Assessment of the Causes and Effects of Packet Loss in Wireless Sensor Networks

Dr. Anthony Luvanda
1. School of Science, Department of Physics and Computer Science, Alupe University College,
P. O Box 854-50400 Busia Kenya

Abstract

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.[1] Like any other wireless network, loss of packets is a common occurrence in WSNs. This may be caused by a variety of events and occurrences on the network which may in the long run affect the performance of the network. This paper therefore studied the connection between the causes of packet loss in wireless sensor networks and their net effect on the outcome and performance of the said WSN in the monitoring of physical and environmental conditions.Primarily the paper relied on secondary data and review of past literature and research and in the process was able to observe that weak signals and malicious attacks such as the black hole attack, selective forwarding attack and radio interferences are the major causes of packet loss whose effects include reduced network life and throughput; higher consumption of energy; denial of service attacks; reduced network efficiency; packet degradation and inconsistent packets.

Keywords: Packet loss, Wireless sensor networks, malicious attacks, Received Signal strength

1. INTRODUCTION

Wireless sensor network (WSN) can be defined as a cable less network consisting of spatially distributed autonomous devices using sensors to monitor physical and environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.[2]

The ability to integrate wireless, sensor and computing technology has made WSN to be highly popular in recent years. WSN consists of a number of nodes that are equipped with processing, communicating and sensing capabilities, which enables them to use ad hoc radio protocols to forward data in multi hop mode of operation. Additionally the ability to be able to measure physical parameters has made WSN to be the most suitable technology for monitoring and reporting important quantifiable measures. Application areas include health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include: Environmental monitoring of air, water, and soil; Structural monitoring for buildings and bridges; Industrial machine monitoring; Process monitoring; Asset tracking.

One should bear in mind however that if one deploys any application that may embark on sensing humidity, sound, pressure, temperatures and the likes may use sensor networks and in that respect then it is right to make the assumption that WSN are not just limited to environmental sensing.

Zhao and Govindan define packet loss as the fraction of packets not successfully received (i.e., passed Cyclic Redundancy Check (CRC)) within some time window, where the time window will be clear from the contexts[13].

The loss of packets in WSN does occur mainly due to attacks affecting the nodes or wireless links connecting the nodes. However in order to swiftly react to such a loss, it is paramount that one determines the actual cause of the loss and the rate at which it does or may occur.

This paper assesses the link between the causes of packet loss in wireless sensor networks and their net effect on the outcome and performance of the said WSN in the monitoring of physical and environmental conditions.

1.1 RELATED WORK

In an attempt to reduce packet loss via WSN, Mizero et al. proposes a combined approach of Modified Distributed Storage Algorithm for wireless sensor networks (MDSA) coupled with Replacing Lost Packets (Packet Loss Concealment) methods. During this study, a Distributed Slot synchronization (DSS) was designed with both repetition code and regeneration code in case there is a link failure. Results from this study showed that for both codes the success probability of both theory and implementation correlate, while the regeneration code showed the highest success probability. And therefore it was chosen for further study. The implementation of regeneration code results showed that the increasing of field size also correlate with the increasing of success probability for both theory and implementation. The implementation of the proposed PLC results showed that showed that the proposed PLC algorithm improves significantly the quality of speech transmitted over an unreliable network with high packet loss rate. Though, the proposed PLC introduces additional delay which needs to be considered but the increased delay is often a necessary expense if the signal quality is a priority.[4]

woo et al. evaluates packet delivery performance by examining the packet loss between a pair of nodes with the purpose of constructing a packet loss evaluation link quality.[5] Ganesan et al. on the other hand performed a large scale study whose main focus was to determine the loss and asymmetry of packet delivery at the link and Mac[6]

From a security point of view, packet loss (irrespective of the technology being implemented) needs to be considered as a security threat. Unfortunately current intrusion detection systems may only be able to detect packet loss without really without really addressing either the cause or impact of the loss. This paper addresses the aforementioned anomaly.

