International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Tracking Communication Quality Degrading Events for Link Quality Estimation

Rehna Elsa Sam[1], Belma Anna Kurian[2]

[1]*P.G scholar Dept. of Electronics and Communication Engineering, Believers Church Caarmel Engineering College, Perunad, Pathanamthitta, Kerala, India rehnaelsasam123@gmail.com*
[2]*Asst. Prof. Belma Anna Kurian, Dept. of Electronics and Communication Engineering, Believers Church Caarmel Engineering College, Perunad, Pathanamthitta, Kerala, India*

Abstract - *Most trust-based security schemes used in networked devices are designed to operate without knowledge of underlying communication infrastructure and as such considers all data or packet losses to be the result of one or more attackers in the network. However improved security schemes should consider this non-ideal nature of the underlying communication equipment and protocols. There are many other reasons for packet loss such as buffer overflow, node mobility, overflow at queue discipline, link changes etc. In this paper, we develop a protocol to estimate the actual reason for the packet loss before punishing the innocent nodes. The contribution of this paper is analysing the causes of packet loss and isolating the malicious node. This model is simulated in Network Simulator 3. The results are analysed***.**

Key Words: Data Loss, Trust Model, Buffer Overflows, Traffic Load, Adhoc Wireless Networks, Link stability

1. INTRODUCTION

Current trust-based security systems assume, malicious node is only reason for packet loss. But there are many other reasons regarding the packet loss. They failed to find out real cause of packet loss and always assume a malicious node as the main attackers. Detecting and analyzing in most trust-based security schemes [2-5], the assumption of packet loss is only due to the malicious attackers. But there are many other reasons for packet loss such as buffer overflow, node mobility, queue discipline, link changes etc.

We classify the causes of packet loss into node related loss, mobility related loss and congestion related loss.

Node related loss is divided into a) a node acts as selfish node b) a node acts as malicious node.

a) When a packet arrives at a node, it do not forward as to save its energy. Here Node act as selfish node.

b) When a packet arrives at a node it do not forward as it is malicious node. Malicious node only forward control packet not data packet.

Loss due to mobility [7]: a) mac layer b) routing layer

In mac layer packet loss due to unavailability of routing information, as nodes are out of range.

In routing layer, packet loss take place in two cases: when a packet comes into routing table, it checks for its next hop address. If their it forwards otherwise, it stays in buffer.

1) If it exceeds the time in the buffer, packet get loss.

2) If the buffer is bandlimited, then packet loss take place.

Congestion [7] related loss: due congestion problems packet loss take place.

a) Queue overflow: due to high data rate, more packet comes to buffer. As the buffer is band limited, packet get loss.

b) Busy channel: as the channel which we forward a packet is busy, they are put into a back off time. If it exceeds the time, packet loss take place.

For the analyzation and detection of various parameter, we implement the model in OLSR protocol, where it updates information continuously. For the simulation, 30 nodes are used. 1 node is considered as malicious node (so as to know if packet loss take place due to malicious attacker). We set queue size of 100 packet. One packet size is 409600 bits.

2. PARAMETERS INFLUENCING FOR PACKET LOSS

In Mac layer, when we send a message, we get an ACK back from the receiver. So when each message is send we get san ACK back. When the data rate is high, more packet are send and more ACK we get. It causes interference in the channel. We implement a packet header in which data are encapsulated. It is forwarded along the HELLO packets. At the receiver the data packets are taken from HELLO packet. When a node is malicious it do not forward the data packet , it only forwards control packets. We can find out the packet by number of packets at the receiver to the total number of packets.

We can calculate the probability of packet loss PM,

PM = Ratio of number of packets received to the total number of packet sent **(1)**

Traffic load intensity	Reserved

Fig -1: Proposed protocol's packet header

OLSR HELLO packet header	Proposed protocol's packet header

Fig -2: Final packet format

Due to high data rata, more packet comes to the buffer. As buffer are band limited packet loss take place.

Average Traffic load intensity

$$TL_B = (q_1+q_2+\ldots q_N)/N \quad \textbf{(2)}$$

Traffic load intensity,

$$TLI_B = TL_B / q_{max} \quad \textbf{(3)}$$

$$PQ = 1 - TL_B \quad \textbf{(4)}$$

As nodes are moving, formation of new link and breakage of old link takes place. Link change is the number of link formation and breakage of link.

$$\eta_a = \lambda_a + \mu_a \quad \textbf{(5)}$$

$$\eta_a = (\lambda_a + \mu_a) / 2\sigma_a \quad \textbf{(6)}$$

Where., a represents node a

$2\sigma_a$ is maximum link arrival rate and link formation rate

λ_a=link formation of node a

μ_a= link breakage of node a

η_a=total number of link formation and link breakage of node a.

