International Journal of Psychosocial Rehabilitation, Vol. 21, Issue 02, 2017
ISSN: 1475-7192

INSIDER ATTACKER DETECTION IN WIRELESS SENSOR NETWORK

V.Satheeswaran[1], Prajith Prakash Nair[2], S.Raja[3] Shreedharan M.D[4] and Jeganathan M[5]
[1,2&3]Assistant Professor, Department of Electronics and Communication Engineering, Nehru Institute of Technology, Coimbatore 641 105
[4]Associate Professor, Excel College of Architecture & Planning, Komarapalayam, Tamil Nadu.
[5]Assistant Professor, Department of Environment and Herbal Sciences, Tamil University, Thanjavur, Tamil Nadu.
satheesw@gmail.com jegann1978@gmail.com

ABSTRACT

Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. The Wireless sensor networks are challenged by much type of attacks like Spoofed, altered, or replayed routing Information, Selective forwarding, Sybil attacks, Wormholes, and HELLO flood.

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi-hop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks but very few can effectively and efficiently identify the intruders. To address this problem, we propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. The scheme uses many powerful algorithms in every rounds of the packet modifier or dropper identification. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme.

Keywords: *WSN, Packet modifier, Intruders, HELLO*

INTRODUCTION

In a wireless sensor network, sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards a sink, which could be a gateway, base station, storage node, or querying user. Because of the ease of deployment, the low cost of sensor nodes and the capability of self-organization, a sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise.

After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are

supposed to forward. To deal with packet droppers, a widely adopted counter - measure is multipath forwarding in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. To locate and identify packet droppers and modifiers, it has been proposed that nodes continuously monitor the for- warding behaviors of their neighbors determine if their neighbors are misbehaving, and the approach can be extended by using the reputation-based mechanisms to allow nodes to infer whether a non-neighbor node is trustable. This methodology may be subject to high energy cost incurred by the promiscuous operating mode of wireless interface; moreover, the reputation mechanisms have to be exercised with cautions to avoid or mitigate bad mouth attacks and others. Recently, Ye et al. proposed a probabilistic nested marking (PNM) scheme. But with the PNM scheme, modified packets should not be filtered out en-route because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes. In this paper, we propose a simple yet effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established.

When sensor data is transmitted along the tree structure towards the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs our proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

Our proposed scheme has the following features:

(i) Being effective in identifying both packet droppers and modifiers,

(ii) Low communication and energy overheads, and

(iii) Being compatible with existing false packet filtering schemes; that is, it can be deployed together with the false packet filtering schemes, and therefore it can not only identify intruders but also filter modified packets immediately after the modification is detected. Extensive simulation on ns2 simulator has been conducted to verify the effectiveness and efficiency of the proposed scheme in various scenarios. (Vasanthy and Jeganathan 2007, Vasanthy et.al., 2008,

Raajasubramanian et.al., 2011, Jeganathan et.al., 2012, 2014, Sridhar et.al., 2012, Gunaselvi et.al., 2014, Premalatha et.al., 2015, Seshadri et.al., 2015, Shakila et.al., 2015, Ashok et.al., 2016, Satheesh Kumar et.al., 2016).

LITERATURE SURVEY

Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications, some of which are quite sensitive in nature and require full proof secured environment. In this paper [1], they address some of the special security threats and attacks in WSNs. They propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi-hop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks but very few can effectively and efficiently identify the intruders [2]. To address this problem, the authors propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme. In this paper [3] a survey of state-of-the-art routing techniques in WSNs. They first outline the design challenges for routing protocols in WSNs followed by a comprehensive survey of routing techniques. They study the design tradeoffs between energy and communication overhead savings in every routing paradigm. We also highlight the advantages and performance issues of each routing technique. In this paper [4] an overview of some of the key areas and research in wireless sensor networks are discussed. In presenting this work, it use examples of recent work to portray the state of art and show how these solutions differ from solutions found in other distributed systems. In particular, he discusses the MAC layer, routing, node localization, clock synchronization, and power management. The author also presents a brief discussion of two current systems in order to convey overall capabilities of this technology. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the sys- tem design. There is currently enormous research potential in the field of wireless sensor network security [5]. The author's survey the major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi-hop sensor networks. Many schemes have been proposed to mitigate the attacks but none can effectively and efficiently identify the intruders. To address the problem, the authors propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets [6].