2. METHODS AND MATERIALS

This paper first attempts to understand the general performance of wireless networks in a wide variety of environments with specific attention being paid to Wireless Sensor Networks. Primarily the paper relies on secondary data and review of past literature and research by mainly looking at but not confining itself to the following works:

a. Reviewing extensively the works of Jerry Zhao and Ramesh Giovindan where they report on a systematic medium scale measurement of packet delivery in three different environments: an indoor office building, a habitat with moderate foliage and an open parking lot. Their findings provided and insight into how to design and evaluate routing and medium-access protocols for sensor networks.

b. Bilal Shebaro et al. proposed and built a fine-grain analysis tool (FGA) that investigates the causes of packet loss and reports the most likely cause of those losses. The tool employed ensures the presence in every received packet of parameters such as Received Signal Strength Indicator (RSSI) and Liquid Quality Indicator (LQI)to profile the links between nodes and corresponding neighborhoods. This enables the tool to be able to differentiate between the various attacks that may affect the nodes and the links.[7]

c. Mihail Cernainu and Aurel Gontean analyze the importance of packet loss consideration (PLC) within the internodes communication of a WSN. They evaluate the link quality between network nodes based on the link packet loss and not on the Received Signal Strength Indicator. The reason for this is so that they are able to portray the impact of the loss of packets on a known routing protocol for WSNs such as Low Level Adaptive Clustering Hierarchy LEACH.[8]

d. Adbellah Chehri, Gwanggil Jeon and Byoingjo Choi conducted research in link quality measurements and reporting in wireless sensor networks where they discuss the deploying of a testbed as a first step towards creating a fully functional heterogeneous wireless network-based underground monitoring system. They deployed mobile and static ZigBee nodes on underground mine galleries for the purposes of measuring ambient temperature. They then described the measured link characteristics such as received signals strength, latency and throughput for different scenarios. [9]

3. FINDINGS

3.1 CAUSES AND EFFECTS OF PACKET LOSS IN WSNs

Overall Packet loss occurs when one or more packets data travelling across a network ad hoc or otherwise fails to reach their destination and is measured as a percentage of packets lost with respect to packets sent.[10] A major cause of packet loss in wireless networks is network congestion. When content arrives for a sustained period at a given router or network segment at a rate greater than it is possible to send through, then there is no other option than to drop packets. A number of other factors such as corrupt or lose packets in transit, faulty networking hardware, or faulty network drivers can also lead to packet loss.[11] However a closer look at packet transmission in WSNs also reveals the following causes of packet loss in WSNs.

3.1.1 SIGNAL STREGNTH

According to Zhao et al, in the harshest environment some nodes will relieve up to 90% succession rates while their neighbors receive less than 50% reception rate this is due to the fact that stronger to the transmitter the direct signal is strong enough and the scattered attenuation insignificant to a level that reception rates are

consistently high. Further away from the transmitter the direct signal is weaker which drops the reception rate and this in turn leads to loss of packets.
effectively this leads to reduces network lifetime, reduces network throughput and the loss of packets ultimately leads a waste of energy consumed by the entire network.

3.1.2 MALICIOUS ATTACKS

As earlier indicated, packet loss can and should be considered as security threat, that said however it is unfortunate that majority of the existing intrusion detection systems are typically only able to detect packet loss and are thus unable to determine the cause of the losses, whether it is node or link related. The existence of interference whether malicious or not can affect the relative Received Signal Strength otherwise known as RSSI and the Link Quality Indicator (LQI) values of received packets that passed through a noisy environment, and can sometimes impair the signal quality of other packets. Attackers in most cases will attempt to use numerous ways to try and conceal the attacks by making them look like normal unintentional interference.

3.1.2.1 Black hole attack

Hackers will in such cases compromise a node and ensure that the compromised node drops all **packets** that are forwarded through it. Such an attack can either be classified under outing attacks and/or a data traffic attack.

