RESEARCH ARTICLE OPEN ACCESS

IMPROVING THE ATTACK DETECTION ACCURACY USING HLA IN WIRELESS AD HOC NETWORK

Veeramani.R (Assistant Professor) [1], Sindhu Bharathy.B[2]
[2](M.Tech Student of CSE),
SRM University, Ramapuram,
Chennai

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

Abstract:

In wireless ad hoc network packets are loosed due to two conditions one is due to the disturbance in the channel and another one is due to the intrusion (i.e.) intruder discard the packet. In this paper we focus on the inner attack (i.e.) the attack caused by the intruder who maliciously discards the packets. The malicious node pretends to be an one of the node in the routing path and cause the attack. Conventional algorithm does not provide the efficient detection of packet loss so, In order to improve the detection accurately we propose correlation function and also for the correct calculation of correlation we implement BLS based Homomorphism Linear Authenticator to check the information provided by the node are true. The HLA architecture provides privacy preserving, collusion proof and allows low communication and storage overheads**.**

Keywords:-**packet dropping, secure routing, attack detection, Homomorphic linear signature, auditing**

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

I .INTRODUCTION

Nodes are co operatively function in the routing path. An attacker uses this cooperation and pretends to be an one of the node in the routing path. Once the attacker included in the routing path starts discarding the packet. The intrusion node stops sending the packet received from the above node to the node below which completely disturb the routing path between the sender and receiver. This type of attack is known as DoS. The malicious node may classify the significance of different packets and discard the most significance packet which leads to degradance of the network performance the authors in [3], [4], [5] Identifying the significant packet is a critical task in a wireless medium.

In this paper we develop an absolute algorithm for identifying the most significant packet discard made by the inside intruder. Our algorithm provides truthful and publicly verifiable decision by the auditor. The accurate detection is obtained by the correlations between the lost packets. The correlations are performed by Auto correlation function [ACF]. To verify the lost packets and the information send by the individual node about the packet loss is checked by constructing Homomorphic linear Authenticator. HLA is a signature scheme and is based on 4 ppt algorithm that provides privacy, collusion avoidance and low storage overheads.As described in the next section, previous work on distinguishing between causes for dropped packets considered only collisions and channel errors [2,[5] and ignored malicious packet drops. On the other hand, protocols that detect malicious packet dropping [6],[8] ignored collisions and channel errors. In this paper we adopt a

unified approach to packet loss considering collisions, channel errors, and malicious packet drops. We consider two possibilities for a malicious node. First, it aims to disrupt network operation by not relaying a packet to the next hop. In this case the node will acknowledge the packet to the sender.

II .RELATED WORK

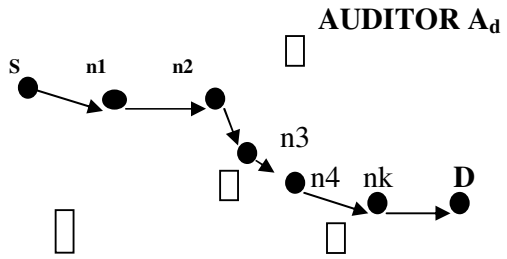
The work is classified into two categories. First category is based on malicious node dropping the packet which works on detecting the malicious node that causes the discarding of packets. Detection accuracy of malicious node is done by four ways i) whenever a node sends a packet it will earn a point for transmitting a packet. The malicious node which continuously discards the packet will lose its point [2] [1] [6] ii) Each node is monitored by its neighbor node. So the misbehaving node is monitored by the neighbor node iii) malicious node place will be identified and removed from the network. Iv) Some cryptographic method is used to have the record of forwarded packets. All this ways of identifying the malicious node have disadvantages and these methods will not be applicable when the packets are highly selective.

