nodes	Limited	High
2.	Gossiping	Flat and Data Centric	Neighborhood Nodes	Limited	High
3.	Direct Diffusion	Flat and Data Centric	Neighborhood Nodes	Limited	Limited
4.	LEACH	Hierarchical	Cluster-Head & Base Station	Good	Maximum
5.	PEGASIS	Hierarchical	Cluster-Head & Base Station	Good	Maximum
6.	TEEN & APTEEN	Hierarchical	Cluster-Head & Base Station	Good	Maximum
7.	SPAN	Hierarchical / Location Based	Continuously	Limited	Limited
8.	GEAR	Location Based	Continuously	Limited	Limited
9.	SPEED	Location Based	Geographical	No	Low

6. PROPOSED PLAN:

- Initially, generate a network environment and initiate the nodes and primitives of the network.
- Then, a novel authenticated group key agreement for IoT environment will be created and develop a key generation using AMES (Advanced multiple encryption system). Moreover, the suggested AMES method is

dependent on Mqtt protocol and Hardy wall technique.

- After that, authentication models interoperability will be determined and secured routing protocol by using agglomerative hierarchical clustering approach will be proposed.
- Performance evaluation will be done for computation cost, Communication cost, Key generation time, Key verification time and session time.
- Finally, compare the existing algorithms and proposed algorithms.

7. CONCLUSION AND FUTURE WORK:

SIoT is considered to be a crucial subject owing to its object discovery, complex and huge research factors of interest. And an agent-based approach for developing large-scale digital environment that leverages edge computing and SIoT paradigms for addressing issues pertaining to interoperability and scalability.

Source-location privacy is important for the effective implementation of wireless sensor networks. A routing-based system is examined first via a conventional-intermediate node. Further, two schemes pertaining to inter-intermediate nodes are implemented.

We carried out simulations to test the outcomes for each of these schemes. Simulation results demonstrate that better efficiency with respect to latency of message delivery, energy consumption, and message delivery ratio can be achieved by the proposed schemes.

REFERENCES:

1. Shaoquan Jiang, Min Li, and Zailiang Tang "A New Scheme for Source-location Privacy in Wireless Sensor Networks". International Journal of Network Security, Vol.20, No.5, PP.879-889, Sept. 2018 (DOI: 10.6633/IJNS.201809 20(5).09).
2. C. Ozturk, Y. Zhang, and W. Trappe, "Source location privacy in energy-constrained sensor network routing," in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), pp. 88–93, 2004.
3. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in Proceedings of the 25th IEEE Distributed Computing Systems (ICDCS'05), pp. 599– 608, 2005.
4. L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu, "Protecting source - location privacy based on multi rings in wireless sensor networks," Concurrency and Computation: Practice and Experience, vol. 27, no. 15, pp. 3863–3876, 2015.
5. Guangjie Han, Lina Zhou, Hao Wang, Wenbo Zhang, Sammy Chan, A Source Location Protection Protocol Based on Dynamic routing in WSNs for the Social Internet of Things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.044.
6. Sanjolly Jain, Amit Grover, "Routing Techniques in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 94 – No 6, May 2014.
7. Jitender Grover, Shikha Sharma, Mohit Sharma, "Location Based Protocols in Wireless Sensor Networks – A Review", IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT 2014)
8. Raghunandan, G. H., & Lakshmi, B. N. (2011). A comparative analysis of routing techniques for Wireless Sensor Networks. 2011 National Conference on Innovations in Emerging Technology.
9. Alnawafa, E., & Marghescu, I. (2018). *New Energy Efficient Multi-Hop Routing Techniques for Wireless Sensor Networks: Static and Dynamic Techniques. Sensors, 18(6), 1863.*
10. Zou, Z., & Qian, Y. (2018). Wireless sensor network routing method based on improved ant colony algorithm. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-018-0751-1 .
11. Echoukairi, H., Bourgba, K., & Ouzzif, M. (2016). A Survey on Flat Routing Protocols in Wireless Sensor Networks. Advances in Ubiquitous Networking, 311–324. doi:10.1007/978-981-287-990-5_25
12. Liu, X. (2015). Atypical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review. IEEE Sensors Journal, 15(10), 5372–5383. doi:10.1109/jsen.2015.2445796 .
13. Grover, J., Shikha, & Sharma, M. (2014). Location based protocols in Wireless Sensor Network — A review. Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT). doi:10.1109/icccnt.2014.6962990
14. Kocakulak, M., & Butun, I. (2017). An overview of Wireless Sensor Networks towards internet of things. 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). doi:10.1109/ccwc.2017.7868374 .