ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

PRIVACY AND DETECTING MALICIOUS PACKET DROPPING USING HLA IN WIRELESS AD HOC NETWORK

*M. Sindhuja ** Mrs A.Sahaya Princy
Ponjesly College of Engineering
sindhujam25593@gmail.com,s.princy2006@yahoo.com

ABSTRACT: **Multi hop wireless ad hoc network is a network were link error and malicious node packet dropping attack more commonly occurs. There is no infrastructure exists for this network. Here every node is a mobile. To overcome all these issues several technique were implemented in the existing. The techniques such as credit system, reputation system, end to end or hop to hop acknowledgement etc are used to find the packet dropping attack in network. In this project a new technique such as HLA (Homomorphic Linear authentication) is proposed to authenticate data security in wireless ad hoc network. Homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. The routing algorithm and cryptographic algorithm is still an drawback in this model. This can be overcome by the proposed technique by implementing HLA with modified algorithm and routing. Thus data security is achieved by Ceaser cipher algorithm and the routing is implemented by OLSR. The OLSR routing is a secure routing methodology which transmits the data more efficiently without any time delay.**

Key Terms: Packet dropping, secure routing, Homomorphic linear signature, auditing

I INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relating / routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be cooperative node in the route discovery starts dropping packets. In the most server form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination. Eventually such a server Denial-of-Service (DoS) attack can paralyze the network by partitioning its topology.

Even though persistent packet dropping can effectively degrade the performance of the network, from the attacker's standpoint such an "always-on" attack has its disadvantages. To find this type of packet dropping there is many types of technique proposed. There are two type of classification in the technique. The first category aims at high malicious dropping rate, where most lost packet are caused by malicious dropping. In this case, impact of link error is ignored. Most of related work is fall is to this category. Based on this methodology used to identify the attacking nodes, these works can be further classified into four sub categories. Creating system, Reputation system, End to end or hop to hop[3] acknowledgement and Cryptographic methods[4]. A credit system [1] provides intensive for cooperation .A node receives credit by relaying packets for others, and uses its credit to send its own packets.

As a result, a malicious node that continuous to drop packets will eventually deplete its creadit, and will not be able to send its own traffic. A reputation system [2] relies on neighbor to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its neighbours.This reputation informatation is propagated by its neighbours.This reputation information is propagated periodically throughout the network and is used as an important metric in selecting route. Consequently, a malicious node will be excluding from any route.

Bloom filters used to construct proof for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. The second category [5] targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

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 [7] [1] ii) Each node is monitored by its neighbor node. So the misbehaving node is monitored by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

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. 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.

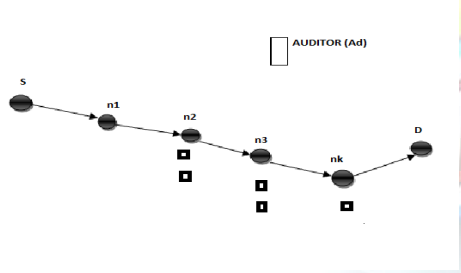

Fig 1 Malicious packet drop

The autocorrelation function of the channel is fc (i) is the time lag of packets. The fc (i) I is the time lag of packets. The fc(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……..am} Where aj Σ {0, 1} j =1……..M. "1" represents packet was transmitted "0" represents packet discarded. fc(i) is derived by fc(i) = E { aj aj+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 digital signature algorithm. Ad requires information the node if any node was not replying correctly it is suspected to be the malicious node.

ROBLEM STATEMENT:

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

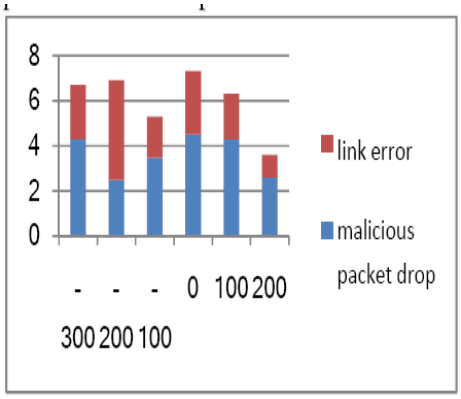

Fig 2 Comparison of correlation of lost packets dropping.

