A QUALITY ESTIMATION TECHNIQUE FOR SECURE DATA TRANSFER IN WANET

Divya.V[1], Rabindranath.S[2]

[1,2]4th Semester M.Tech,Software Engineering, AMC Engineering College Bangalore
divs.viju@gmail.com, rabin_s@yahoo.com

Abstract

Malicious packet dropping and link error are the two main references for message dropping in all dual hop wireless adhoc-network. Since the observation made on continuous packet losses that taking place in the network. Hence this paper is interested in determining various causes for message dropping and mainly focused on identifying whether it's caused because of connectivity errors by the nodes only or even by the mixed force of destructive and connecting error of packet drop. The main interest is on inside attacker case, where the malicious nodes are even the part of any particular route that exploits their knowledge of the communication context that selectively drop a small packets at each node that critical the performance of the network. Since the packet dropping rate is compatible to the channel error rate, various conventional algorithms that are used in determining the packet loss don't bring satisfactory determining accuracy. Hence to improve the detection accuracy, auto correlation functions are proposed in between the lost packets. The public based auditing function is implemented in the architecture known as Homomorphic Linear Authenticator (HLA) is done in the detector side to check for the truthfulness for the lost packets by any node that is involved in data transfer. Hence, it provides collusion proof, and also lowers the communication and storage overheads and privacy preserving. Finally, to reduce the computation overheads the block based packet mechanism is proposed.

Keywords: *HLA, Packet Block Based, Attack Detection, Packet Dropping*

----------***----------

1. INTRODUCTION

In context of multi hop wireless network, nodes are usually co-operated in relaying traffic. An adversary (intruder) of a new node at the same time exploit this co-operative nature to the attacks.

Example, consider the intruder node might initially act to be a trust worthy node in the network that will be created.; the intruder slowly starts initializing to drop the packets in the network. In some of the serious form, the destructive node can simply stops forwarding the packet that is received from upper nodes, during like erasing the path between the sender and the receiver will be exhausted. Henceforth, such a severe, Denial Of Service attack can paralyse the network by partitioning its topology (arrangements of links/nodes). The continuous message dropping in the network can spoil or lower the performance of the network, from the attacker's base point it so called as "always-on" attack which is its disadvantage. The malicious node itself can be a part of route which will exploit its knowledge of the communication context and the network protocol so as to launch the attacker. Inside an attack that is intermittent, but it can achieve the real performance rate degradation effect as the persistent attack at much lower risk of detecting. But when we start targeting these of the malicious node, which are highly critical packets, the authors [21],[24],[25] have shown that they can significantly damage the entire network with the least probability of they being caught. Hence detecting the selective packet dropping in the network will be very highly being challenging in dynamic wireless network environment. The difficult arise not only finding the message drop where it is dropped but also finding a dropping is intentional or unintentional. This dropping can be because of fading, interference, noise or the link errors due to the nature of the wireless medium. This paper propose a solution to the above public-auditing problem is based on the authenticateion for the detector to find truthfulness of the packet dropped. Homomorphic linear authenticator (HLA)mechanism which is cryptographic primitive method [2],[3],[27] which is basically a solution of signature used in server which helps in storage and also in cloud computing. It also provide privacy preserving and also reduces low communication cost and storage overheads in the middle nodes of sender and reciever.

2. RELATED WORK

For this paper, the related work is carried out by finding how much weight age can the detective algorithm gives to the link errors relative to destructive packet drop. It can be classified into many categories as follows: The first category always aims at high malicious dropping rates, where all the lost packets are caused due to destructing of packets by the route or the intruder in the network. In this, the effect of each of link errors will not be calculated. Most of the related survey will fall into this mechanism. The techniques that are used to identify the attacking nodes, these of the mechanism can be further classified into four categories. The first will be the credit system [9],[34],[10]. The second will be the reputation system which will depend on neighbouring nodes to address their nodes when misbehaving happens [8],[14],[11],[20],[12]. This system will be used as an important metric to eliminate the malicious node. The third

will be the hop-to-hop which provides acknowledgments directly where the packet drop takes place [23],[5],[22]. Further that node will be excluded from the network. Finally the problem can be addressed by cryptographic methods. As we know there a common technique that are used by the routing protocol for all the adhoc wireless network is to basically establish the routing path only on-demands. Since in all adhoc wireless network each of the network nodes are not in the same range they are scattered around the network. Hence they will significantly cause the damage in packet dropping by the introduction of intruder in between any nodes in the network. Hence to overcome all these byzantine failures a new method was proposed to overcome the damage caused by each of the node in demand routing protocol. This protocol basically relays on the technique that would actually find the cause for the messge drop in the network. But various methods that are used earlier will not provide required accuracy to the network. That is because the message dropped due to link error and the message dropped by the destructive node, the errore will be in very small differences. So they will be neglected.

3. EXISTING SYSTEM

The key criterion is to identify the various techniques to reduce the packet dropping that is caused because of link errors or only by the malicious nodes or even at the combination of both the link error and malicious nodes. But all the related papers were mainly concentrated in identifying the packet drop that was happening only because of either of the method. The big challenge is that detecting selective packet-dropping attacks in a dynamic wireless environment. The problem arises that we need not only to identify the place or the node where actually the message dropping is taking place. The various techniques used were:

- **A large dropping rates due to malicious nodes:** It aims at the huge range of malicious dropping rates where most of the packet is lost due to the malicious dropping. But where are the impact that is happening due to the link error is completely ignored.