3. IMPLEMENTATION

Protocol is developed. Behavior model is developed, that is making a node malicious. Malicious node do not forward data packet, they actually forward only control packet. Calculate queue load, forward to its neighbors. Special packet headers are developed. Along with OLSR protocol, special packet headers are forwarded. Table to update the details of incoming and outgoing HELLO packets. Calculating the HELLO packet. Calculate the link formation and link breakage

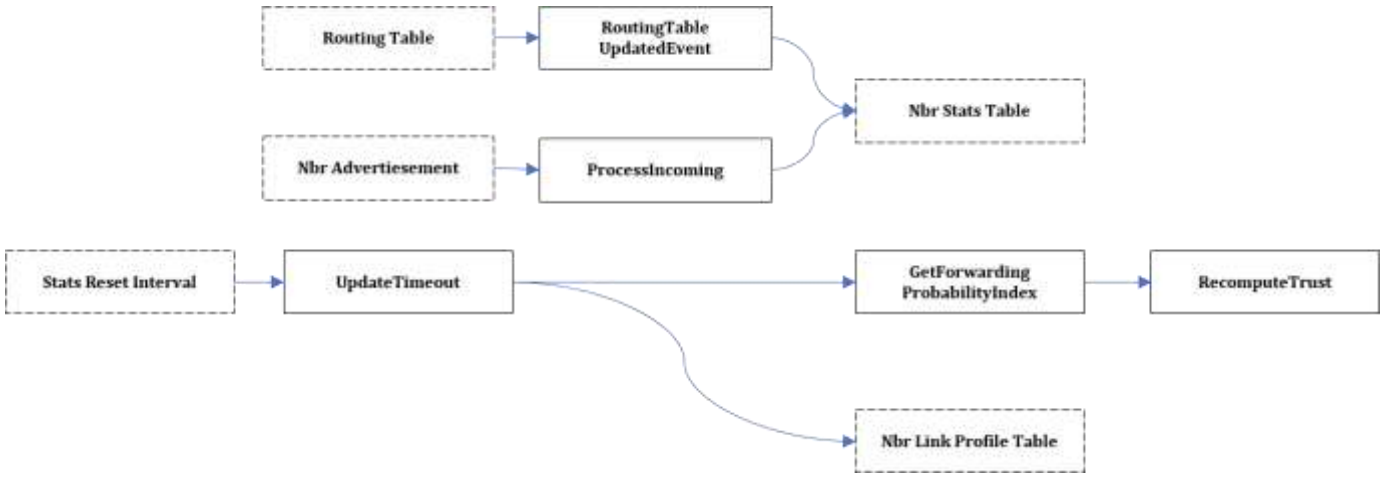

Fig -3: Functional block diagram for incoming packet

In the above figure, it shows as the function call diagram for the incoming packet. When a packet comes to a node, three steps operate at the same time. 1. Update times out 2. Process incoming and 3. Routing table updated events.
When a new packet enters, it checks whether it is from new neighbors. If it is from new neighbor, it updates the routing table. Then the updating and all the details about the neighboring nodes are mentioned in neighbor stats table. Stats Reset interval provide the intervals to make calculation. All the calculation are stored in neighbor link profile. Then recompute trust , where we decide a node is malicious or not. It seeks the help of forward probability index. Two threshold value are there. Trust threshold and FPI threshold. If the calculation is below the FPI threshold and if it is below trust threshold the node is malicious and we isolate the attacker.

Ip address	Neighbor discovery message packet	Link arrival count	Link breakage count	Traffic load intensity	Link stats

Fig -4: Single row of neighbor stats table

In figure 4 shows the neighbor stats table of each node that is detailed information of neighboring node. In the figure 5 all the calculation of the nodes are stored