Extensive analysis and simulations using ns2 simulator have been conducted and verified the effectiveness and efficiency of the scheme. (Manikandan et.al., 2016, Sethuraman et.al., 2016, Senthil Thambi et.al., 2016, Ashok et.al., 2018, Senthilkumar et.al., 2018,).

EXISTING SYSTEM

False data injection is a severe attack that compromised nodes can launch. These nodes or moles can inject large number of bogus traffic that can lead to application failures and exhausted network resources. The Probabilistic Nested Marking scheme locate such moles within the framework of packet marking, when forwarding moles collude with source moles to manipulate the marks. Previously existing internet trace back mechanisms do not assume compromised forwarding nodes and are easily defeated by manipulated marks.

The Probabilistic Nested Marking scheme is secure against such colluding attacks. No matter how colluding moles manipulate the marks, PNM can always locate them one by one. PNM also has fast-trace back within about 50 packets, it can track down a mole up to 20 hops away from the sink. This virtually prevents any effective data injection attack. The moles will be caught before they have injected any meaningful amount of bogus traffic.

But with the PNM scheme, modified packets should not be filtered out en-route because they should be used as evidence to infer packet modifiers hence, it cannot be used together with existing packet filtering schemes.

Demerits: * Not effective in identifying both packet droppers and modifiers. * High communication and energy overheads. * Not compatible with existing false packet filtering schemes; that is, it can be deployed together with the false packet filtering schemes, and therefore it can not only identify intruders but also filter modified packets immediately after the modification is detected.

PROPOSED SYSTEM

Our proposed scheme consists of a system initialization phase and several equal-duration rounds of intruder identification phases.

1. In the initialization phase, sensor nodes form a topology which is a directed acyclic graph (DAG). A routing tree is extracted from the DAG. Data reports follow the routing tree structure.
2. In each round, data is transferred through the routing tree to the sink. Each packet sender/forwarder adds a small number of extra bits to the packet and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad (i.e., packet droppers or modifiers) and nodes that are suspiciously bad (i.e., suspected to be packet droppers and modifiers)

3. The routing tree is reshaped every round. As a certain number of rounds have passed, the sink will have collected information about node behaviors in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship.

Security Issues and Goals: The major security issues in a wireless sensor networks are said to be mainly data confidentiality, data authenticity, data integrity, data freshness, robustness and survivability which are described below. The security issues have to be minimized because even the compromise of a single node can affect the working of the network very badly.

Attacks on Sensor Network Routing: Many sensor network routing protocols are Quite simple, and for this reason are sometimes Susceptible to attacks from the literature on routing in ad-hoc networks. Most network layer attacks against sensor networks fall into one of the following categories: 1. Spoofed, altered, or replayed routing information 2. Selective forwarding 3. Sinkhole attacks 4. Sybil attacks 5. Wormholes and HELLO flood attacks

Node Categorization Algorithm: In every round, for each sensor node u, the sink keeps track of the number of packets sent from u, the sequence numbers of these packets, and the number of flips in the sequence numbers of these packets, (i.e., the sequence number changes from a large number such as Ns −1 to a small number such as 0). In the end of each round, the sink calculates the dropping ratio for each node u. Suppose nu, max is the most recently seen sequence number, nu, flip is the number of sequence number flips, and nu, rcv is the number of received packets. The dropping ratio in this round is calculated as follows:

$$d_u = \frac{n_{u,flip} * N_s + n_{u,max} + 1 - n_{u,rcv}}{n_{u,flip} * N_s + n_{u,max} + 1}.$$

Tree Reshaping and Ranking Algorithms: The tree used to forward data is dynamically changed from round to round, which enables the sink to observe the behavior of every sensor node in a large variety of routing topologies. For each of these scenarios, node categorization algorithm is applied to identify sensor nodes that are bad for sure or suspiciously bad. After multiple rounds, sink further identifies bad nodes from those that are suspiciously bad by applying several proposed heuristic methods.