Black hole attacks lead to a denial of service attack which prevents the WSN nodes from maintaining and transmitting physical and environmental conditions for a while and/or permanently, which might lead to a slight inconvenience to the users of such networks at a lower scale or on the extreme it may lead to devastating effects on people’s lives.

3.1.2.2 Selective forwarding attacks

Based on the intentions of the hacker and by extension the malicious instructions, a malicious node may simply refrain from forwarding certain messages thus ensuring that they are not propagated any further.

Through the selective dropping of packets from a particular node or a group of nodes, a denial of service attack is perpetrated which again prevents the WSN nodes from maintaining and transmitting physical and environmental conditions. Furthermore, the dropping of packets translates in low or lack of efficient exchange of packets amongst nodes which affects the overall network efficiency.

3.1.2.3 Radio interference

whether intentional or not, radio interference is considered a major threat to sensor network services. This is basically the addition of unwanted signals to the useful signal which modifies or disrupts the signal as it travels along a channel from sending to receiving node. [12]

Interference leads to network degrading, resulting in packet degrading and inconsistent packet behavior.

4. DISCUSSION

Despite the fact that packet loss on a WSN may be perpetrated by a malicious attacker, it is also worth noting that the same can be attributed to multi-hop routing paths in wireless sensor networks, nodes near the destination having higher packet delivery performance, signal attenuation due to the distance between the nodes, asymmetry in wireless communication links, non-uniform radio signal strength, wireless propagation effects (fading and multipath), interference due to hidden terminal problem, in addition to being greatly affected by the deployment environment, and the behavior of wireless communication can also cause packet loss.

If reduced network life and throughput; higher consumption of energy; denial of service attacks; reduced network efficiency; packet degradation and inconsistent packets is of major concern when deploying a Wireless Sensor Network then it is equally important that during the setting up of the network, the causes that lead to this are carefully assessed and circumvented before deployment.

5. REFERENCES

[1] Anna Hac, (2003)*Wireless Sensor Network Designs,*John Wiley and Sons

[2] A Cerpa, J. Elson, D.Estrin, l.Girod, M. Hamilton, and J. Zhao. Habitat monitoring: application Driver For wireless Communication Technology. *In proceedings* of the ACM SIGCOMM *Workshop on data Communications in Latin America and the Caribbean, San Jose,* Costa Rica, April 2001. ACM.

[3] SenSys’03, November 5-7, 2003, Los Angeles, Carlifornia USA.

[4] Mizero Adrien, Cheruiyot Kipruto W., Ann Kibe, *Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol.4, No.5, 2014*

[5] A. Woo and D. Culler, “Evaluation of Efficient Link Reliability Estimators for Low-Power Wireless Networks”, Technical Report number UCB/CSD-03-1270, University of California, Berkeley, April 2003

[6] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker, “Complex Behavior at Scale: An Experimental Study of Low-Power Wireless Sensor Networks”, In Technical Report UCLA/CSDTR 02-0013, Computer Science Department, UCLA, July 2002

[7] Shebaro, Bilal; Midi, Daniele; and Bertino Elisa, “Fine-grain analysis of Packet loss in Wireless Sensor

Networks" (2014). Cyber Center Publications. Paper 646

[8] https://www.reserachgate.net/publication/260863298

[9] https://www.ncbi.nlm.gov/pubmed/23459389

[10] Kurose, J.F. & Ross, K.W. (2010). *Computer Networking: A Top-Down Approach*. New York

[11] A. Cerpro, J. Elson, D Estrin, L.Girod, M.Hamilton and J. Zhao. Habitat monitoring: Applicxation driver For Wireless Communication Technology. In *proceedings of the ACM SIGCOMM workshop on Data Communications in latin America and the Caribbean,* San Jose, Costa Rica, April 2001. ACM

[12] Charles L. Hutchingson, Michael B. Kaczynski; 4th ed. Newington, CT American Radio Relay League c1987