ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Wireless Sensor Network Security on Latency Control Configuration

Felomino P. Alba[1], Dr. Enrique Festijo[2]

IT-Instructor, Institute of Computing Engineering and Technology, SPAMAST, Digos City, Davao, Philippines[1]

Professor, Graduate Programs, Technological Institute of the Philippines, Quezon City, Philippines[2]

Abstract: In the previous years, wireless sensor network (WSN) is captive with unbelievable change in technology. It imply to monitoring, controlling, tracking and evaluating. On this paper, the researchers discussed Wireless Sensor Network that focuses on security. The technology applied on this research paper includes measurement on latency configuration on how to secure network. Wireless Sensor Network will be the future of communication and it plays the vital rule of super internet in the future were all data are powered by wireless communication for transmission. However, solutions on security especially on Wireless Sensor Network are very limited. This gap is the main target on this research paper. It discusses on how to provide security on Wireless Sensor Network latency configuration. In this research paper we present an experimental evaluation of Dynamic Resource Routing (DSR) and Self Selective Routing. The research paper is very useful and helpful to all network designer and network administrator and generally to the entire community. The researchers conduct the experiments within the cygwin and g-sense simulator.

Keywords: Network Security, Wireless Sensor Network Security, Latency, Layer, Network Layer, Media Access layer.

I. INTRODUCTION

According to the author of Publish Journal entitled Wireless Sensor Network, The (WSN) wireless network sensor is a adhock network that are separated by distance elements and system configuration with protocol settings [2],[3]. The nodes between devices play a vital role that connects each one to communicate a certain volume of nodes called as latency. When the nodes from one point of devices is sent through another devices, the verification of how the nodes was acquired while in the process of sending remains the greatest key concepts of this research. How could we determine that the nodes from devices significantly sent without errors and what are the approaches best applied from both devices points. While the sensor nodes that transmit data based on the devices output is with a mechanism of receiving and sending is sufficient and efficient enough to thoroughly be identified as secured. Between two devices the nodes passing and communicating on each devices is going to stress of nodes sender and nodes receiver.

Latency between the devices provides the best way on understanding connectivity security of wireless sensor network. All the latency approaches are possible avenue that can provide clarity on how we can determine the solution of securing the nodes between devices. Wireless Sensor network share the same connection property like computer network. The connectivity between computers to another computer is the simplest example of how network works. When typical network of computers connect with each other, they are govern by different rules and policy. On the other hand, the connection that appears and present between the two devices on how and why they are connected is empowered by occurrences of different factors. One of the main factors is nodes latency communication. Now on this research paper, the researchers going to discuss several security issues governing latency that govern networks. Sensor networks are expected to play an essential role in the upcoming age of pervasive computing [20]. Interference on nodes between devices while in connection result to failure on latency configuration. Failure of stabilizing the configuration into normal state of connection latency when sending devices and receiving device transmits nodes.

Inability of devices to develop latency security protocol during the devices attempts to re-connect. Establish an advance mechanism between connected devices when connection are attempted to be interfered through means of distance. Create minimum and maximum latency volume that will stabilized the connection latency of a devices which is connected to another device. Develop security protocol for latency security to devices that attempts to re-connect on other devices.

II. PRELIMINARY REVIEW OF LITERATURE

Wireless sensor networks introduce new security challenges due to their dynamic topology, severe resource constraints, and absence of a trusted infrastructure [1], [3]. In a typical WSN we see following network components: Sensor motes (Field devices) Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

with the process itself. [9]. Gateway or Access points A Gateway enables communication between Host application and field devices. Network manager A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network. Security manager The Security Manager is responsible for the generation, storage, and management of keys. [15] International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009. For secure transmission of various types of information over sensor networks, several cryptographic techniques are used: symmetric key ciphers and asymmetric key ciphers. The security of asymmetric cryptography depends on the difficulty of a mathematical problem and the resulting algorithm consumes considerably more energy than symmetric key ciphers, which are constructed by iteratively applying simple cryptographic operations [1].