RESULTS AND DISCUSSION

Network Animator is a TCL/TK based animation tool for viewing network simulation traces and real world packets traces. A network animator provides packet level animation and protocol specific graphs to aid the design and debugging of the network protocols have been describes. Taking data from network simulator or live networks NAM was one of the first tool to provide general purpose, packet level and network animation before starting to NAM, a trace file needs

to be created. This trace file is usually generated by NS. Once the trace file is generated NAM can be used to animate it.

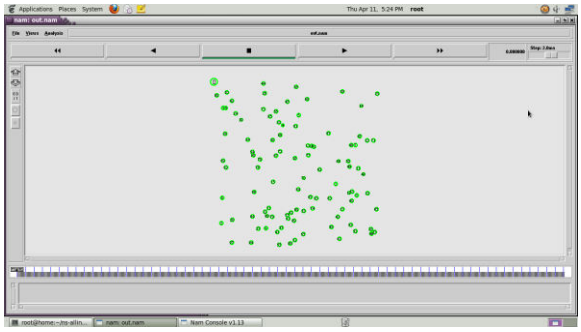


Fig 1: Creation of 100 nodes and Base station

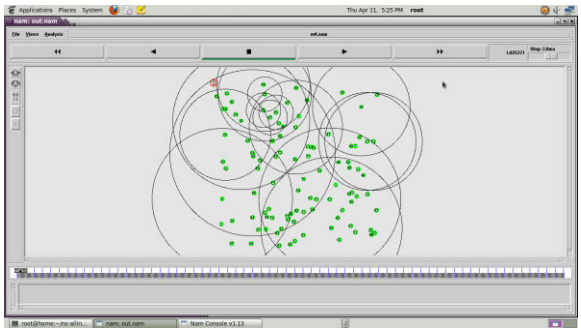


Fig 2: Node Initialization

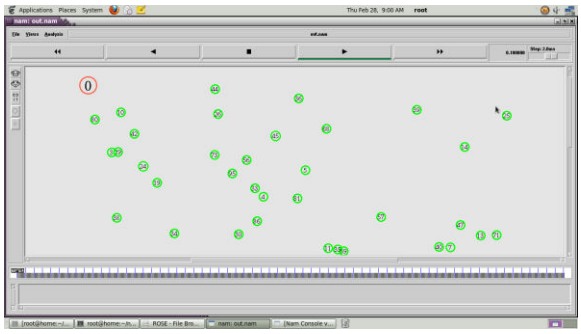


Fig 3: Before Tree Implementation

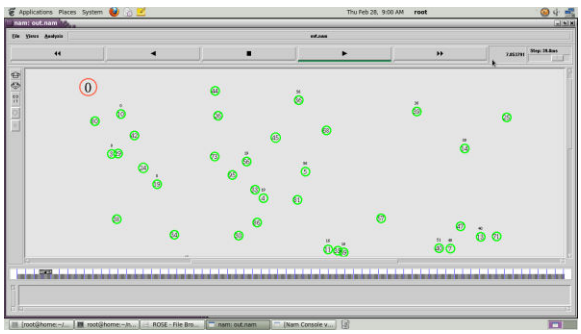


Fig 4: Establishing Tree Topology according to DAG

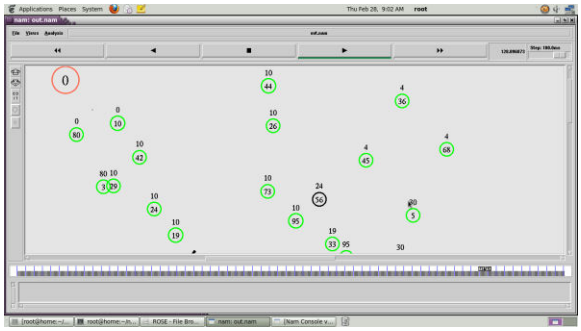
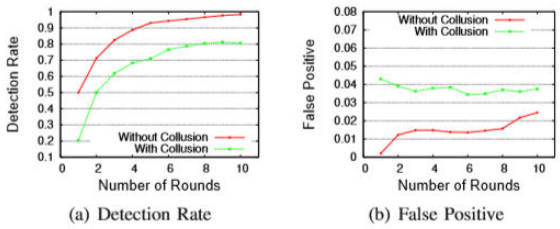


