ENHANCED DATA STREAM FOR SECURE AND COLLISION ATTACKS FREE TRANSACTION USING MULTIPLE PATHS

Ms J. Jerusha, Assistant Professor, Department of Mathematics,
KG College of Arts and Science, Coimbatore-35

Abstract

Graphs are classified according to their complexity, the number of edges allowed between any two vertices, and whether or not directions (for example, up or down) are assigned to edges. Various sets of rules result in specific properties that can be stated as theorems. In our research we are going to explain about basic networks, graph of networking and architectural logics. In distinct usage in distributed computing, the term network architecture often describes the structure and classification of distributed application architecture, as the participating nodes in a distributed application are often referred to as a network. A customized system to detect, monitor and block the data packets according to the definitions submitted to the Graph mechanism. The mechanism is robust easy to implement, maintain, update and enhance for further enhancements. The mechanism takes input as sample data packets which are to be blocked and checks those definitions with the data packets according to the protocols, network structure and algorithms which are a part of the mechanism.

1. INTRODUCTION

Graph theory is about the relationship between edges and nodes. A graph consists of points called vertices and lines called edges between them. No attention is paid to the position of points and the length of the lines. Usually in engineering and science, we obtain experimental number of corresponding values for two variables x and y. It will be necessary to find a mathematical relation between them. For the purpose, we first plot the corresponding values (xi, yi) (i = 1, 2 ... n) of the given data as rectangular coordinates in graph paper. A smooth curve can be drawn to pass through near the plotted points. Such a curve is called an approximating curve. The equation this curve may be taken as an approximate relation between x and y and it is called an empirical equation.

A network has been defined as any set of interlinking lines resembling a net, *a network of roads*, an interconnected system, *a network of alliances*. A computer network is simply a system of interconnected computers. The data streams being transmitted on a network as data or as result of operation of an application over the network are required to be monitored and in adverse circumstances blocked. The network nodes can interrupt the communication path at the application layer and force the data packets to identify themselves. Alternatively, the nodes can try to extract the information by analyzing the application layer part of the communication data. Both methods have drawbacks:

- The active or passive gathering of user information is not always possible.
- The passive information retrieval is costly and may result in a reduction of performance.

Additionally it involves a considerable implementation effort.

2.1 Necessitate of wing

Due to limited computations of power and energy resources, aggregating with data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However this aggregation is known to be highly compactable to node compressing mising attacks. Since, WSN are usually unattended and without temper resistant hardware, they are highly predictable to such attacks. Thus, ascertaining reliability of data and reputation of sensor nodes is crucial for WSN.

To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, for more accurate and faster converging. But reputations will make overload in receiver part. Receiver will maintain queue for receive packets simultaneously, this will occupy large amount of space and increase queue in the time of slow process. Increasing of monitoring path and network traffic, transaction will be collusion robust in both of sides (Sender and Receiver) **(Fig[1])**.

2.2 Problem of wireless sensor nodes

The primary goal for our interaction mechanism must be a high accuracy in the selection of nodes. The occurrence of both false positives (i.e., selecting nodes that the user did not intend to interact with) and false negative (i.e., ignoring nodes chosen by the user) should be avoided. Closely related to that is our second goal, a good usability of the system. It must be simple and intuitive to use – despite the limitations of the sensor nodes involved in the interaction. Finally, we also need to take the resource limitations of the wireless sensor nodes into account. For that reason, we need to limit the complexity of the operations performed on the individual nodes. Moreover, we cannot require additional hardware like a display on the sensor nodes just for facilitating the interaction.

As for all solutions discussed in this thesis, the main target scenario for our interaction approaches are indoor deployments of wireless sensor networks as part of pervasive computing scenarios **(Fig[2]).**

2.3 Techniques used at present

Iterative Filtering algorithms are an ease available option for WSNs (Wireless Sensor Networks) because they solve both problems data aggregation and data trustworthiness assessment using a single iterative procedure.