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. SYSTEM ARCHITECTURE

The initially the network is configured with calling the Node configure function with number of nodes. And then Link create will create link, while creating link we need to specify the levels with which the node is associated. Once the network is configured we take up server as the destination and any of the nodes as the sender. Once the network is set we browse for the file we need to send. In the source we split the entire file in to number of packets these packets will be encrypted and Add bit function will help in adding bits to identify the change in number of packets and packet will be forwarded further.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

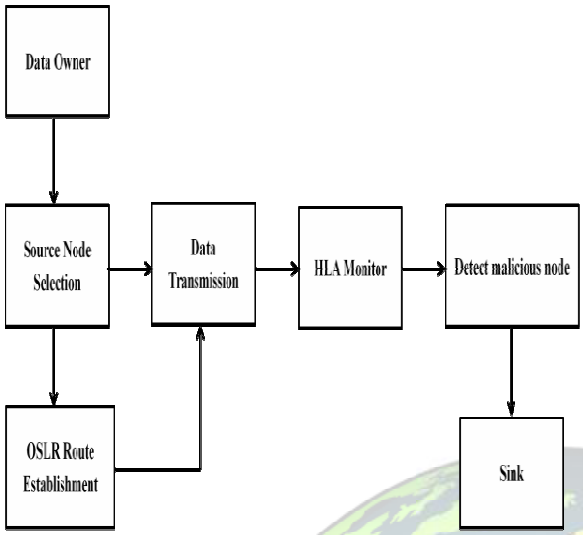

Fig 1 system architecture

The packet will be received by the intermediated node in normal transition packet will be encrypted and forwarded whereas in attacker mode packet will be dropped or modified or both will be done and forwarded. Once the packet reach destination in normal node packet will be verified, bit identified, decrypted and finally merged. In attacker mode when packet is verified the packet dropped is identified, bit identification will let us know about packet modification. On modification or dropped packet cannot be decrypted. To develop an accurate algorithm for detecting selective packet drops made by insider attackers. Christo Ananth et al. [6] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

Public- auditing problem is constructed based on the homomorphism linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients.

V. SYSTEM MODULES

The system contains three modules.

1. Network modeling.
2. OLSR Routing
3. Independent auditing.
4. Packet dropping detection

A. Network modeling

The wireless channel is modeled of each hop along PSD (Path to Source and Destination) as a random process that alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. It is assumed quasi-static networks, whereby the path PSD remains unchanged for a relatively long time. Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, maintaining stable connectivity between nodes is a greater concern than detecting malicious nodes. A sequence of M packets is transmitted consecutively over the channel.

B.OLSR Routing

Here the OLSR routing is the secure routing network. It is an IP routing protocol optimized for mobile ad hoc networks. The link error rate is avoid in this network model .Thus the OLSR routing is a promising routing protocol that can be simply used to develop

C. Independent auditor

There is an independent auditor Ad in the network. Ad is independent in the sense that it is not associated with any node in PSD. The auditor is responsible for detecting malicious nodes on demand. Specifically, it is assumed S receives feedback from D when D suspects that the route is under attack. Once the destination click on verify, the action takes places to identify the packet loss. To facilitate its investigation, Ad needs to collect certain information from the nodes on route PSD.

D. Packet drop detection

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

packets that are transmitted consecutively over a wireless channel. Under different packet dropping conditions, packet loss is identified.

VI. 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 aj Σ {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 r1……..rm. The sender transmits ri and si through the route. The HLA signature is constructed by the way ΣM i=1 ci ri. Our construction is that Si and ri are transmitting along the route so knowing S1…….Sm also verifies that node must have received r1……..rm..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 nj and sends cipher text to nj. Node j decrypts the cipher text using its private key to get the key i. . S also specifies two hash functions H1 and all nodes in routing path .S also generate HLA keys. Secret HLA key is sx =x and public HLA key is a tuple pk = (v, g, u)

1) Sender*:* Sender(s) transmits the packet pi along the routing path. Before transmitting the packet pi, S computes ri=H1(pi) and generates HLA signature of ri for node nj as follows. S ij= [H2 (I‖J)u ri]x, for j=1……k……..[1] This signature is send along with the packet with one- way chained encryption. After getting S ij for j=1……..k. then n1 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 ni 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 cj=(cj1…….cjm) to node nj. 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 nj generates the packet reception bitmap bj = (bji……bjm) where bji=1 if P has been received by and bji=0. Node nj calculates nj= Σim=, bji#0 cjiri and the HLA signature Sj=Πi=1, Sjibji#0 cji……. [2] Node nj submits bj, 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.

VII. 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] 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.

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

[3] W. Kozma Jr. and L. Lazos. REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009.

[4] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172, 2001..

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks

in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57, 2005.

[**6**] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

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

[**8**] Tao Shu and Marwan Krunz. Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks, IEEE Transactions on MobileComputing ,April 2015