Fig 5: Tree Topology Reassigning



(a) Detection Rate (b) False Positive

Fig 6: Comparison between collusion and non-collusion

CONCLUSION AND FUTURE WORK

To address the problem of packet dropping and modification we propose a simple yet effective scheme to identify misbehaving forwarders that drop or modify packets. Each packet is encrypted and padded so as to hide the source of the packet. The packet mark, a small number of extra bits, is added in each packet such that the sink can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. The routing tree structure dynamically changes in each round so that behaviors of sensor nodes can be observed in a large variety of scenarios. Finally, most of the bad nodes can be identified by our heuristic ranking algorithms with small false positive. Extensive analysis, simulations and implementation have been conducted and verified the effectiveness of the proposed scheme.

Our scheme can be used for effectively finding the packet droppers and modifiers in a wireless network. The proposed scheme can be extended for identifying packet modifiers. Particularly, it can be slightly modified so that the statistical en-route filtering scheme (SEF) and the interleaved hop-by-hop authentication scheme can be deployed to filter the modified packets.

Even though the lower layers can be secured by using our scheme the upper layers of the network are still under crisis. In future we are hoping to encounter this security threats faced by the upper layers of the network proving it with hybrid security solutions.

REFERENCES

[1] Siba K. Udgata, Alefiah Mubeen Department of Computer & Information Sciences University of Hyderabad, Samrat L. Sabat School of Physics University of Hyderabad, Wireless Sensor Network Security model using Zero Knowledge Protocol, 2011

[2] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang, Member, IEEE, Catching Packet Droppers and Modifiers in Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 2011

[3] Jamal N. Al-Karaki, The Hashemite University, Ahmed E. Kamal, Iowa State University, Routing Techniques in Wireless Sensor Networks: A Survey, 2009

[4] John A. Stankovic, Department of Computer Science, University of Virginia, Wireless Sensor Networks, June 19, 2006.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary Department of Computer Science Wayne State University, Wireless Sensor Network Security: A Survey, 2006.

[6] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, and Wensheng Zhang, Department of Computer Science, Iowa State University, Department of Computer Science, New Jersey Institute of Technology, Catching Packet Droppers and Modifiers in Wireless Sensor Networks, 2005

[7] Joseph Migga Kizza, Implementing Security in Wireless Sensor Networks, 2005

[8] Winnie Louis Lee, Amitava Datta, and Rachel Cardell-Oliver School of Computer Science & Software Engineering The University of Western Australia, Network Management in Wireless Sensor Networks, 2004

[9] F. L. LEWIS Associate Director for Research Head, Advanced Controls, Sensors, and MEMS Group Automation and Robotics Research Institute The University of Texas at Arlington, Wireless Sensor Networks, 2004

[10] Hemanta Kumar Kalita and Avijit Kar, Department of Computer Engineering, Jadavpur University, Kolkata, India, Wireless Sensor Network Security Analysis, 2004

[11] [11]. Sushma, Asstt. Prof, HIT Asodha, (India), Deepak Nandal, Student, P.D.M. Bahadurgarh, (India), Vikas Nandal, Asstt. Prof, U.I.E.T. Rohtak, (India), Security Threats in Wireless Sensor Networks, 2004.

[12] Deborah Estrin, Sensor Network Protocols, 2003

[13] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A Survey on Sensor Networks. IEEE Communications Magazine, 2002.

[14] M. Al Ameen, S. Riazul Islam, and Kyung Sup Kwak. Energy Saving Mechanisms for MAC Protocols in Wireless Sensor Networks. International Journal of Distributed Sensor Networks (IJDSN), 2002.

