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 2, March 2016

Truthful Detection of Packet Dropping and Attacks in Wireless Ad-Hoc Network

S.Bhuvaneswari[#1], M.Ramya[#2], M.Vinothini[#3]
B.E., – Final Year (CSE)
Bharathiyar Institute of Engineering for Women,
Deviyakurichi.
sellaiya.bhuvaneswari@gmail.com,
ramcse24@gmail.com,
mvinothinibe10@gmail.com

M.R.Nithya, M.E., AP/CSE
Bharathiyar Institute of Engineering for Women,
Deviyakurichi.
nithyarathinam@gmail.com

Abstract—In the multi-hop wireless ad hoc network there two sources of packet losses are link error and malicious packet dropping. While observing a sequence of packet losses in the network, to determining whether the losses are caused by link errors only or by the mingled effect of link errors and malicious drop. We are exclusively interested in the insider-attack case, thereby malicious nodes that are. part of the route adventure their knowledge of the communication context to selectively drop a small amount of packets degrade to the network performance. So the packet dropping rate in this case is proportionate to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfying detection accuracy. To improve the detection accuracy, we compute the correlations between lost packets. To ensure truthful computation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that grants the detector to verify the truthfulness of the packet loss information reported by nodes. This development is privacy preserving, collusion proof, and incurs low communication and storage overheads. To decrease the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which grant one to trade detection accuracy for lower computationa complexity. Through extensive simulations, we verify that the planned mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

Index terms: Packet drops, Attack detection, Secure routing, Homomorphic linear authenticator, Auditing.

1 INTRODUCTION

In a multi-hop wireless ad-hoc network, nodes cooperate in relating/ routing traffic. An adversary can adventure this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes; completely disturb 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 corrupt the performance of the network, from the attacker's standpoint, such an "always-on" the attack has its damage.

To find this types of packet dropping there is many types of technique proposed. There are two type of classification in the technique. The first class aims at high malicious dropping rate, where most lost packets are caused by malicious dropping. In this case, impact of link error is ignored. Most of related work is fall is in this category. Based on this methodology used to identify the attacking nodes, these works can be further classified into four subcategories. 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 confidence to send its own packets. As a result, a malicious node that continues to drop packets will eventually decrease its confidence, and will not be able to send its own traffic. A reputation system [2] relies on neighbours to monitor and identify misconduct nodes.

A node with a high packet dropping rate is given a bad reputation by its neighbours. This reputation information is propagated by its neighbours. This reputation information is

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
ET)
Vol. 3, Special Issue 2, March 2016

propagated periodically everywhere the network and is used as an important measured in selecting a path. Therefore, a malicious node will be prohibited from any route. Bloom filters used to construct proofs for the forwarding of packets at each node. By examining the hand over packets at successive hops along a route, one can identify suspicious hopes that exhibit high packet loss rates. The second category [5] targets the synopsis where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the meeting of link errors is non-negligible.

2 RELATED WORK

The work is classified into two classes, the first category is based on malicious node dropping the packet which works by detecting the malicious node that elements the cancelling of packets. Detection accuracy of malicious node is done by four ways i) at any time a node sends a packet, it will earn a point for transmitting a packet. The malicious node which continuously dispatches the packet will lose its point [7] [6] [1] ii) Each node is audited by its nearby node. So the misbehaving node is audited by the nearby node iii) malicious node place will be identified and removed from the network. iv) Some cryptographic process is used to have the record of forwarded packets.

All this way of identifying the malicious node had demerits and these methods will not be applicable when the packets are highly selective. If a basic access policy is used, the senders trust in
comment from the receiver to determine the element of packet loss. If a packet with an exploited header is
received, the receiver sends nobody and the sender
will timeout and concludes that a collision arises. If a packet with a faultless header is received, but the data part is corrupted, the receiver can recall the sender and reaction with a NAK frame. Here, the sender will assume that the packet was absent due to channel error.

3 SYSTEM MODELS AND PROBLEM STATEMENT

3.1 NETWORK AND CHANNEL MODEL

Let us see a routing path intermediate the nodes in the multi-hop wireless network. The source node "S" sends packet to the destination "D" over different transitional node n_1, n_2, n_3……n_k. The sender node learns the routing procedure by using Dynamic Source Routing method [DSR]. In Dynamic wireless ad hoc network, we can handle a fragment path operation to asset the routing path between the sender and receiver.