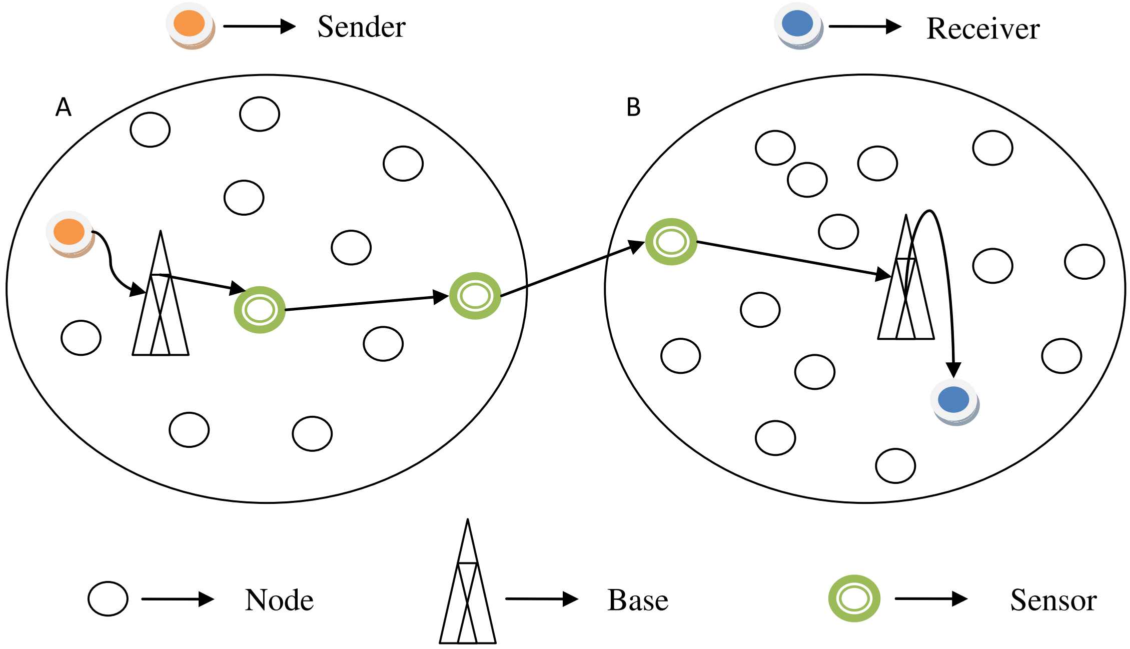
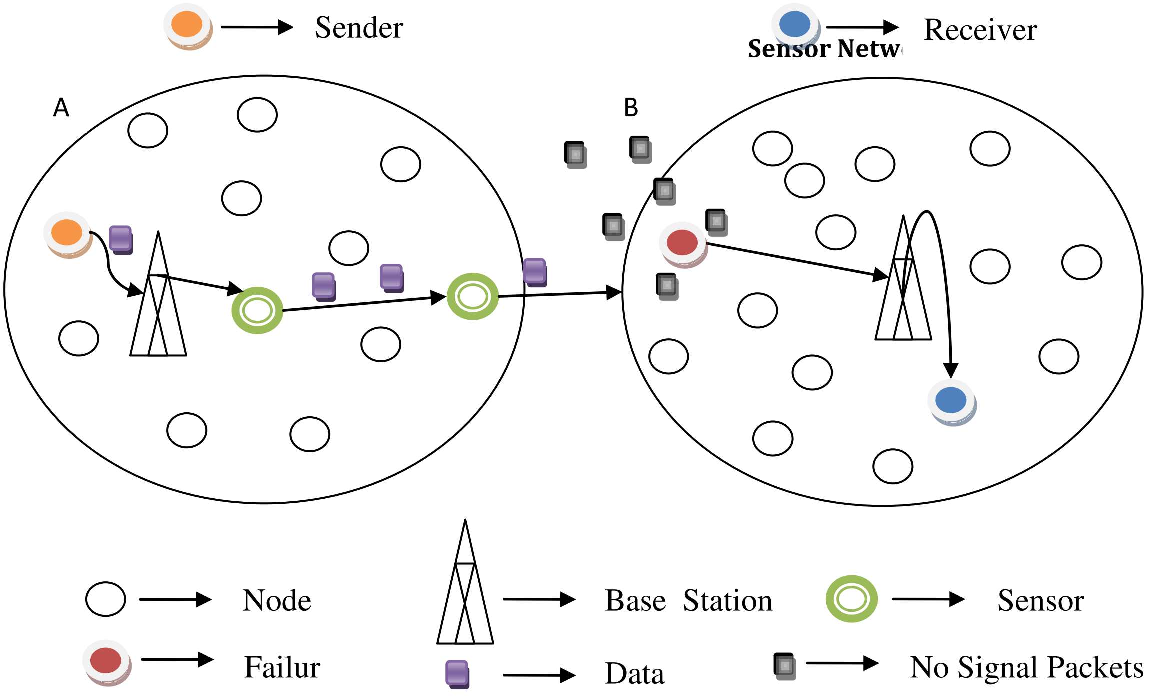