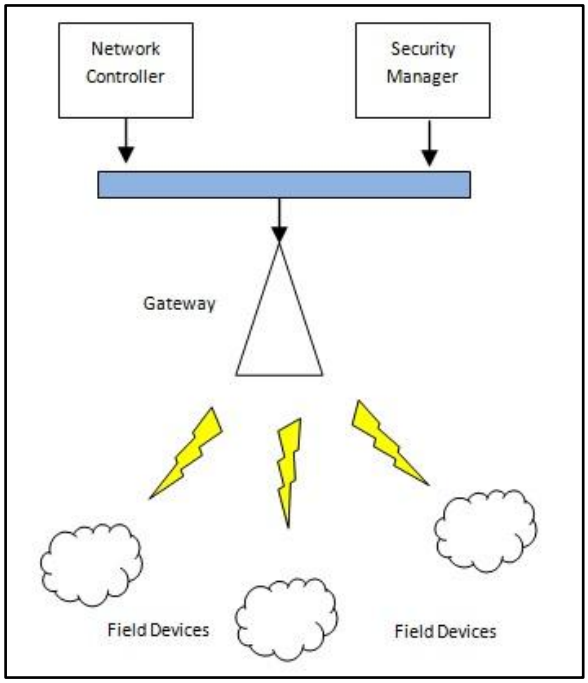

Figure 1 Wireless Sensor Network Architecture

A sensor network is a special type of Adhoc network. So it shares some common property as computer network. There are usually several security requirements to protect a network. Security Threats A threat is a circumstance or event with the potential to adversely impact a system through a security breach and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk. There can be many potential threats to WSNs, for example, power drainage, physical tampering, extinction immediately up on deployment due to the hostile environment or deliberate attempts to subvert a node by breaching the security. The categories of the threats could be (a) Passive Information Gathering, (b) Subversion of node or Insertion of a false node, (c) node malfunction, (d) node outage, (e) message corruption, (f) denial of service, or (g) traffic analysis [4]

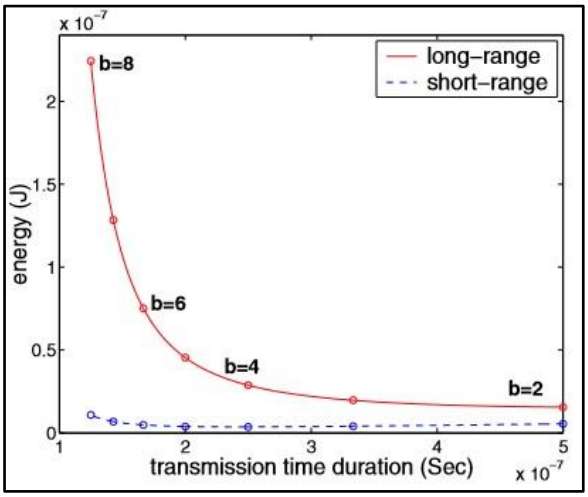

Figure 2 Transmission Time Duration (Seconds)

Figure 2 plots the energy functions with b 2, 8 for the long and short range communication based on the above analysis. In practice, b is typically set to positive integers (indicated by circles in the figure), resulting in discrete values of . It can be observed that the transmission energy for the short-range communication eventually increases after the transmission time exceeds 300 n Sec. intuitively; it is more beneficial to explore the energy-latency tradeoffs for the long range communication. However, we demonstrate in Section VI that up to 60 energy savings can still be achieved by our algorithms for the short-range communication [12].

By relying on slightly different assumption, we define two interesting problems, the k-traveling salesperson problem with neighborhood (k-TSPN) and the krooted path cover problem with neighborhood (k-PCPN). Since both problems are NP-hard, we propose constant factor approximation algorithms for them. Our simulation results indicate our algorithms outperform their alternatives [7]. Although most, if not all, security threats against the TCP/IP stack in a wired network are equally applicable to an IP-based wireless network, the latter possesses a number of additional vulnerabilities; wireless medium unreliability, spectrum use, power management, security, limited bandwidth, system complexity, routing, Interfacing with wired networks and health concern make it more challenging to secure[14],[22]. Each node performs some sensing of a particular confined area, and sends the result to a data collecting node (called sink) in a multi-hop fashion, using other nodes as relays [8]. Packet loss that occurs due to mobility of the sensor nodes is one of main challenges in Wireless Sensor Network (WSN) and it comes in parallel with energy consumption [5]. We focus on data collection application in sensor networks and use the term data mules to refer to such mobile devices from now on [11]. Wireless sensor network (WSN) is a heterogeneous system combining thousands to millions of tiny, inexpensive sensor nodes with several distinguishing

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

characteristics [4]. Both scheduling first and routing first scheme have their disadvantages [1],[10]. A sensor node integrates hardware and software for sensing, data processing, and communication [21], [22].