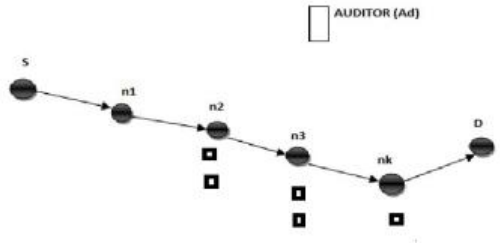

Fig .3.1. Malicious packet drop

The auto-correlation function of the channel is f_c (i) is the time lag of packets. The f_c (i) I am the time lag of packets. The f_c (i) is calculated by probing approach. Arrangement of packets is transmitted from the sender through the channel. In order to verify the packets are transmitted or not the receiver will control a record such as $\{a_1$…….$a_m\}$ Where a_j Σ
{0, 1} j=1…….M. "1" represents packet was
transmitted "0" represents a packet damaged. F_c (i) is derived by f_c (i) = E { a_j a_{j+1}} for I =0,……M ACF represents packet translated is received or lost in a particular time. There is an actuary in the routing path of the nodes. It doesn't have any knowledge about the secret of the nodes. The actuary is used to disclose the malicious node when it collects the ADR request from the source. Source receives comments from the destination. The integrity and authenticity of D is documented by the algorithm elliptic curve digital signature algorithm. Ad desires report the node if any node was not reacting correctly, it is incredible to be the malicious node.

3.2 PROBLEM STATEMENT

From the network model and adverse model we can resolve the nodes on the routing path that element the packet

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
ET)
Vol. 3, Special Issue 2, March 2016

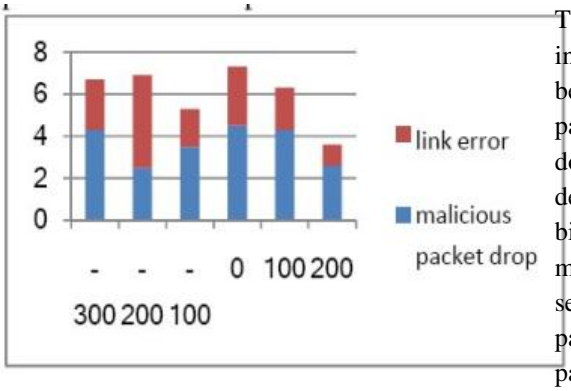

Fig.3.2.Comparison of correlation of lost packets dropping.

This assurance is carried out by the analyst who doesn't know any mystery above the node. When a particularly misconduct node is found detector gives a publicly verifiable proof which should be privacy protecting and should be low communication and storage skyward.

4 SYSTEM ARCHITECTURE

The initially the network is configured by calling the Node configure function with the number of nodes. And then Link creates will create links, 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 into the number of packets these packets will be encoded and Add bit function will help in adding bits to finding the change in number of packets and packet will be forwarded another.

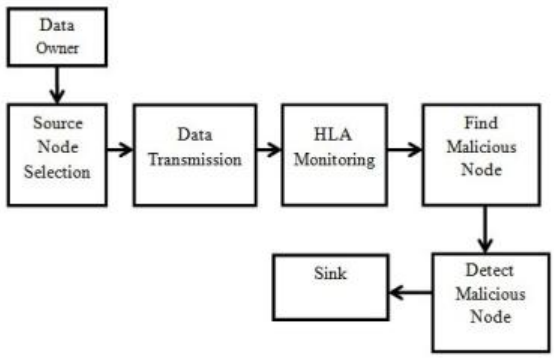

Fig. 4.1 System architecture

The packet will be received by the intermediated node in normal transition packet will be encoded 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 selected, decoded and finally joined. In attacker mode when packet is verified the packet dropped is selected, bit identification will let us know about packet modification. On modification or dropped packet cannot be decoded. To develop an accurate algorithm for detecting choosy packet drops made by join attackers.

This algorithm also gives a truthful and publicly verifiable decision sensuous as a proof to guide the detection decision. The high detection accuracy is achieved by attaining the correlations between the situations of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap representing the lost/received condition of each packet in a continuity of follow packet transmissions. By finding the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is added reaction of link error and malicious drop. The main relevance in mechanism lies in how to relevance that the packet-loss bitmaps dispatched by individual nodes along the route are truthful, i.e., reflects the actual dignity of each packet transmission. Such truthfulness is crucial for correct calculation of the correspondence between lost packets.

