ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Secure Data Aggregation Scrutiny (SDAS) through Orthogonal Set Verification (OSV) Method for Wireless Sensor Network

1. N.S.Kavitha, Assistant Professor / CSE, Erode Sengunthar Engineering College, Erode
2. B.Gopinath, Associate Professor / ECE, Info Institute of Engineering, Coimbatore
nskavi17@gmail.com, gopiphd@yahoo.com

Abstract : Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless communications capabilities for data transmission, security, energy efficient among the cluster of nodes and maximum lifetime within the transmission range to broadcasts the information. Data aggregation, key pre distribution, energy efficient mechanism, lifetime and security are various factors for sensor networks for transmitting the information to make the sophisticate communication. In this paper, orthogonal function is proposed to verify the path direction between the two nodes and it is always perpendicular to other points with angle degree and finds the direction of the data of the nodes sending as well as to find network path of the route travel for Security Data Aggregation Scrutiny (SDAS). The mathematical derivation to find the direction of the data path and how many data path direction are sending from a single cluster in angle of degree with support of Orthogonal Set Verification (OSV) method.

Keywords: Wireless sensor network, Data Aggregation, path direction of data, Orthogonal Set function.

1. Introduction

In modern years, the extensive research has opened challenging issues about performance evaluation for Wireless Sensor Networks (WSNs). The promising technologies can be used to achieve a variety of goals and objective from health monitoring to human healthcare activities, industrial automation, emergency management and environmental monitoring system [1]. A designed process is required to collect data and report to a central unit, connected to the internet or monitored.

A WSN is a network composed of numbers of small independent sensor nodes and it helps to transmit and receive the information gathered from location to another location with a wide range of information and communication technology. The earlier development of wireless sensor networks was originally inspired by military applications like of GPS, surveillance etc. However, WSN are used in many environments such as habitat monitoring, healthcare applications, home appliance automation, and traffic control. Sensor network is equipped with components for radio transmitter and receiver, microchip, battery, topology design and communication devices [1][2].

2. Outline: Basic requirement of WSN

Wireless Sensor Network (WSN) are deployed in many application based environment and topology construction patterns like square, triangle, circle, hexagonal etc., even though it needs the basic component to make the network to communicate through the component support and essential belongings. The sensor node contains on-board sensors, processors, memory unit, transceiver the information and power supply and sensor network consists of an outsized number of sensor nodes and deployed either inside or close to the monitored object/process. The collecting and sensed data by an aggregation mechanism is called as data aggregation.

The data sensed by sensor nodes is sent to the base station [3][5]. As the sensor nodes need the base station, it may be located in very far away. In data gathering, the sensed data is gathered systematically from multiple sensors and it will be sent to the sink for advance processing [4]. The basic concept and introduction part are required for this research work.

3. Type of Sensors and its applications:

Type of sensors can be classified into different ways as listed below:

a. **Displacement Sensors**: The sensor component support with resistance, inductance, capacitance, piezoelectric.

b. **Temperature Sensors**: These types of sensors support for heating forecast from the climate changes, sea water etc., through the component such as thermostats and thermocouples.

c. **Electromagnetic radiation Sensors**: The sensor is related to the thermal and photon detectors for electromagnetic radiation technologies.

d. **Computational Power Constraints:** This sensor is related to encryption and decryption techniques, crypto algorithms, Public Key Vs Symmetric Key service are taken of this sensor.

e. **Communications Energy:** Exchange of Keys, certificates, Per-message additions (Signature, authentication tags) etc.

These types of sensors support to various environments applications such as Military, Health, environment monitoring, attack detection surveillance, home and office, industrial automotive secured etc., Most significant issues factors focusing mainly on WSN application that are the data aggregation, key distribution, authentication, energy efficient and security [6]

3.1 Basic Layout and Custom of WSN

Wireless network are sequences of vulnerable and threads to security attacks, improper protocol and low key distribution, the broadcast of transmitting and receiving data from one location to another location. Many types of WSNs are used environment application such as Terrestrial, Underground, under water, Multimedia and Mobile. Terrestrial is capable of communicating base stations efficiently which consist of 100 to 1000 of sensor nodes to be deployed either in unstructured or structured.

For example, the underground pattern is more expensive in terms of deployment, continuance and tools cost consideration with require planning; transmit the information from the sensor nodes to the base station. Additional sink nodes are located above the ground and it is difficult to recharge, whereas sensor nodes are deployed underground and main challenges are high level of attenuation and signal loss. Under water consists of number of sensor nodes and vehicles deployed under water vehicles are used for gathering data from these sensor nodes and major challenges are long propagation delay, bandwidth and sensor failures since they are equipped with a limited battery that cannot be recharged or replaced. Multimedia WSNs are used to track and monitor events in the form of multimedia, video, audio etc. These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation and it consumes high energy, large bandwidth requirements, data processing and compressing techniques [8].

3.2 Research Gap of WSM:

Mobile WSNs are comprised of sensor nodes that can be moved on their own and interacted with the physical environment to ability to sense and communicate which include better and improved coverage, better energy efficiency etc. Limitations of WSNs are

- Possess very small storage capacity
- Modest processing power-8 MHz
- Works in short communication range results in consuming a lot of power.
- Requires minimal energy – constraints protocols
- Batteries with a finite life time

- Passive devices offer little energy.