Algorithm for Initial Route Construction

Present an algorithm for initial time-dependent shortest path route construction in duty-cycled WSNs, where the distances from all nodes to the sink node are initially infinite. The proposed algorithm, referred to as the FTSP algorithm, for Fast Time-Dependent Shortest Path algorithm, is inspired by the work infinite [9].

Latency Network Leak

These services leak some information about the network latency between the sender and one or more nodes in the system. We present two attacks on low-latency anonymity schemes using this information. The first attack allows a pair of colluding Web sites to predict, based on local timing information and with no additional resources, whether two connections from the same Tor exit node are using the same circuit with high confidence. The second attack requires more resources but allows a malicious Web site to gain several bits of information about a client each time he visits the site. We evaluate both attacks against two low-latency anonymity protocols—the Tor network and the Multi-Proxy proxy aggregator service—and conclude that both are highly vulnerable to these attacks [16].

Basic Security Schemes in WSN

To address the kernel security issues in WSNs, we talk about cryptography and its applicability. Basically, the major challenge for employing any efficient security scheme in WSNs is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensor nodes, as well as the limited communication capacity [1]. Simulation studies, we have performed a series of simulations to validate the results concerning latency [8].

III. METHODOLOGY

Data Modeling

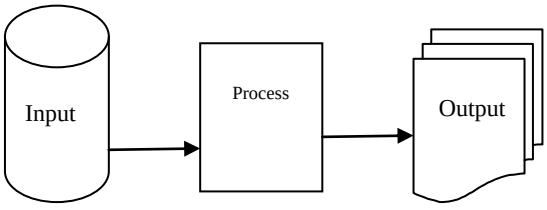

Figure 3 Input Process Output

Figure 3 presents the Input and Process and Output. The inputs are Stop Time, Number of Nodes, and Terrain Size in Meters, Number of Source of Nodes, Packet Size and Time Interval by Seconds. The process clearly defines the application of appropriate algorithm to come-up with desired output. These figures also illustrate the entire Operation Framework undertaken on this research paper. It was conducted simulation using the cygwin and g-sense simulator.

Testing and Simulation Data

StopTime	Nodes	TerrainSize	Source	Size	Interval
4	16	1200	24	128	4
8	30	2400	24	256	4
12	45	3600	24	512	4

The table 1.0 Data

The table 1.0 represents the testing and simulation data used, Stop Time, Number of Nodes, Terrain size in Meters, Number of Source of Nodes, Packet Size and Time Interval by seconds.

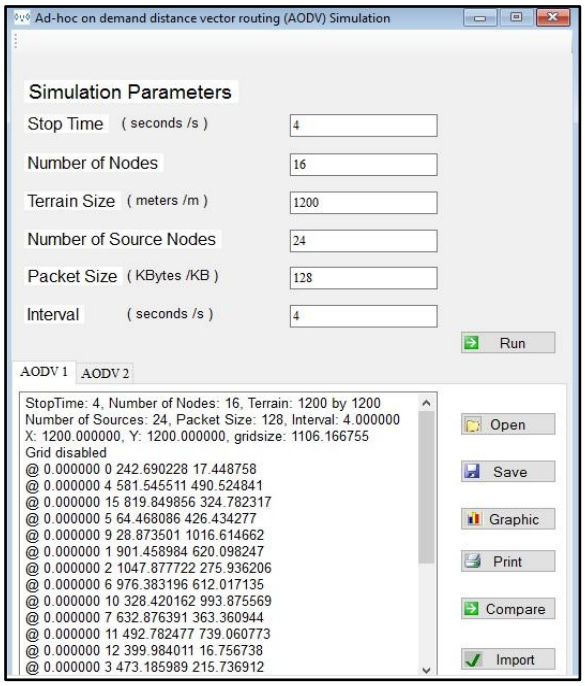

Figure 4 Ad-hoc distance Vector Routing

Figure 4 presents the simulation parameters for Ad-hoc on demand Distance vector routing. Stop Time is 4, Number of nodes is 16, Terrain Size in Meters 1200, Number of Source Nodes 23, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4.