[15] Anwar and L. Lavagno, Energy and Throughput Optimization of a Zigbee-Compatible MAC Protocol for Wireless Sensor Networks. In Seventh International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP10), Newcastle upon Tyne, England, July 2001.

[16] F. Ashraf, R. Crepaldi, and R. Kravets. Know Your Neighborhood: A Strategy for Energy- Efficient Communication. In IEEE Seventh International Conference on Mobile Ad Hoc and Sensor Systems (MASS10), San Francisco, CA, November 2001.

[17] S. Chandra. Wireless Network Interface Energy Consumption: Implications for Popular Streaming Formats. ACM Multimedia Systems Journal, 2000.

[18] S. Chatterjea, L. van Hoesel, and P. Havinga. AI-LMAC: An Adaptive, Information-Centric and Lightweight MAC Protocol for Wireless Sensor Networks. In The Second International Conference on Intelligent Sensors, Sensor Networks and Information Processing(ISSNIP04), pages 381 – 388, Melbourne, Australia, December 2000.

[19] C.Y. Chong and S.P. Kumar. Sensor Networks: Evolution, Opportunities, and Challenges. Proceedings of the IEEE, 91(8):1247 – 1256, August 2001.

[20] S. Coleri, A. Puri, and P. Varaiya. Power Efficient System for Sensor Networks. In The Eighth IEEE International Symposium on Computers and Communications (ISCC03), pages 837 – 842, Kiris-Kemer, Turkey, July 1999.

[21] M. Demircin and P. van Beek. Bandwidth Estimation and Robust Video Streaming Over 802.11e Wireless Lans. In IEEE International Conference on Multimedia and Expo (ICME 2005), pages 1250– 1253, Amsterdam, Netherlands, July 1998.

[22] G.P. Halkes and K.G. Langendoen. Crankshaft: An Energy-Efficient MAC-Protocol For Dense Wire- less Sensor Networks. In The Fourth European Conference on Wireless Sensor Networks (EWSN07), pages 228 – 244, Delft, Netherlands, January 1998.

[23] S. Liu, K. Fan, and P. Sinha. CMAC: An Energy Efficient MAC Layer Protocol Using Convergent Packet Forwarding for Wireless Sensor Networks. In Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks(SECON07), San Diego, CA, June 1997.

[24] H. Pham and S. Jha. An Adaptive Mobility-Aware MAC Protocol for Sensor Networks (MS-MAC). In The IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, Fort Lauderdale, FL, October 1996.

[25] V. Rajendran, K. Obraczka, and J. Garcia-Lina-Aceve. Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks. IEEE Transactions on Mobile Computing, 1(4):278 – 292, 1996.

[26] H. Zhu, M. Li, I. Shiny, and B.Prabhakaran. A Survey of Quality of Service in IEEE 802.11 Networks. IEEE Wireless Communications, 11(4):6 – 14, August 1996.

[27] Y. Zhao, C. Miao, and M. Ma. Performance of Adaptive Scheduling MAC (AS-MAC) Protocol with Different AS-Period in Multi-Hop Networks. In The Sixth IEEE Conference on Industrial Electronics and Applications (ICIEA11), pages 1881 – 1886, Beijing, China, June 1996.

[28] T. Zheng, M. Reshma, and V. Sarangan. PMAC: An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks. In The 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS05), pages 65 – 72, Denver, CO, April 1996

[29] O. Younis and S. Sriram. Distributed Clustering in Ad-Hoc Sensor Networks: A Hybrid, Energy- Efficient Approach. In The IEEE 23rd Annual Joint Conference of the IEEE Computer and Com- munications Societies (InfoCom04), pages 629 – 640, Hong Kong, China, March 1996.

[30] B. Yahya and J. Ben-Othman. An Adaptive Mobility Aware and Energy Efficient MAC Protocol for Wireless Sensor Networks. In IEEE Symposium on Computers and Communications (ISCC09), pages 15 – 21, Sousse, Tunisia, February 1996.

[31] J. Yin, X. Wang, and D. Agrawal. Optimal Packet Size in Error-Prone Channel for IEEE 802.11 Distributed Coordination Function. In IEEE Wireless Communications and Networking Conference (WCNC04), volume 3, pages 1654 – 1659, January 1996.