4. Potential attacks and its various protocols methodology of sensor network

a. False routing information: Fake routing control packets are injected into the network. Examples: attract / repeal traffic, generate false error messages and due to this, there will be routing loops, increased latency, decreased lifetime of the network, low reliability.

b. Selective forwarding: In WSN, the nodes faithfully forward and receive messages and compromised node might refuse to forward packets, however neighbours might start using another route [9]. So, more dangerous in compromised node forwards selected packets.

c. Sinkhole and Sybil attacks: Sinkhole attack, the WSN are highly susceptible to this kind of attack because of the communication pattern: most of the traffic is directed towards sink – single point of failure. • Sybil attack are single node pretends to be present in different parts of the network and it mostly affects geographical routing protocols

d. Denial of Service: An attack on wireless sensor networks is to jam a node or set of nodes. Jamming is the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network.

e. Traffic Analysis Attack & Rate Monitoring Attack: For an adversary to effectively render the network useless, the attacker can simply disable the base station. Rate monitoring attack makes use of the idea that nodes closest to the base station tend to forward more.

f. Key pre-distribution: Generate a large key pool and its corresponding key identifiers to create n key rings by randomly selecting k keys from P. Save key identifiers of a key ring and associated node identifier on a controller and each node load a key which is shared with a base station [10],[11].

5. Proposal Methodology

Transmitting of security data aggregate to nodes through Orthogonal Set Verification (OSV) method is proposed in this paper. The concept which implies communication system to encounter wave's form is non- deterministic due to random and unpredictable in nature of transmission the information. The data set of transmission should be statistical and probabilistic terms which are not analysis manually. With this connection, the wave's forms to construct the correction and auto correction find their true usefulness of data set.

Orthogonality is the relation of two lines or relation into 'N' dimensions, simply mentioned as perpendicularity and variety of relations describing non-overlapping / uncorrelated and independent objects to regulate the unwanted signals and lack of redundancy, to allow an error free data set transmission.

The inner product of orthogonal function (f,g) = ∫ f(x) * g(x) dx and the variable of interest in time 't' and the length of time interval is T respective of conjugate and Euclidean space, then Fourier expansion of a function tV= Tnt BT. The Ortho-normal functions are,

Case 1: the term 'n' is not equal to zero, i.i = j.k = k.i = 0. **In Case 2:** i.i = j.j = k.k = 1 .Vector A is represented in an XYZ co-ordinate system three unit vectors i, j and k in the X, Y and Z directors, corresponding between the specification of vector in terms of Ortho-normal vector components and a signal in terms of orthogonal function v(t) is ;1 : T 2 T nt π 2cos , n 0 ≠ ; T 2 T nt π 2sin , ∫= T dttVTA)(/10 ; ∫ = T n tV TA () 2 T nt π 2cos dtn 0 ≠ ; ∫ = T n tV TB ( ) 2T nt π 2cos dt.

The every transmission communicates between the two nodes and these nodes may be a straight lines transmission. The data or nodes are connected in perpendicular each other's with different angle, because of connectivity of edges of the point nodes are different direction.

6 Conclusion

The Orthogonal Set Verification (OVS) method finds the outcomes which help,

a. The direction of nodes with angle values.
b. Finding the data sends with security using of angles values.
c. To ensure the data aggregate with valid data and sending with security.

These three outcome help to make effective transmission through orthogonal set function calculation to verify the angle of direction of among nodes direction.

7. References

[1]. David and W. Carman, “New Directions in Sensor Network Key Management”, International Journal of Distributed Sensor Networks, Vol.2. No.1, pp. 3-15, 2005.

[2]. Eduru Hariprasad, J.S.V.R.S. Sastry and N. Subhash Chandra, “Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks”, SSRG International Journal of Computer Science and Engineering, Vol.1, No.7, 2014.

[3]. Eric Ke Wang, Lucas C.K.Hui and S.M.Yiu,”A New Key Establishment Scheme for Wireless Sensor Networks”, International Journal of Network Security and its Applications, Vol.1, No.2, 2009.

[4]. Kamal Kumar, A. K. Verma and R. B. Patel, “Secure Multipath routing scheme using key pre-distribution in wireless sensor network”, International Journal in Foundations of Computer Science & Technology, Vol.4, No.4, 2014.

[5]. Keith M. Martin and Maura B. Paterson, “Ultra-Lightweight Key redistribution in Wireless Sensor Networks for Monitoring Linear Infrastructure”, Information Security Group Royal Holloway, University of London supported by EPSRC grant EP/D053285/1.

[6]. Manoj kumar.A, P. Jaya prakash, M.Giri, DorinBibicu and LuminitaMoraru, “Providing efficient measurable key by using unital based key pre- distribution scheme for wireless sensor networks”, IOSR Journal of Computer Engineering, Vol.16, No.5, pp. 121-124, 2014.

[7]. J. Jose, J. Jose, and F. Jose, “A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks”, International Journal of Computer Applications, Vol.55, No.1, 2012.

[8]. N. S. Patil, P. R. Patil, “Data Aggregation in Wireless Sensor Network”, in IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[9]. S. Ozdemir, Y. Xio, “Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview”, in Journal of Computer Networks, Elsevier, Vol.53. No.12, 2009, pp. 2022–2037.

[10]. 10.L. Hu, D. Evans, “Secure Aggregation for Wireless Networks”, in Symposium on Applications and the Internet Workshops, 2003, pp. 384-391.

[11]. B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks”, in proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp. 255-265.