Figure 5 presents the simulation parameters for Ad-hoc on demand Distance vector routing. Stop Time is 4, Number of nodes is 16, Terrain Size in Meters 1200, Number of Source Nodes 24, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4 with graphical presentation of position Y and X. The positions X represent the Distance of Latency Travelling. The Graph also present success rate of 20.5 for application layer, 0.69869 for network layer, 0.627737 Media Access Control Layer. The delay of latency is 0.127 seconds with the average hop of 4.000.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

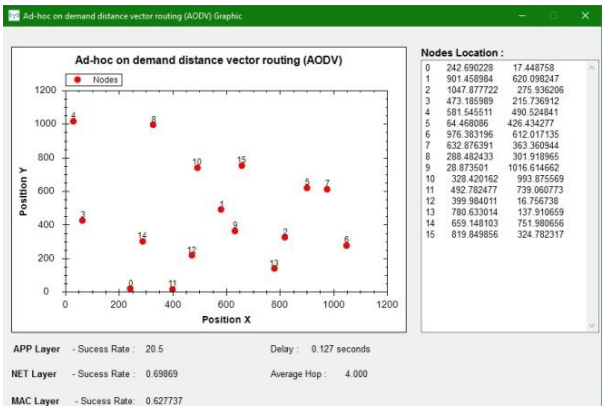

Figure 5 Ad-hoc DVR Graph

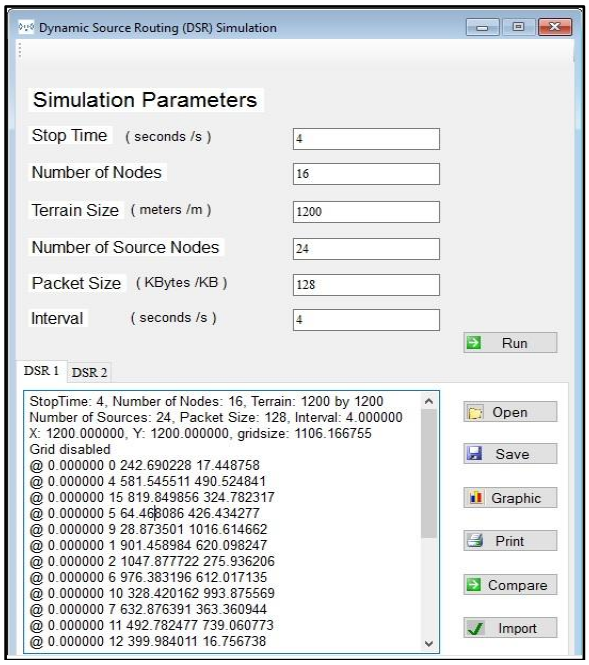

Figure 6 Dynamic Source Routing

Figure 6 presents the simulation parameters for Dynamic Source Routing. Stop Time is 4, Number of nodes is 16, Terrain Size in Meters 1200, Number of Source Nodes 23, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4.

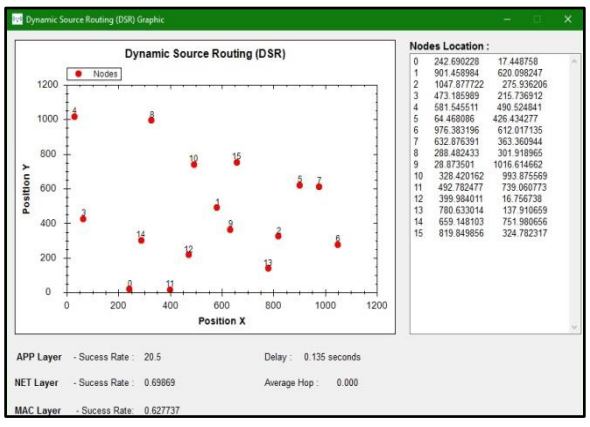

Figure 7 Dynamic Source Routing Graph

Figure 7 presents the simulation parameters for Dynamic Source Routing Graph. Stop Time is 4, Number of nodes is 16, Terrain Size in Meters 1200, Number of Source Nodes 23, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4 with graphical presentation of position Y and X. The positions X represent the Distance of Latency Travelling. The Graph also present success rate of 20.5 for application layer, 0.69869 for network layer, 0.627737 Media Access Control Layer. The delay of latency is 0.135 seconds with the average hop of 0.000.

