R.Vijayakumar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 9-12 **ISSN: 2321-8363**

PACKET LOSS MAINTENANCE USING PUZZLE-LOGIC ALGORITHM IN WIRELESS SENSOR NETWORKS

R.Vijayakumar[1], G.Rajasekar[2], E.K.Deepanchakkaravarthi[3]

[1]Department of CSE, Muthayammal Engineering College, Namakkal,
r.vijay155@gmail.com

[2]Department of CSE, Muthayammal Engineering College, Namakkal,
rajasekarmeccse2014@gmail.com

[3]Department of CSE, Muthayammal College of Engineering, Namakkal,
dchakkaravarthi1@gmail.com

Abstract

In recent electronic and wireless communications are enables the development of low-cost sensor networks. Wireless sensor networks have been used in a variety of application areas such as, home, environment and some other commercial purposes. But every application contains particular technological issues. One of the main key issues is packet loss in data communication. So we want to propose a new algorithm called puzzle-logic in sensor network platform.

Keywords: Wireless Sensor Networks (WNS); Packet Dropping; Puzzle-logic.

1. Introduction

Wireless sensor networks are an innovative technology for engineers and researchers to examine physical phenomena and respond to it. In recent times, wireless sensor networks are come into importance because they hold the potential to modernize many segments of our financial system and life, from environmental monitoring and maintenance to develop and business asset management, to automation in the transportation and health-care industries [1]. The design, performance, implementation and function of a sensor network requires the confluence of many disciplines, including signal processing, networking and protocols, information management, embedded systems, and distributed algorithms.

Such networks are frequently deployed in resource-controlled environments, for instance with battery operated nodes. These controls says that sensor network problems are best approached in a holistic manner, by together considering the physical layer, networking layer, and application layer and making major design trade-offs across the layers.

Some of the commercial applications are monitoring material weakness, managing inventory, building virtual keyboards, robot control, constructing smart office spaces, monitoring product quality, environmental control in office buildings, local control of actuators, guidance in automatic manufacturing environments, interactive toys, interactive museums, monitoring and detecting car thefts [2].

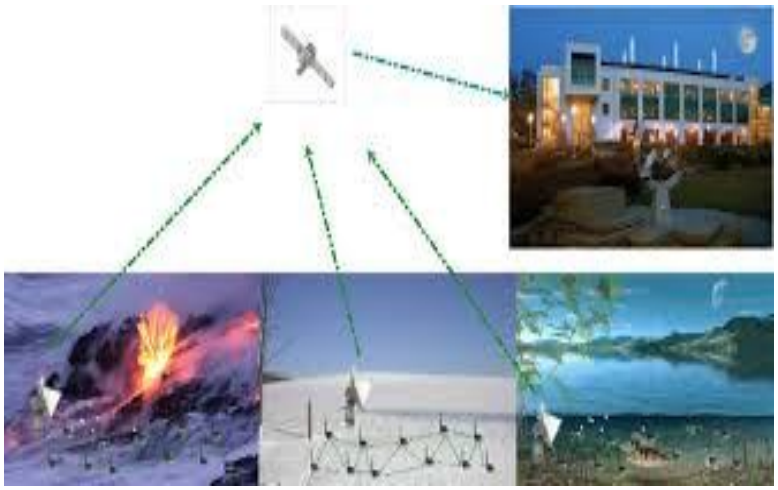

Figure 1: Wireless Sensor Network

This sensor networks can provide wide range of applications,

- Military applications
- Environmental applications
- Health applications
- Home applications
- Other commercial applications

The below section of the paper is prepared as follows. In Section II shows the problem statement of this paper. In Section III explains the overview of proposed system and puzzle-logic algorithm in detail. Finally, the conclusion and future work of the proposed system is presented in Section IV.

2. Problem Statement

The existing approach for detecting packet dropping attacks requires, the destination is send information about how many packets the source will send to it next. The initial packet is contains count number i.e., the count of packets to be transmitted including sequence numbers in packets.

It's first find out one shortest route using routing protocol [3] and then sends all packets through that selected route. If packet is received by destination node, the destination is sending back the acknowledgement to the appropriate sender. A source that does not receive a reply from its destination be able to guess that packets are being dropped by an attacker. Sometimes the packets are being dropped due to collisions, congestion, buffer overflow etc. The basic idea is works as follows. An intermediate node that forwards a packet to the next node on the path but does not receive a reply within a timeout period guesses that its neighbor is dropping packets. Then it informs the source about misbehavior of the neighbor. The source node finally chooses another route to reach the destination node. The attacker can drop all the packets including the initial packet. So it will not help to source node to find out the particular dropping packet.