[32] X. Yuan, S. Bagga, Soumya Bhaskaran, and D. Benhaddou. DS-MAC: Differential Service Medium Access Control Design for Wireless Medical Information Systems. In The 30th Annual IEEE Conference on Engineering in Medicine and Biology Society, pages 1801 – 1804, Vancouver, BC, December 1995.

[33] T. Zauner, L. Haslett, W. Hu, S. Jha, and C. Sreenan. A Congestion-Aware Medium Access Control Protocol for Multi-rate Ad-hoc Networks. In The 31st IEEE International Conference on Local Computer Networks (LCN06), pages 97 – 104, Tampa, FL, October 1995

[34] S. Sundresh, W. Kim, and G. Agha. SENS: A Sensor, Environment and Network Simulator. In The IEEE 37th Annual Symposium on Simulation (ANSS04), pages 221 – 228, Arlington, VA, April 1995.

[35] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler. An Analysis of a Large Scale Habitat Monitoring Application. In The Second International Conference on Embedded Networked Sensor Systems (SenSys04), pages 214 – 226, Baltimore, March 1995.

[36] Vasanthy M and M. Jeganathan. 2007. Ambient air quality in terms of NOx in and around Ariyalur, Perambalur DT, Tamil Nadu. Jr. of Industrial pollution Control., 23(1):141-144.

[37] Vasanthy. M ,A.Geetha, M. Jeganathan,and A.Anitha. 2007. A study on drinking water quality in Ariyalur area. J.Nature Environment and Pollution Technology. 8(1):253-256.

[38] Ramanathan R ,M. Jeganathan, and T. Jeyakavitha. 2006. Impact of cement dust on azadirachtain dicaleaves – ameasure of air pollution in and Around Ariyalur. J. Industrial Pollution Control. 22 (2): 273-276.

[39] Vasanthy M and M. Jeganathan. 2007. Ambient air quality in terms of NOx in and around Ariyalur, Perambalur DT, Tamil Nadu. Pollution Research., 27(1):165-167.

[40] Vasanthy M and M. Jeganathan. 2008.Monitoring of air quality in terms of respirable particulate matter – A case study. Jr. of Industrial pollution Control.,24(1):53 - 55.

[41] Vasanthy M, A.Geetha, M. Jeganathan, and M. Buvaneswari. 2008. Phytoremediation of aqueous dye solution using blue devil (Eichhornia crassipes). J. Current Science. 9 (2): 903-906.

[42] Raajasubramanian D, P. Sundaramoorthy, L. Baskaran, K. Sankar Ganesh, AL.A. Chidambaram and M. Jeganathan. 2011. Effect of cement dust pollution on germination

and growth of groundnut (*Arachis hypogaea* L.). IRMJ-Ecology. International Multidisciplinary Research Journal 2011, 1/1:25-30 : ISSN: 2231-6302: Available Online: http://irjs.info/.

[43] Raajasubramanian D, P. Sundaramoorthy, L. Baskaran, K. Sankar Ganesh, AL.A. Chidambaram and M. Jeganathan. 2011. Cement dust pollution on growth and yield attributes of groundnut. (*Arachis hypogaea* L.). IRMJ-Ecology. International Multidisciplinary Research Journal 2011, 1/1:31-36.ISSN: 2231-6302. Available Online: http://irjs.info/

[44] Jeganathan M, K. Sridhar and J.Abbas Mohaideen. 2012. Analysis of meterological conditions of Ariyalur and construction of wind roses for the period of 5 years from January 2002. J.Ecotoxicol.Environ.Monit., 22(4): 375-384.

[45] Sridhar K, J.Abbas Mohaideen M. Jeganathan and P Jayakumar. 2012. Monitoring of air quality in terms of respirable particulate matter at Ariyalur, Tamilnadu. J.Ecotoxicol.Environ.Monit., 22(5): 401-406.