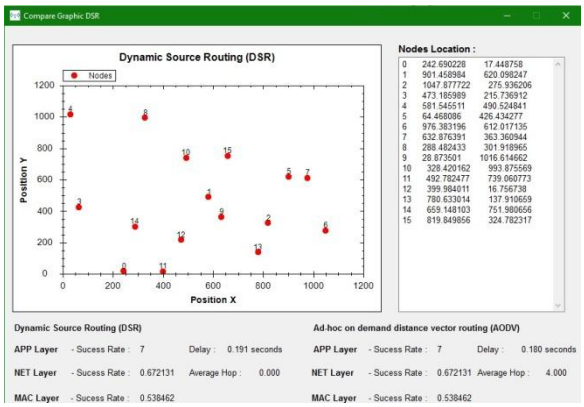

Figure 8 Comparison Graphic of DSN and Ad-Hoc demand Vector Routing

Figure 8 presents the simulation parameters for Dynamic Source Routing Graph. Stop Time is 4, Number of nodes is 16, Terrain Size in Meters 1200, Number of Source Nodes 24, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4 with graphical presentation of position Y and X. The positions X represent the Distance of Latency Travelling. The Graph also present success rate of 7 for application layer, 0.672131 for network layer, 0.538462 Media Access Control Layer. The delay of latency is 0.191 seconds with the average hop of 0.000 compared to Simple Flooding; success rate of 7 for application layer, 0.672131 for network layer, 0.538462 Media Access Control Layer. The delay of latency is 0.180 seconds with the average hop of 4.000.

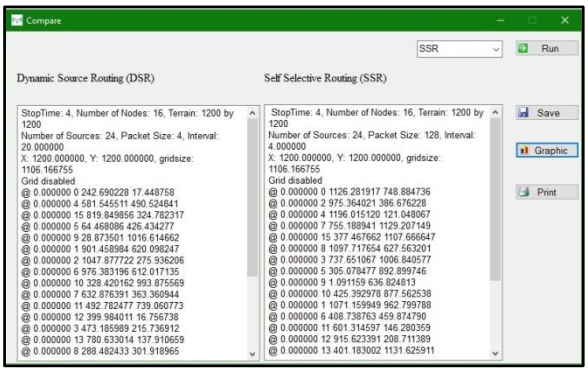

Figure 9 Comparison Nodes Result of DSN and Self Selective Routing

Figure 9 presents the simulation parameters for Dynamic Source Routing Graph. Stop Time is 4, Number of nodes

DOI 10.17148/IJARCCE.2017.6201

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

is 16, Terrain Size in Meters 1200, Number of Source Nodes 23, Packet Size in Kilobyte 128 and Time Interval in Seconds is 4.

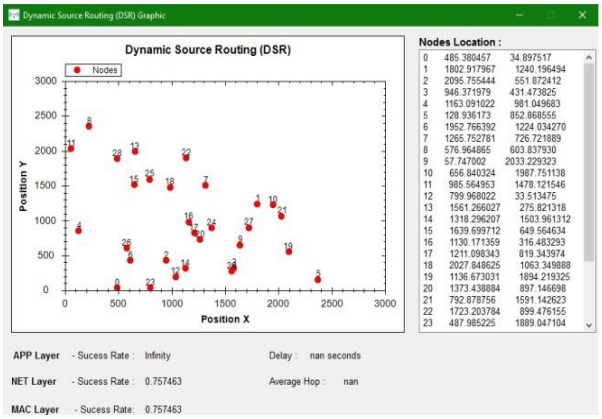

Figure 10 Dynamic Source Routing Graph

Figure 10 presents the simulation parameters for Dynamic Source Routing Graph. Stop Time is 8, Number of nodes is 30, Terrain Size in Meters 2400, Number of Source Nodes 24, Packet Size in Kilobyte 256 and Time Interval in Seconds is 4 with graphical presentation of position Y and X. The positions X represent the Distance of Latency Travelling. The Graph also present success rate of infinity for application layer, 0.757463 for network layer, 0.757463 Media Access Control Layer. The delay of latency is zero (0) seconds with the average hop of (0).