The above method can be sub divided into various sub categories as follows:

- Reputation method: These methods completely rely on the neighbouring nodes for identifying miss behaves nodes. The node that has very high dropping rate will be the given the least reputation number.
- Credit System: It provides cooperation for an incentive. The node that gets the points by sending packet and it will in turn use its credit to send its own packets.
- Acknowledgment to hop-hop: this method is used to directly identify the place where messages are getting dropped. A node that has high packet dropping will be directly excluded from the network.
- Cryptographic technique: in this mechanism the bloom filters are used as proof for the construction of packet forwarding at each node. By studying the relayed packets at each of successive node along the route, one can easily identify the harmful hope that takes place in the network.

But the number of harmful packets dropping is comparibly high than that of link errors.

Disadvantages:

- They assume that the reason for packet dropping is only by malicious dropping.
- The credit system cannot be trustworthy since the neighbour node might give good credit to the node it is close too.
- The technique of bloom filter itself can contain the error in its proof.
- In the reputation mechanism the harmful node sometimes itself maintain a good reputation by forwarding many of the packets to the neighbouring node.

4. PROPOSED SYSTEM

The main idea in this paper is to propose a mechanism that would reduce the packet dropping by both the link error and the malicious node dropping. A new algorithm can be designed for detecting the particular packet drops that are made by the internal attackers. This accurate algorithm provides a real trust worthy and publicly verifiable decision as a identical proof to support the detection decision.

A phenomenon of high detection accuracy is attained by the correlation of the nodes between the position of the packets, as it is calculated from the auto-correlation function (ACF) of the message loss by a bitmap- bitmap that will in turn describe the status packet lost of in a correct sequence.

Hence, by detecting the correlation between the packet that are lost sender can conclude whether the packet that is lost is due to regular connectivity error or by the combination of connectivity error and destructive drop.

The challenging task in our paper is to identify that how to guarantee message loss in the network bitmaps that is reported by the individual node. Such truthfulness is very essential in calculating the correct correlation between the lost packet and this can be achieved by public auditing. The idea of auditing, is constructed based on the (HLA)
Homo-morphic authenticator, which involves the scheme of signature.

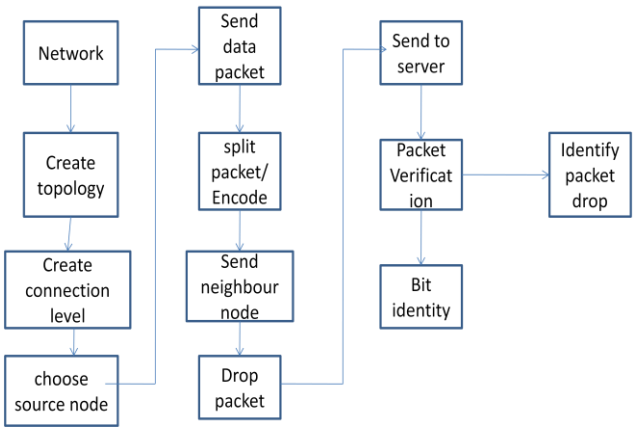

Fig 4. System architecture

The various modules involved in this present paper are**:**

Network Model: It is the wireless channel that is modelled between the source and destination as a random path. The packets that are transmitted between the good states reaches the destination where as packets that travel through bad path, the packets will be lost.

- **Set up phase:** this phase will be established before the transmission of packet takes place in the route.
- **Independent auditor:** It refers to the node which is independent of both source and destination node. It will be responsible in detecting all the destructive node in the network.
- **Packet drop detection:** the present mechanism, is based on detecting the packet that are lost in the network during transmission.

Advantages

- It reduces the communication and also storage overheads at the intermediate nodes.
- Accuracy is highly maintained.
- Privacy preserving helps in packet delivery on the correct route submitted by individual nodes in the network.

CONCLUSION

The present paper is compared with the detecting of packet loss algorithms that will utilize only the number of loss packets that are distributed, by identifying the correlation function between the lost packets that will significantly higher the accuracy in identifying the packet drop. This type of improvement is only possible only when it is compared with the link errors that are causing the packet drop. Hence to correctly calculate the packet drop the auto correlation function is used in between the nodes. The other mechanism called HLA public auditing architecture is also developed to ensure the truthful packet drop at individual node. Therefore it provides relatively high computational capacity at the sender node but also concentrates at low communication issues and the storage overheads.

A block based packet mechanism is used so that will allow only one to trade the identifying accuracy for the low computation complexity.

FUTURE ENHANCEMENT

Some of the open issues will be targeted at our future work. This proposed mechanism is limited only to the static wireless adhoc network. The continuous changes in the topology and the linking characteristics are not yet considered. Next the extension to the mobile environment will be enhanced further. The optimization and the implementation of the proposed mechanism with respect to various protocols will be considered in further studies.

REFERENCES

[1] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, “ODSBR: An on-demand secure bzantine resilient routing protocol for wireless ad hoc networks,”

[2]ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

https://www.google.co.in/webhp?sourceid.

[3] G. Ateniese, S. Kamara, and J. Katz, “Proofs of storage from homomorphic identification protocols,” in Proc. Int.

[4]. https://mail.google.com