[46] Jeganathan M, K Maharajan C Sivasubramaniyan and A Manisekar. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of *healianthus annus* plant – a case study. J.Ecotoxicol.Environ.Monit., 24(1): 29-34.

[47] Jeganathan M, C Sivasubramaniyan A Manisekar and M Vasanthy. 2014. Determination of cement kiln exhaust on air quality of ariyalur in terms of suspended particulate matter – a case study. IJPBA. 5(3): 1235-1243. ISSN:0976-3333.

[48] Jeganathan M, S Gunaselvi K C Pazhani and M Vasanthy. 2014. Impact of cement dust pollution on floral morphology and chlorophyll of *healianthus annus.*plant a case study. IJPBA. 5(3): 1231-1234. ISSN:0976-3333.

[49] Gunaselvi S, K C Pazhani and M. Jeganathan. 2014. Energy conservation and environmental management on uncertainty reduction in pollution by combustion of swirl burners. J. Ecotoxicol. Environ.Monit., 24(1): 1-11.

[50] Jeganathan M, G Nageswari and M Vasanthy. 2014. A Survey of traditional medicinal plant of Ariyalur District in Tamilnadu. IJPBA. 5(3): 1244-1248. ISSN:0976-3333.

[51] Premalatha P, C. Sivasubramanian, P Satheeshkumar, M. Jeganathan and M. Balakumari.2015. Effect of cement dust pollution on certain physical and biochemical parameters of castor plant (*ricinus communis*). IAJMR.1(2): 181-185.ISSN: 2454-1370.

[52] Premalatha P, C. Sivasubramanian, P Satheeshkumar, M. Jeganathan and M. Balakumari.2015. Estimation of physico-chemical parameters on silver beach marine water of cuddalore district. Life Science Archives. 1(2): 196-199.ISSN: 2454-1354.

[53] Seshadri V, C. Sivasubramanian P. Satheeshkumar M. Jeganathan and Balakumari.2015. Comparative macronutrient, micronutrient and biochemical constituents analysis of *arachis hypogaea.* IAJMR.1(2): 186-190.ISSN: 2454-1370.

[54] Seshadri V, C. Sivasubramanian P. Satheeshkumar M. Jeganathan and Balakumari.2015. A detailed study on the effect of air pollution on certain physical and bio chemical parameters of *mangifera indica* plant.Life Science Archives. 1(2): 200-203.ISSN: 2454-1354.

[55] Shakila N, C. Sivasubramanian, P. Satheeshkumar, M. Jeganathan and Balakumari.2015. Effect of municipal sewage water on soil chemical composition- A executive summary. IAJMR.1(2): 191-195.ISSN: 2454-1370.

[56] Shakila N, C. Sivasubramanian, P. Satheeshkumar, M. Jeganathan and Balakumari.2015. Bacterial enumeration in surface and bottom waters of two different

fresh water aquatic eco systems in Ariyalur, Tamillnadu. Life Science Archives. 1(2): 204-207.ISSN: 2454-1354.

[57] Ashok J, S. Senthamil kumar, P. Satheesh kumar and M. Jeganathan. 2016. Analysis of meteorological conditions of ariyalur district. Life Science Archives. 2(3): 579-585.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.

[58] Ashok J, S. Senthamil Kumar, P. Satheesh Kumar and M. Jeganathan. 2016. Analysis of meteorological conditions of cuddalore district. IAJMR.2 (3): 603-608.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.

[59] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. South Indian vernacular architecture -A executive summary. IAJMR.2 (4): 655-661.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.

[60] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. Green buildings - A review. Life Science Archives. 2(3): 586-590.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.

[61] Satheesh Kumar P, C. Sivasubramanian, M. Jeganathan and J. Ashok. 2016. Indoor outdoor green plantation in buildings - A case study. IAJMR.2 (3): 649-654.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.

[62] Manikandan R, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. Assessment of ground water quality in Cuddalore district, Tamilnadu, India. Life Science Archives. 2(4): 628-636.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.

[63] Manikandan R, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. A study on water quality assessment of Ariyalur district, Tamilnadu, India. IAJMR.2 (4): 687-692.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.