IV. RESULT AND DISCUSSION

The research paper discusses the security implementation on latency between nodes. It was routing configuration of network, going to the next routing phase and to the next hop. When the passing nodes go through with different level of parameters, it was there that latency was measured. The conclusion on measuring and anticipating latency defines how long it will take to be transmitted from separate devices. Comparing the different approach on measuring latency gives us the best anticipation solution. From Ad-hoc compared to Dynamic Source Routing, the two different approaches give the same result on Application layer, Media Access Control Layer and Network Layer. The varying between the two are, the packets delay on transmission and average hop between devices. After several testing and simulation, we found out that latency on network configuration is one of best techniques on creating network security. Developed scheme that connect to the nearest nodes from where the existing connection nodes propagate. Select correct methods for different nodes such as Application Layer, Media Access Control and Network Layer. Present different techniques on connecting nodes. Additionally, Ad-hoc Routing, Dynamic Source Routing, Self Selective Routing are possible approaches that was used to simulate the data presented. Wireless sensor network is still subjects to different security problem.

V. CONCLUSION AND RECOMMENDATION

The researchers concluded based on the data simulated that, the nodes are affected while being transmitted especially with greater distance. The effects of distance to latency configuration are a great factor that determined lesser time delay. While connection between nearer hop is much lesser in time delay, these conclude to put up a much closer hop that connects the entire multiple nodes. The simulation purposes are to create a real time scenario and it was based on legitimate data.

It is recommended to have further research on the following topics: Time Delay interval that interferes on connecting devices security. Cryptography on setting up configuration for transmission and receiving. Establish local network policies on security, it will govern the entirety of users. Conduct researches on new network security approaches and protocols.

ACKNOWLEDGMENT

This research was made possible with the guidance and help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this research. First and foremost, to the Almighty God, for the strength and good health to have this research done. Second, to his family, Anelyn and Kyoshi the author inspiration, for providing love and moral support, advices and encouragement to complete this task.

The Developer would like also to thank Southern Philippines Agri-Business and Marine and Aquatic School of Technology, Institute of Computing, Engineering and Technology, Information Technology Department whom the developer is working extends his thanks and great appreciation for allowing him conduct this project. The Researcher is also thankful to Technological Institute of the Philippines, his **Alma-Mater** on this Doctorate Degree for guiding him throughout the research duration. To University of Mindanao, College of Computing, Matina Campus, whom the researcher spends studying extends his thanks and great appreciation in the conduct of this research. The Developer is very thankful to his colleagues for helping him get through difficult times and for all the emotional support, camaraderie, entertainment and care they provided. To all of you who have been part of this project, THANK YOU VERY MUCH!

REFERENCES

[1] Kahina CHELLI "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures "Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.

[2] Kiran Maraiya, Kamal Kant, Nitin Gupta "Wireless Sensor Network: A Review on Data Aggregation "International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011 .1 .ISSN 2229-5518