Fig1: Network Model for WSN (A&B-Network Area)

Such relativity of calculating each sensor is depended on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of generating of the readings of all sensors.

Usually, there are two ways of selecting a sensor node for an interaction, either using its node identifier or with the help of geographic position information. If the client device knows the node identifier of the target node, then initiation an interaction with this node is trivial: the client device can directly start sending uncast messages to this node.

Fig2: Failure/Interrupt/Damage in Sensor Network



If the sensor nodes are aware of their respective geographic positions and the client device knows the points of the target node, then it can use this information to start the interaction. This can either be done by comparing the coordinate information of the candidate nodes with the specified geographic coordinate of the target node and determining its node identifier this way or by directly communicating with the target node using geographic routing. However, in effort to the problems of node localization in sensor networks, it is also very complex for the user to determine the exact geographical position of the target node he wants to interact with.

An Algorithm and technique was used for forming Network security, Time consuming, avoiding data packet losses, finding some of shortest paths, monitoring network traffics using sensor, finding failure sensor nodes, selecting alternative path apart from sensor nodes.

i. Finding Last N number of Shortest paths – virtual selection of nodes algorithm

ii. Dribble Check Algorithm

2.4Problem finding, description and solution-Virtual selection of nodes Algorithm

2.4.1 Selecting shortest paths

A network is usually represented as a weighted digraph, $G = (N, E)$, where $N = \{1 \ldots n\}$ denotes the set of nodes and $E = \{e_1 \ldots e_m\}$,

denotes the set of communication links connecting

the nodes. Let $M = \{n_0, u_1, u_2 \ldots u_m\} \subseteq\subseteq N$ be a set of form source to destination nodes, where n_0 is source node and $U = \{u_1, u_2 \ldots u_m\}$ denotes a set of destination nodes. $P(n_0, u_i)$ is a path from source node n_0 to destination node u_i € U.

The path P is the shortest path if the bandwidth of that path is equal to constant value B (this value is determined from the user or is a required value of the bandwidth). The Hence, the problem of bandwidth constrained k shortest path is to find all the paths from source node to each destination node which satisfy:

Band **(P) ⩾B**

2.4.2 Selecting N number of shortest paths

Selecting number of shortest paths, between two network areas or between sender and receiver.

Shortest path → *Band* (P) ⩾B

(i). ASC [Band (P)]

(ii). Select Band (P) ⩾B

→ Bandwidth constrained shortest path

(iii). Select array [N] from ASC [Band (P)]

N = 2;

N = {0, 1, 2};

Array [0] = [Band (P)]

→Shortest Path 1

Array [1] = Select Min [Band (P)] not in Array [0].values;

→Shortest Path 2

Array [2] = Select Min [Band (P)]
not in (Array [0].values, Array [1].values);

→Shortest Path 3

...

...

...