[64] Sethuraman G, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. Assessment of air quality in Ariyalur, Tamilnadu, India. Life Science Archives. 2(4): 637-640.ISSN: 2454-1354. DOI: 10.21276/lsa.2016.2.3.9.

[65] Sethuraman G, M. Jeganathan, P. Satheesh Kumar and J. Ashok. 2016. A study on air quality assessment of Neyveli, Tamilnadu, India. IAJMR.2 (4): 693-697.ISSN: 2454-1370. DOI: 10.21276/iajmr.2016.2.3.3.

[66] Senthil Thambi J, C. Sivasubramanian and M. Jeganathan. 2018. Ambient Air quality monitoring in terms of (Nitrogen di oxide in and around Ariyalur District, Tamilnadu, India. IAJMR.4 (3): 1414-1417.ISSN: 2454-1370. DOI: 10.22192/iajmr.2018.4.3.2.

[67] Senthil Thambi J, C. Sivasubramanian and M. Jeganathan. 2018. Study of Air pollution due to vehicle emission in Ariyalur District, Tamilnadu, India. Life Science Archives. 4(4): 1409-1416.ISSN: 2454-1354. DOI: 10.22192/lsa.2018.4.4.3.

[68] Ashok J, S.Senthamil kumar, P.Satheesh kumar and M.Jeganathan. 2018. Estimation of Cement kiln exhaust on Air quality of Ariyalur in terms of suspended particulate matter - A Case Study. International Journal Of Civil Engineering And Technology. 9 (12): Scopus Indexed Journal ISSN: 0976 – 6316.

[69] Ashok J, S.Senthamil kumar, P.Satheesh kumar and M.Jeganathan.2018. Air quality assessment of Neyveli in Cuddalore District, Tamilnadu, India. International Journal Of Civil Engineering And Technology. 9 (12): Scopus Indexed Journal ISSN: 0976 – 6316.

[70] Senthilkumar M, N. Nagarajan, M. Jeganathan and M. Santhiya. 2018. Survey of Medicinal Plants diversity on Bodha Hills in Salem District, Tamil Nadu, India. Indo – Asian Journal Of Multidisciplinary Research (IAJMR) ISSN: 2454-1370.

[71] Senthilkumar M, N. Nagarajan, M. Jeganathan and M. Santhiya. 2018. Survey of Traditional Medicinal Plants in and around Ariyalur in TamilNadu, India. Life Science Archives (LSA) ISSN: 2454-1354. DOI: 10.22192/lsa.2018.4.6.5.

[72] Malarvannan J, C. Sivasubramanian, R. Sivasankar, M. Jeganathan and M. Balakumari. 2016. Shading of building as a preventive measure for passive cooling and energy conservation – A case study. Indo – Asian Journal of Multidisciplinary Research (IAJMR): ISSN: 2454-1370. Volume – 2; Issue - 6; Year – 2016; Page: 906 – 910. DOI: 10.21276.iajmr.2016.2.6.10.

[73] Malarvannan J, C. Sivasubramanian, R. Sivasankar, M. Jeganathan and M. Balakumari. 2016. Assessment of water resource consumption in building construction in tamilnadu, India. Life Science Archives (LSA) ISSN: 2454-1354 Volume – 2; Issue - 6; Year – 2016; Page: 827 – 831 DOI: 10.21276/lsa.2016.2.6.7.

[74] Sivasankar R, C. Sivasubramanian, J. Malarvannan, M. Jeganathan and M. Balakumari. 2016. A Study on water conservation aspects of green buildings. Life Science Archives (LSA),ISSN: 2454-1354. Volume – 2; Issue - 6; Year – 2016; Page: 832 – 836, DOI: 10.21276/lsa.2016.2.6.8.

[75] Ashok J , S. Senthamil Kumar , P. Satheesh Kumar and M. Jeganathan. 2016. Analysis and design of heat resistant in building structures. Life Science Archives (LSA), ISSN: 2454-1354. Volume – 2; Issue - 6; Year – 2016; Page: 842 – 847. DOI: 10.21276/lsa.2016.2.6.10.