3. Proposed System

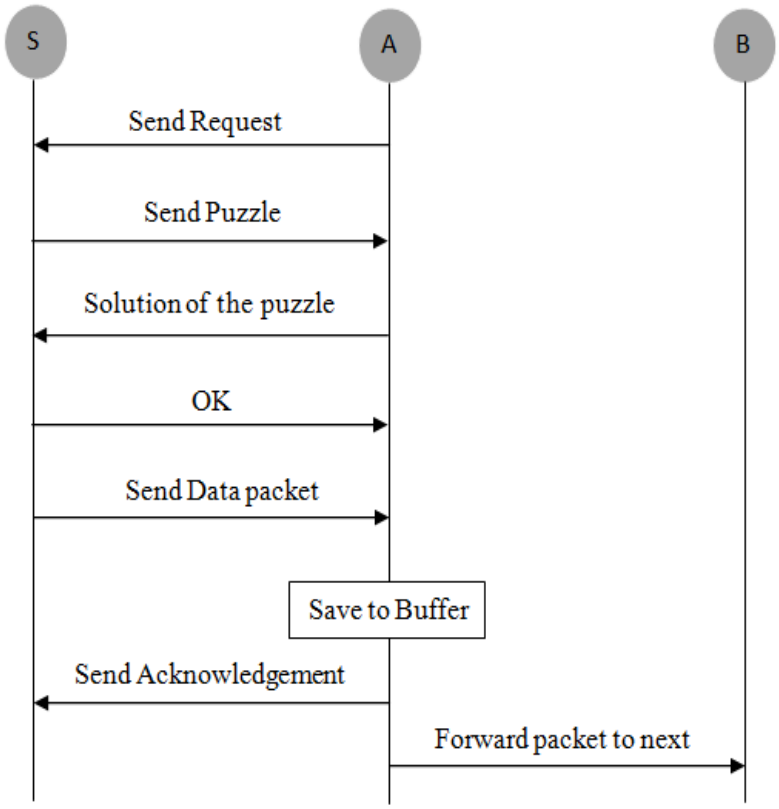

Figure 2: Puzzle-logic workflow diagram

The sender can send all data packets to destination in appropriate route DSR [4] routing request. The intermediate node that receives the packets and stores in own buffer and forwards a packet to the next node along the path from source to destination. If any one of the intermediate node in wireless network may be controlled by attackers. The attacker can send the dummy packets to that node and full the buffer. So the attacking intermediate node can receive the packet means that packets will be dropped.

A new algorithm is proposed for prevents dropping data packets from attackers named as puzzle-logic algorithm. This algorithm works and that creates new puzzles randomly when new node is registered in that network. The data will send to neighbor node means it first sends the puzzle question [5]. It send the correct solution means then only the packet will be send from previous node. The neighbor node cannot send the solution within a timeout period that neighbor is reported as attacker. The puzzle-logic workflow diagram is shown in figure 2.

4. Conclusion and Future work

The Wireless sensor networks are used for a wide range of application. In this paper we demonstrate that the performances of the wireless sensor networks are increased by preventing packet loss and delays. The buffer can be maintained and controlled by user so the intermediate nodes cannot easily controlled by attackers using efficient puzzle-logic algorithm.

This algorithm is works only in bi-directional communication process. So this approach is not suitable for unidirectional communication because there are no replies from neighbor nodes. In future work we plan to research new technique to solve this problem in unidirectional communication.

References

[1]Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, March 2013, EAACK – A Secure Intrusion Detection System for MANETs, *IEEE Transactions on Industrial Electronics*, Vol. 60, No. 3, pp.1089-1098

[2]Davidpallassini, 2005, Packet Loss Performance and MAC Design for Estimation in Wireless Sensor Networks, *Master's Degree Project Stockholm, Sweden*, pp.1-87

[3]Shio Kumar Singh, M P Singh, and D K Singh, November 2010, Routing Protocols in Wireless Sensor Networks – A Survey, *International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2*

[4]D. Johnson and D. Maltz, 1996, Dynamic Source Routing in *ad hoc* wireless networks, *in Mobile Computing. Norwell, MA: Kluwer*, ch.5, pp. 153–181

[5]S.Kannadhasan, N.SivaKumar, V.B Bhapith and R.Ragavendra, August 2013, Data Aggregation Using Transmitted Power Fuzzy Logic Techniques in Wireless Sensor Networks, *International Journal Of Advanced Research In Electrical, Electronics And Instrumentation Engineering*, Vol. 2, Issue 8

A Brief Author Biography

R.Vijayakumar – received the B.E. degree in Computer Science Engineering from Chennai University, in 2012. Now I am studying ME – Computer Science in Muthayammal Engineering College, Rasipuram. And I am Microsoft Certified Professional (MCP) Member from 2011. (For more details: vairavi.webnode.com)

G.Rajasekar – received the B.E. degree in computer science engineering from Coimbatore university. Currently studying ME Computer Science in Muthayammal Engineering College, Rasipuram.

E.K.Deepanchakkaravarthi – Studied B.E. Computer Science under Coimbature university. Presently studying ME Computer Science in Muthayammal College of Engineering, Rasipuram.