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

[3] An Liu,1 Mihui Kim,2 Leonardo B. Oliveira,3 and Hailun Tan4 "Editorial: Wireless Sensor Network Security "Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume2013,ArticleID362385,1page http://dx.doi.org/10.1155/2013/362385
[4] Shio Kumar Singh 1, M P Singh 2, and D K Singh 3 "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks "International Journal of Computer Trends and Technology- May to June Issue 2011
[5] Samer A. B. Awwad, Chee K. Ng, Nor K. Noordin, and Mohd. Fadlee A. Rasid "Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network "International Journal of Computer Trends and Technology- May to June Issue 2011
[6] Waltenegus Dargie and Christian Poellabauer "Fundamental of Wireless Sensor Networks, Theory and Practice "This Edition First Publish 2010
[7] Donghyun Kim∗, Baraki H. Abay∗, R.N. Uma∗, Weili Wu†, Wei Wang‡, and Alade O. Tokuta "Minimizing Data Collection Latency in Wireless Sensor Network with Multiple Mobile Elements "2012 Proceedings IEEE INFOCOM
[8] Olivier Dousse, Petteri Mannersalo, Patrick Thiran, "Latency of Wireless Sensor Networks with Uncoordinated Power Saving Mechanisms" Mobile Elements "1202, 02044 VTT Finland
[9] Shouwen Lai, Member, IEEE, and Binoy Ravindran, Senior Member, IEEE, "Least-Latency Routing over Time-Dependent Wireless Sensor Networks" The preliminary result was presented at IEEE INFOCOM 2011
[10] Gang Lu and Bhaskar Krishnamachari,Department of Electrical Engineering University of Southern California, Los Angeles, CA 90089,ganglu, bkrishna @usc.edu "Minimum Latency Joint Scheduling and Routing in Wireless Sensor Networks" IEEE WSNA 2002
[11] Ryo Sugihara and RajeshK.Gupta, Computer Science and Engineering Department, University of California, San Diego ryo, rgupta@ucsd.edu "Improving the Data Delivery Latency in Sensor Networks with Controlled Mobility"
[12] Yang Yu, Bhaskar Krishnamachari, and Viktor K. Prasanna Department of Electrical Egineering University of Southern California "Energy-Latency Tradeoffs for Data Gathering in Wireless Sensor Networks" 00 (C) 2004 IEEE INFOCOM 2004
[13] ADRIAN PERRIG, JOHN STANKOVIC, and DAVID WAGNER "SECURITY IN WIRELESS SENSOR NETWORKS" COMMUNICATIONS OF THE ACM June 2004/Vol. 47, No. 6
[14] Al-Sakib Khan Pathan Department of Computer Engg. Kyung Hee University, Korea spathan@networking.khu.ac.kr Hyung-Woo Lee Department of Software Hanshin University, Korea hwlee@hs.ac.kr Choong Seon Hong Department of Computer Engg "Security in Wireless Sensor Networks: Issues and Challenges" Feb. 20-22, 2006 ICACT 2006
[15] Hemanta Kumar Kalita1 and Avijit Kar2 "WIRELESS SENSOR NETWORK ECURITY ANALYSIS International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009
[16] NICHOLAS HOPPER, EUGENE Y. VASSERMAN, and ERIC CHAN-TIN University of Minnesota "How Much Anonymity does Network Latency Leak" ACM Trans. Info. Syst. Sec. 13, 2, Article 13 (February 2010), 28 pages
[17] Antonio G. Ruzzelli, Richard Tynan and G.M.P. O'Hare, Department of Computer Science University College Dublin Belfield, Dublin 4 Ireland "A Low-Latency Routing Protocol for Wireless Sensor Networks"
[18] Paolo Santi, "On the Data Gathering Capacity and Latency in Wireless Sensor Networks" Member, IEEE, IIT-CNR Pisa, ITALY.
[19] D. W. Carman* and B. J. Matt Network Associates Laboratories Rockville, "ENERGY-EFFICIENT AND LOW-LATENCY KEY MANAGEMENT FOR SENSOR NETWORKS" September 30, 2000
[20] ELAINE SHI AND ADRIAN PERRIG, CARNEGIE MELLON UNIVERSITY, "DESIGNING SECURE SENSOR NETWORKS" IEEE Wireless Communications • December 200438
[21] Yenumula B Reddy, Grambling State University, "Security Issues on Wireless Sensor Network" SENSOCOMM 2011.
[22] T.Kavitha1, D.Sridharan2, "Security Vulnerabilities In Wireless Sensor Networks: A Survey" Received June 23, 2009.

BIOGRAPHIES

Felomino P. Alba is currently pursuing his degree in Doctor in Information Technology at Technological Institute of the Philippines, received his Master Degree in Information Management at University of Southern Mindanao, Phlippines. His degree at Central Mindanao Computer School. His research interest are Computer Network, Information Security, Data Mining.

Dr. Enrique Festijo is a Professor at Technological Institute of the Philippines, took his Doctorate degree at Notre Dame University Korea. His involved researches are in the field of Information Security, Computer Networks, and Emphatic Computing.