Ip address	Probability M	Probability Q	Probability η	Malicious	trust

Fig -5: Single row of neighbor link profile

In the figure 6 shows the function call diagram of outgoing packets. When a packet goes out of a node it catches the packet and generate a header and calculate its traffic load

intensity. Then along with the HELLO Packet, the packets are forwarded

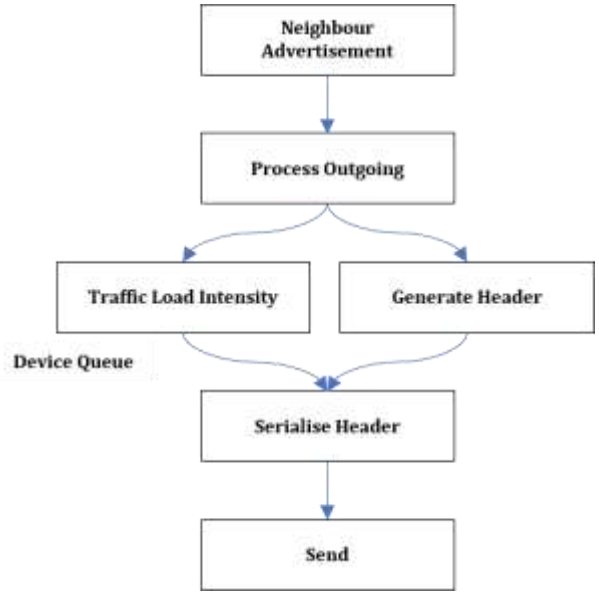

Fig -6: Functional block diagram for outgoing packets

4. APPLICATIONS

All the security protocols, are developed using different algorithm. Mostly in security protocols such as power control, speed control etc.., assumptions are made. One of the assumptions used in security protocol is that main cause of packet loss is attack of malicious node(attacker). But that assumption is wrong and changed that assumption find out the definite reason for the packet loss for more security.

5. CONCLUSION

In this paper we introduce a packet header along with the HELLO packets. We implemented behavioral model that is making one node as malicious. Find out and analyzed the various causes of packet loss. Some of the parameters are queue overflow, link changes, unavailability of routing information. queuing discipline etc. we simulated in network simulator3. Implemented new algorithm. We developed a packet header, along with the HELLO packets, our data packets are forwarded.

In future work Queuing discipline will also be taken into consideration. Analysis of packet loss in terms of the transport protocol used.

6. SIMULATION RESULTS

Implementation of the model are simulated in NS3. Fig 6 show packet loss when data rates increases. X- axis represents effects of data rate and Y axis represents number of packets drop. As more data packets, queue overflows due limited bandwidth, so packet gets loss. As data rate increase packet loss increases in non-linear manner**.** Only nodes which are in the path of receiver and sender are contribute to the packet loss

