International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
Volume 31, Issue 04, Quarter 04 (2019)
Publishing Month and Date: Oct 24, 2019
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (Online): 2347-601X
www.ijemhs.com

Review on Wireless Sensor Network Issues Related to Broken Link Problem

Pardeep Dalal[1] and Rekha[2]

[1]M.Tech student, Department of Computer Science,
CBS Group of Institutions, Fatehpuri, Jhajjar
[2]Assistant Professor, Department of Computer Science & Engineering
CBS Group of Institutions, Fatehpuri, Jhajjar

Abstract

When links consists of new weights in a network at the time of using router could create duplicities through performing more computations & unnecessary corrections by repeating operation for every node regardless of location of link weight change. So it could cause network instability because overall routing table is frequently updated. A multi-path routing system is presented & it uses multi-path information to create shortest path tree when some links have new weights. So high speed routing is considered more significant in Open Shortest Path First that is frequently used intra-autonomous system routing protocol. Whenever a topological gets modified due to unexpected reason in Open Shortest Path First, network routing algorithms have been used in order to update routing table.

Keyword: *System, Shortest, unnecessary, node regardless, routing.*

1. Introduction

Wireless communications has been achieving consideration from 1990 & it is considered as base of wireless sensor network. Wireless sensor network consist of lot of constraints like limited power energy, small storage capacity, slow processing power. Many sensors like humidity, accelerator, & light could be used in this network to detect environmental conditions. Today demand for network applications has grown quickly. So high speed routing is considered more significant in Open Shortest Path First that is frequently used intra-autonomous system routing protocol. Whenever a topological gets modified due to unexpected reason in Open Shortest Path First, network routing algorithms have been used in order to update routing table. For example, if there is a failure of link in a network then shortest paths must be recomputed. Here smallest paths calculation is done using router. When links consists of new weights in a network at the time of using router could create duplicities through performing more computations & unnecessary corrections by repeating operation for every node regardless of location of link weight change. So it could cause network instability because overall routing table is frequently updated. A multi-path routing system is presented & it uses multi-path information to create shortest path tree when some links have new weights.

Sensor Networks: A sensor network is a consisted of communicating sensing devices, or nodes. Al nodes are not necessarily communicating at any particular time, and nodes can only communicate with a few nearby nodes.

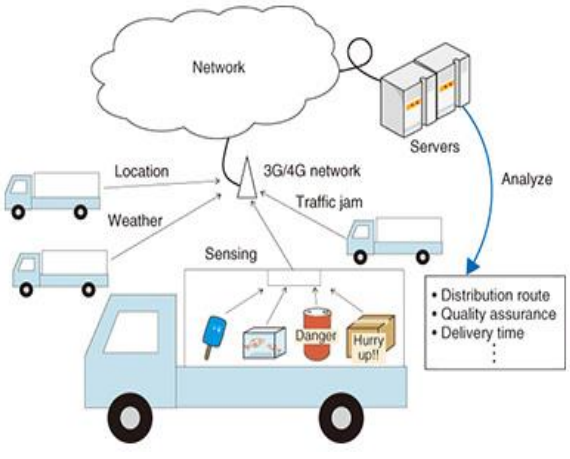

Figure: 1 Sensor Networks

Wireless Sensor: Node architecture Wireless sensor node is made up four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. There can be application dependent additional components such as a location finding system, a power generator and a mobilizer.

2. Literature Review

P. Natesan (2012) Multi Stage Filter Using Enhanced Ad boost for Network Intrusion
Based on the analysis and distribution of network attacks in KDDCup99 dataset and real time traffic, this paper proposes a design of multi stage filter which is an efficient and effective approach in dealing with various categories of attacks in networks.

By Parul Chhikara (2013) Enhancing Network Security using Ant Colony Optimization Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 4 Version 1.0 Year 2013
Security of the information in the computer networks has been one of the most important research areas. To preserve the secure condition it is essential to be aware of the behavior of the incoming data. Network Security is becoming an important issue for all the organizations, and with the increase in knowledge of hackers and intruders they have made many successful attempts to bring down high-profile company networks and web service

Sonu (2016) et al, International Journal of Computer Science and Mobile Computing
A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages.

Udaya Wijesinghe (2015) An Enhanced Model for Network Flow Based Botnet Detection Information and Networked Systems Security
The botnet is a group of hijacked computers, which are employed under command and control mechanism administered by a botmaster. Botnet evolved from IRC based centralized botnet to employing common protocols such as HTTP with decentralized architectures and then peer-to-peer designs. As Botnets have become more sophisticated, the need for advanced techniques and research against botnets has grown. In this paper, we propose techniques to detect botnets by analyzing network traffic flows.

3. Tools & Technology

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server. After initial contact, either the client or the server is capable of sending and receiving data.

4. Overview of IP4 Addresses

IP4 addresses are 32 bits long. They are expressed commonly in what is known as dotted decimal notation. Each of the four bytes which makes up the 32 address are expressed as an integer value (0 – 255) and separated by a dot. For example, 138.23.44.2 is an example of an IP4 address in dotted decimal notation. There are conversion functions which convert a 32 bit address into a dotted decimal string and vice versa. Often times though the IP address is represented by a domain name, for example, hill.ucr.edu. Several functions described later will allow you to convert from one form to another (Magic provided by DNS!).The importance of IP addresses follows from the fact that each host on the Internet has a unique IP address.

Table 1: Port

Port	Service Name, Alias	Description
1	Tcpmux	TCP port service multiplexer
7	Echo	Echo server

9	Discard	Like/dev/nu11
13	Daytime	Systems date/time
20	ftp-data	FTP data port
21	ftp	Main FTP connection
23	telnet	Telnet connection
25	SMTP, mail	UNIX mail
37	Time, timeserver	TIME server
42	Name server	Time server
70	Gopher	Text/menu information
79	Finger	Current users
80	www, http	Web server

5. Scope of Research

This research aims at the enhancement of reliability of wireless network. This research is useful in cases where data is transmitted at distance location. Such networks usually face the problem of broken link. If the connection is broken then data transmission is interrupted. Due to unexpected interruption the transmission of data gets stop and need to be retransmitted in case of re connectivity. This leads to the wastage of time and network usage. So this research is quite useful for such circumstances.

References

[1] Fei Hu Secure (2017) Wireless Sensor Networks: Problems and Solutions Electrical & Computer Engineering Department, Clarkson University

[2] By Parul Chhikara (2013) Enhancing Network Security using Ant Colony Optimization Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 4 Version 1.0 Year 2013

[3] Kuldeep Tomar (2014) Enhancing Network Security and Performance Using Optimized Acls International Journal In Foundations Of Computer Science & Technology (Ijfcst), Vol.4, No.6, November 2014

[4] Sonu (2016) et al, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.5, May- 2016, pg. 808-813

[5] Udaya Wijesinghe (2015) An Enhanced Model for Network Flow Based Botnet Detection Information and Networked Systems Security Research, Department of Computing, Faculty of Science, Macquarie University, Sydney, Australia Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), Sydney, Australia, 27 - 30 January 2015

[6] Udaya Wijesinghe (2015) An Enhanced Model for Network Flow Based Botnet Detection Information and Networked Systems Security Research, Department of Computing, Faculty of Science, Macquarie University, Sydney, Australia Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), Sydney, Australia, 27 - 30 January 2015

[7] Mikko Kulmala (2016) Improving Network Security With Software-Defined Networking Tampere University Of Technology Master Of Science Thesis, 48 Pages, 3 Appendix Pages April 2016

[8] Syed Taha Ali (2016) A Survey of Securing Networks using Software Defined Networking.