The main idea is that shorter RTS/CTS and MAC headers in 802.11 are less vulnerable to errors than data. Thus, during the RTS/CTS access procedure, errors are assumed to be due to collisions. If the node receives the CTS frame but not the ACK frame then the transmission has more likely failed due to a channel error. However, if an RTS/CTS frame is not received, then the transmission more likely failed due to a collision. If a basic access procedure is used, the sender depends on feedback from the receiver to determine the cause of packet loss. If a packet with a corrupted header is received, the receiver sends nothing and the sender will timeout and assumes that a collision occurred. If a packet with a correct header is received but the data part is corrupted, the receiver can recognize the sender and reply with a NAK frame. Here, the sender will assume that the packet was lost due to channel error.

III.SYSTEM MODELS AND PROBLEM STATEMENT

A.NETWORK AND CHANNEL MODEL

Let us consider a routing path between the nodes in the multi-hop wireless network. The source node "S" sends packet to the destination "D" through various intermediate node n1, n2, n3……nk. The sender node knows the routing path by using Dynamic Source Routing Algorithm [DSR]. In Dynamic wireless ad hoc network we can apply trace route operation to find the routing path between the sender and receiver.



Malicious packet drop Fig 1

The autocorrelation function of the channel is $f_c(i)$ is the time lag of packets. The $f_c(i)$ I is the time lag of packets. The $f_c(i)$ is calculated by probing approach. Sequence of packets is transmitted from the sender through the channel. In order to verify the packets are transmitted or not the receiver will maintain a record such as $\{a_1 \ldots\ldots\ldots a_m\}$ Where $a_j \sum \{0, 1\}$ $j = 1\ldots\ldots\ldots M$. "1" represents packet was transmitted "0" represents packet discarded. $f_c(i)$ is derived by $f_c(i) = E\{ a_j \; a_j+1\}$ for I =0,……M ACF represents packet transmitted is received or lost at different time. There is an auditor in the routing path of the nodes. It doesn't have

any knowledge about secret of the nodes. Auditor is used to detect the malicious node when it receives ADR request from the source. Source receives feedback from the destination. The integrity and authenticity of D is verified by the algorithm elliptic curve digitalsignaturealgorithm.

Ad requires information the node if any node was not replying correctly it is suspected to be the malicious node.

B.ADVERSARIAL MODEL: The aim of attacker is to degrade the network performance by dropping or discarding the packet. Malicious packet discarding can be any type (ie) it may be a significant packet or random packet. There may be some collision between malicious node. So, a malicious node may establish separate routing path apart from the original routing path and transmits its packet to the below malicious node this form of exchange can't be dected by the auditor.

C.PROBLEM STATEMENT:

From the network model and adversial model we can determine the nodes on the routing path that causes the packet

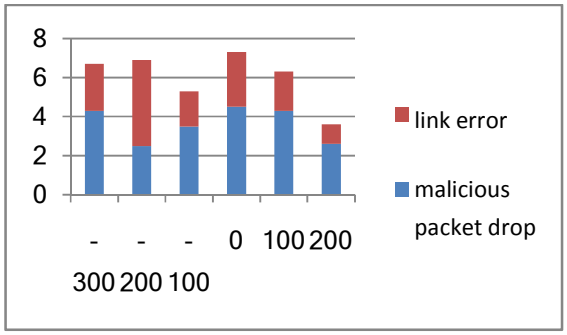


Fig 2

Comparison of correlation of lost packets dropping. This determination is carried out by the auditor who doesn't know any secrets above the node. When a particularly misbehaving node is identified auditor provides a publicly verifiable proof which should be privacy preserving and should be low communication and storage overheads.

IV PROPOSED DETECTION SCHEME

A. Overview:-

The proposed detection scheme is based on correlation of lost packets. Basically the packet loss of each hop is a random process alternating between 0 & 1. Consider packets are transmitted over a wireless channel and the packet transmitted are successful or not reached to the destination will be determined by the receiver bitmap such as (a1……am) where $a_j \sum \{0, 1\}$. Correlation of lost packets is calculated by Auto – Correlation Function (ACF).