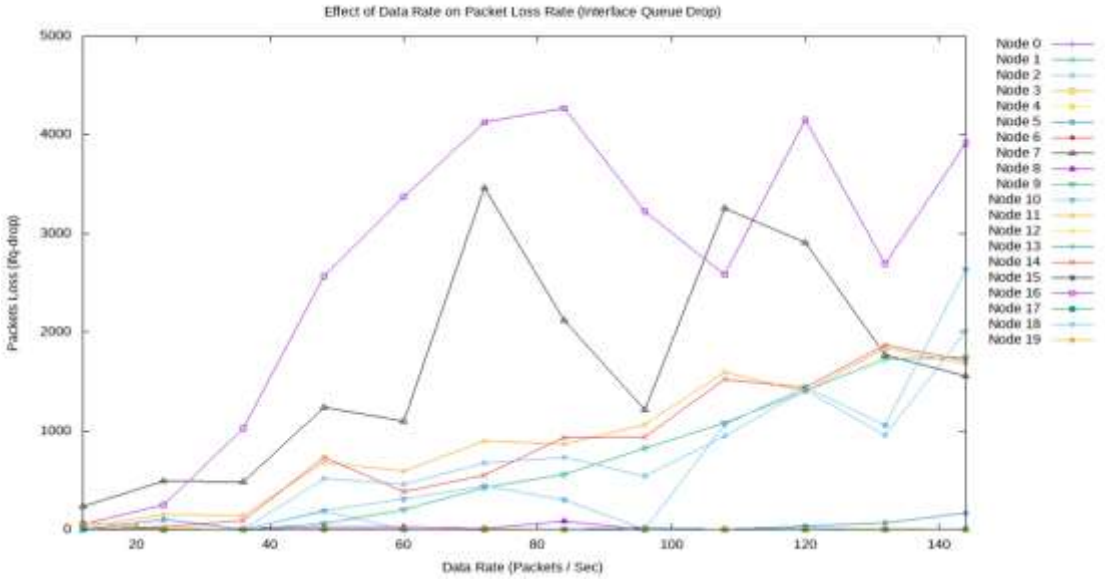

Fig -7: Packet loss due to queue interference

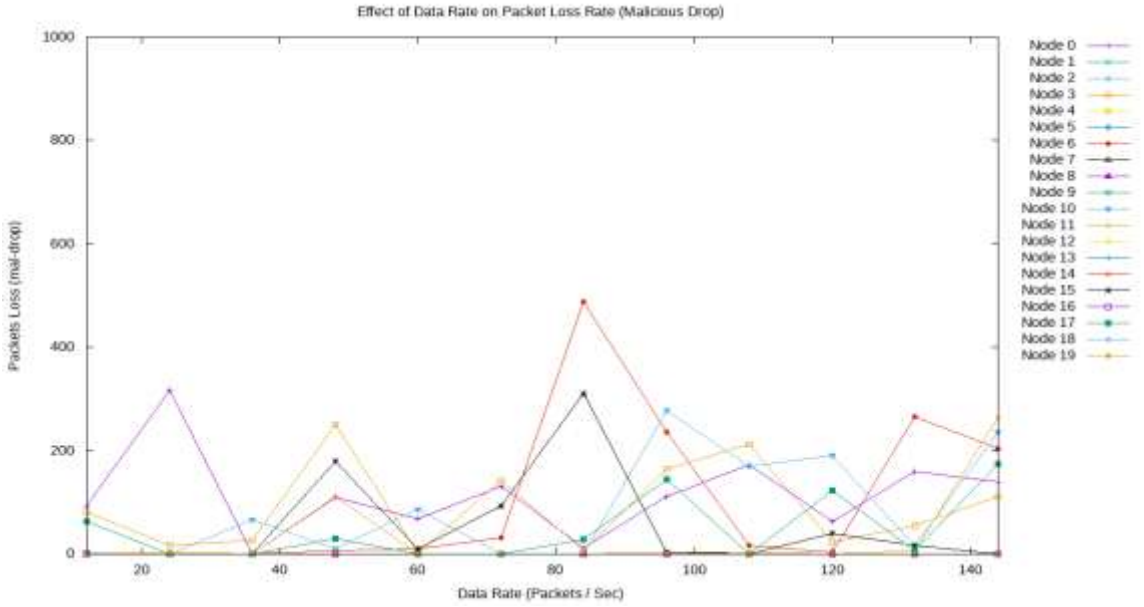

Fig.-8: Packet loss due to malicious drop

Fig8 shows packet loss due to malicious drop as the data rate increases. X- axis represents effect of data rate (malicious node) and Y -axis represents packet loss. As the data rate increases there is slight increase in packet loss. This is due the increase in number of packets send to the malicious node.

Table -1: Results after a single run

Node	IFQ drop	Malicious drop	No-RT -drop
0	0	317	0
1	0	0	0
2	0	0	0
3	0	17	0
4	0	0	0
5	101	0	0
6	0	0	0
7	487	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	153	3	0
12	0	0	0
13	0	0	0
14	24	0	0
15	0	0	0
16	246	0	0
17	0	0	0
18	8	0	0
19	12	0	0

REFERENCES

[1] A. A. Cardenas, N. Benammar, G. Papageorgiou, and J. S. Baras, ‘‘Cross- layered security analysis of wireless ad hoc networks,’’ presented at the 24th Army Sci. Conf., Orlando, FL,USA,2004

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ‘‘Mitigating routing misbehaviour in mobile ad hoc networks,’’ in Proc. 6th Annu. ACM Int. Conf. Mobile Comput. Netw., 2000, pp. 255–265]

[3] S. Buchegger and J. L. Boudec, ‘‘Performance analysis of the CONFIDANT protocol,’’ in Proc. 3rd ACM Int. Conf. Mobile Ad Hoc Netw. Comput., 2002, pp. 226–236

[4] K. Balakrishnan, J. Deng, and P. K. Varshney, ‘‘TWOACK: Preventing selfishness in mobile ad hoc networks,’’ in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 2005, pp. 2137–2142.

[5] A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, ‘‘AACK: Adaptive acknowledgment intrusion detection for MANET with node detection enhancement,’’ in Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl., Apr. 2010, pp. 634–640

[6] E. M. Shakshuki, N. Kang, and T. R. Sheltami, ‘‘EAACK—A secure intrusion-detection system for MANETs,’’ IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089–1098,Mar.2013

[7] Y. Lu, Y. Zhong, and B. Bhargava, ‘‘Packet loss in mobile ad-hoc net-works,’’ Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, USA,Tech. Rep. CSD-TR 03–009, 2003.

[8] O. Khalid et al., ‘‘Comparative study of trust and reputation systems for wireless sensor networks,’’ Secur. Commun. Netw., vol. 6, no. 6, pp. 669–688, 2013