Array [N-1] = Select Min [Band (P)]
not in (Array [0] values, ... Array [N-1].values);

→Shortest Path N-1

Array [N] = Select Min [Band (P)]
not in (Array [0].values. Array [N].values);

→Shortest Path N

2.5 Dribble Check Algorithm

The limit value or delay variation tolerance also controls how many packets can arrive in a burst, determined by the excess depth of the bucket over the capacity required

bandwidth of P ($Band$ (P)) is the minimum value of link bandwidth ($Band(e)$) in P. i.e.,$Band(P) = \min(Band(e,\ e \in E_p))$

for a single packet. Hence MBS is also a measure of burst or jitter, and it is possible to specify the burst as an MBS and derive the limit value τ from this or to specify it as a jitter/delay variation tolerance/limit value, and derive the MBS from this.

Where the packets are transmitted with a maximum bandwidth determined by the Sustainable Cell Rate (SCR) and cells within the packets are transmitted at the Peak Cell Rate (PCR); thus allowing the last cell of the packet, and the packet itself, to arrive significantly earlier than it would if the cells were sent at the SCR: transmission duration = (MBS-1)/PCR rather than (MBS-1)/SCR. This bursting at the PCR puts a significantly higher load on shared resources,

e.g. switch output buffers, than does transmission at the SCR, and is thus more likely to result in buffer overflows and network congestion. *The maximum size of this burst, M.*

τ – Min / Max interval Time

T – Emission Interval

δ – Arrive time /each packet

$$M = \left\lfloor 1 + \frac{\tau}{T - \delta} \right\rfloor$$

Equally, the minimum value of jitter tolerance τ that gives a specific MBS can be calculated from the MBS as follows:

$$\tau = (M - 1)(T - \delta)$$

Sample for selected shortest path roots

Sender – n1

Receiver – n29

n1, n2, n3 ... n29

n1-n4-n8-n12-n19-n22-n29 = 7ns

n1-n4-n8-n12-n19-n22-n29 = 7ns

n1-n4-n9-n13-n20-n22-n29 = 8ns

n1-n5-n9-n15-n16-n27-n28-n29 = 8ns
n1-n5-n6-n7-n15-n16-n27-n28 = 8ns

n1-n2-n3-n17-n23-n24-n26-n29 = 10ns

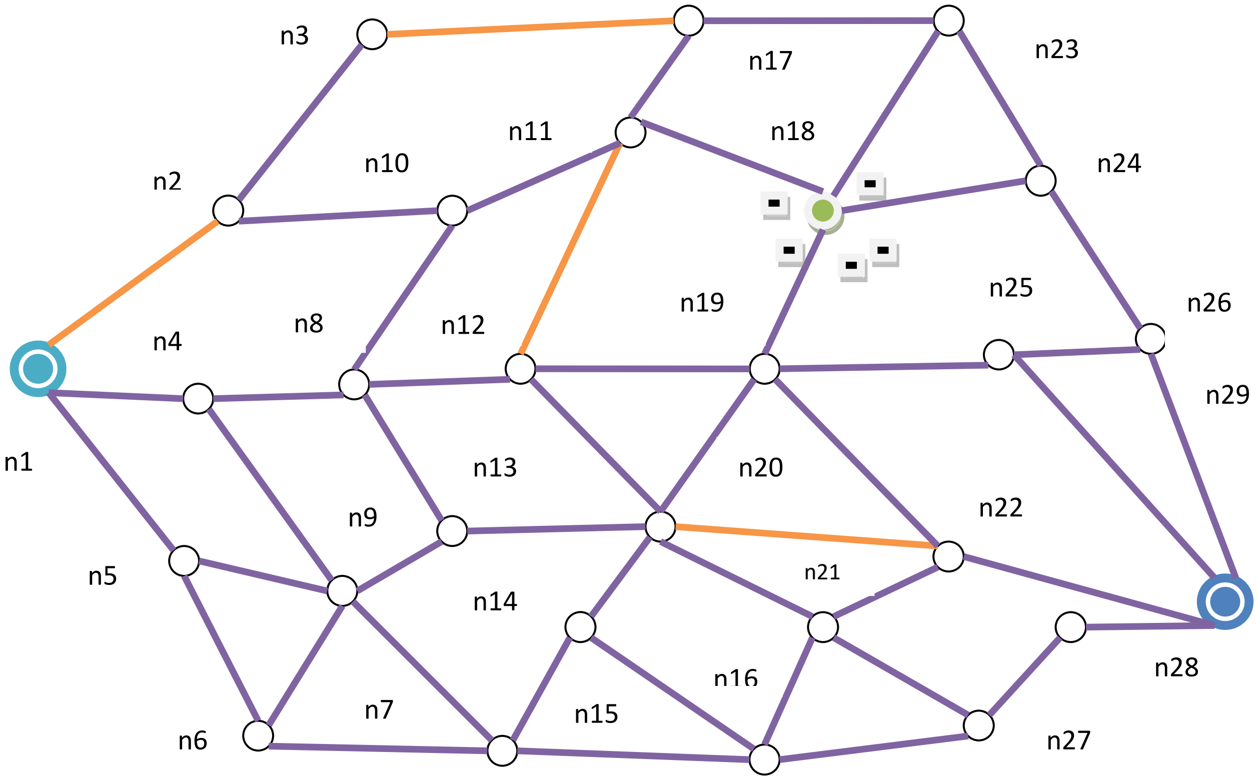


Fig3: Network structure with overall layout

◎ Sender ◉ Receiver ● Busy Node ▪ Waiting for Signal

— 1 ns travel — 2 ns travel time

Table1: A Trace table of distance travelled by node

Node	Distance (ns)	Node	Distance(ns)	Node	Distance(ns)	Node	Distance (ns)
n1-n2	2	n2-n10	1	n11-n18	1	n25-n26	1
n2-n3	1	n10-n11	1	n18-n24	1	n1-n5	1
n3-n17	2	n7-n15	1	n1-n4	1	n5-n9	1
n17-n23	1	n15-n16	1	n8-n12	1	n13-n21	1
n27-n28	1	n12-n19	1	n16-n27	1	n9-n13	1
n20-n21	2	n13-n20	1	n22-n29	1	n5-n7	1

3. CONCLUSION

The mechanism can be made customized to provide for making the trade-off between the security level and speed move in nature. In other words more security features like sending of data packets definition to be scouted dynamically from the given packets, in depth finding of each packet be introduced and user having the chance to decide which of these he wishes to implement because all of them will have their constrain in terms of speed.

References

[1]. J.A. Bondy and U.S.R. Murty, Graph Theory with Applications, (2nd Edition), North Holland, 1976.

[2]. Reinhard Diestel, Graph Theory , Graduate Texts in Mathematics, Vol. 173, Springer Verlag, Berlin, 1991.

[3]. Douglas West, Introduction to Graph Theory, (2nd Edition), Prentice Hall, 2000.

[4]. B. Bollobas, Modern Graph Theory, Springer-Verlag.

[5]. Fan Cheung and Linyuan Lu, Complex Graphs and Networks, Regional Conference Series in Mathematics, Vol. 107, AMS, 2004

[6]. Dieter Jungnickel, Graphs, Networks and Algorithms, Algorithms and Computation in Mathematics, Vol. 5, Springer Verlag, Berlin, 2005

[7]. Japan Network Security Association: Fiscal 2007 Information Security Incident Survey Report. 2008. http://www.jnsa.org/en/reports/incident.html

[8]. Trusted Computing Group. http://www.trustedcomputinggroup.org Enterprise Strategy Group: Information-Centric Security and Data Erasure (White Paper), 2006.

[9]. G. Lawton: New Technology Prevents Data Leakage. IEEE Computer , Vol. 41, No. 9, pp. 14–17 (2008).

[10]. HDE: Survey of Erroneous E-Mail Transmission.(in Japanese), 2008 http://www.hde.co.jp/reports/20080423/

[11]. H. Tsuda: Toward Secure Use of Corporate Information. (in Japanese), Semantic Web Conference 2009, Keio University SFC, 2009.

[12]. ANDRÁSFAI, B.:Introductory Graph Theory.The Institute of Physics (1978)

[13]. ANDRÁSFAI, B.:Graph Theory: Flows, Matrices.The Institute of Physics (1991)

[14].BANG-JENSEN, J. & GUTIN, G.:Digraphs: Theory, Algorithms and Applications.Sprin-ger–Verlag (2002)