The information send by the node about the lost packet should be true and this is verified by the HLA. The source who knows the HLA secret key generates HLA signatures .for distinct messages such as r_1……r_m. The sender transmits r_i and s_i through the route. The HLA signature is constructed by the way $\sum^{M}_{i=1}$ ci $_{ri.Our}$ construction is that S_i and $r_{i\ are}$ transmitting along the route so knowing S_1……S_m also verifies that node must have received r_1……..$r_{m.}$Our Architecture consists of 5 phases Ad hoc Network Formation, Sender, Packet Classification, Auditor, Receiver.

B.Scheme Details:-

Ad hoc Network Formation: - In which nodes are connected in an ad hoc network and a routing path is established. The sender decides the symmetric key cryptosystem and distributes the key and decrypt key to all the nodes on the routing path. Key distribution is based on RSA algorithm. S encrypts the key_i using the public key of the node n_j andsends cipher text to n_j. Node j decrypts the cipher text using its private key to get the $key_{i.}$. S also specifies two hash functions H_1 and all nodes in routing path .S also generate HLA

keys. Secret HLA key is s_x =x and public HLA key is a tuple $p_{k=}$ (v, g, u)

1) Sender: Sender(s) transmits the packet pi along the routing path. Before transmitting the packet pi, S computes r_i=H1(pi) and generates HLA signature of r_i for node n_j as follows.

S i_j= [H2 (I||J)u r_i]x, for j=1……k……..[1]

This signature is send along with the packet with one- way chained encryption. After getting S i_j for j=1……..k. then n_1 extracts Si and T2i from the decrypted text. It stores r1=H1 (pi) and Si in its proof of reception database. Database is maintained by every node by FIFO basis. Finally n_i assembles pi || T2i in to one packet and send this to node. In the equality test n1, marks the loss of pi in its proof of reception database and doesn't transmit packet to n2. The same process is repeated at every intermediate node.

2) *Auditor*: - when the auditor receives ADR request from the sender "S" it starts is auditing process. The ADR request consist of the id of the nodes, HLA public key information pk= (v, g, u) and the sequence number of the packet send from S and the sequence number of the subset of this M packets are received by D.

Ad conducts auditing process as follows.

Ad submits a random challenge vector c_j= (cj_1…….cj_m) to node n_j. The sequence number of packets in the current proof of reception database is p1……pm. Where pm is the most sent packet by S. Depending upon this information the node n_j generates thepacketreceptionbitmapbj = (b_{ji}……b_{jm}) where b_{ji}=1 if P has been received by and b_{ji}=0. Node n_j calculates n_j= $\sum_{im}$=, bji#0 $c_{ji}r_i$ and the HLA signature S_j=$\prod_{i=1,}$ Sjibji$_{\#0}$ ^{cji}…… [2]

Node n_j submits b_j, r $^{(j)}$ and S $^{(j)}$ to Ad as a proof of packet it is received.

3) Receiver: - The packets sent by the sender are received by the receiver. If the receiver doesn't receives the packet it sends a notification message to the sender.

CONCLUSION: - In this paper correlations of lost packet are correctly calculated. To ensure the truthfulness of information send by the nodes HLA based auditing architecture is used to provide privacy preserving collision avoidance and low communication storage overheads. Extension to dynamic environments will be studied in our future work.

REFERENCES:-

[1]. G.Ateniese, S.Kamara and J. Katz *proof of storage from Homomorphic Identification protocols. In proceedings of the international conference on the theory and application of cryptology and information security.*

[2]. G. Noubir and G. Lin. *Low power DoS attacks in WLANS and countermeasures.*

[3] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. *ODSBR: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM TISSEC, 10(4), 2008.*

[4] D. Boneh, B. Lynn, and H. Shacham. *Short signatures from the Weil pairing. Journal of Cryptology, 17(4):297–319, Sept. 2004.*

[5] S. Buchegger and J. Y. L. Boudec. *Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the ACM MobiHoc Conference, 2002.*

[6] L. Buttyan and J. P. Hubaux. *Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5):579–592, Oct. 2003.*

[7] J. Eriksson, M. Faloutsos, and S. Krishnamurthy. *Routing amid colluding attackers. 2007.*

[8] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor*: Scalable secure routing for ad hoc networks. In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, march 2010.*