This can be accomplished by some auditing. Recognizing that a typical wireless device is asset-constrained, we also require that a user should be able to deputise the difficulty of checking and detection to some public server to save its own assets. The public-auditing problem is composed based on the homomorphism linear authenticator (HLA) cryptographic basic, which is basically a trademark design widely used in cloud computing and storage server systems to give a proof of storage from the server to allocating clients.

5 SYSTEM MODULES

The system consists of three schedules.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
ET)
Vol. 3, Special Issue 2, March 2016

1. Network modelling.
2. Independent auditing.
3. Packet dropping detection

5.1 Network modelling

The wireless channel is modelled of each hop along PSD (Path to Source and Destination) as an unplanned action that equivalents between good and bad states. Packets transmitted during the acceptable state are benefiting, and packets broadcasted during the bad state are absent. It is accepted quasi-static networks, whereby the path PSD endures constant for a related high time. Detecting malicious packet drops may not be an interest in highly mobile networks, because the agile-developing topology of such networks makes route interruption the assertive cause of packet losses. In this case, preserving stable connectivity between nodes is a greater burden than detecting malicious nodes. A sequence of M packets is transmitted consecutively over the channel.

5.2 Independent auditor

There is an independent auditor Ad in the network. The Ad is autonomous in the sense that it is not joined with any node in PSD. The analyst is culpable for detecting malicious nodes on need. 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 place to identify the packet loss. To facilitate its inquiry, Ad needs to gather assured information from the nodes on route PSD.

5.3 Packet drop detection

The proposed mechanism is based on detecting the correlations intermediate the lost packets over each hop of the path. The basic concept is to model the packet loss process of a hop as an unplanned technique doubling between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are translated consecutively over a wireless channel. Under different packet dropping conditions, packet loss is identified.

6 DETECTION SCHEME

6.1 Overview

The proposed detection scheme is based on correlation of lost packets. Essentially the packet loss of each hop is a random progress alternating between
0 & 1. Consider packets are transmitted over a wireless channel and the packet translate are successful or not reached to the destination will be determined by the receiver bitmap such as (a1……am) where a_j Σ {0, 1}. Correlation of lost packets is calculated by Auto – Correlation Function (ACF). The information send by the node around the lost packet should be true and this is verified by the HLA. The source who knows the HLA classified 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 ΣM i=1 c_i r_i. Our construction is that s_i and r_i are transmitted 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 deposit, Sender, Packet Classification, Auditor, Receiver.

6.2 Scheme Details

6.2.1 Ad hoc Network Formatting

In which nodes are connected in an ad hoc network and a routing path is established. The senders agree the symmetric key cryptosystem and distribute the key and decrypt key to all the nodes on the routing path. A major distribution is based on the RSA algorithm. S encrypts the key i using the public key of the node n_j and sends the cipher text to n_j. Node j decodes the cipher text using its private key to get the key i. S has also specifies two hash functions H1 and all nodes in routing path .S also generate HLA keys. The secret HLA key is s_x =x and public HLA key is a duple p_k = (v, g, u)

6.2.1.1 Sender

Sender(s) translate the packet pi along the routing path. Before transmitting the packet pi, S calculates r_i=H_1 (p_i) and achieves HLA signature

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
ET)
Vol. 3, Special Issue 2, March 2016

of r_i for node n_j as follows. S_{ij}= $[H_2(I\|J)\underline{u}r_i]x$, for j=1……k……..[1] This signature is sent onward with the packet with one-way chained encoded. After getting S_{ij} for j=1……..k. Then n1 extracts Si and T2i from the decoded text. It stores r1=H1 (pi) and Si in its proof of receiving database. The database is maintained by each one node by FIFO basis. Finally n_i assembles p_i ‖ T_{2i} into one packet and send this to node. In the parity test n, marks the debit of pi in its proof of receiving database and doesn't transmit packet to n_2. The same step is repeated at every common node.

6.2.1.2 Auditor

When the auditor accept the ADR request from the sender "S" it starts is auditing progress. The ADR request consists of the id of the nodes, HLA public basic information p_k= (v, g, u) and the arrangement number of the packet send from S and the sequence number of the subgroup of this M packets are received by D. Ad conducts auditing process as follows. Ad submits a random challenge vector c_j = (c_{j1}…….c_{jm}) to node n_j. The arrangement number of packets in the current proof of receiving database from p_1……p_m. Where pm is the most sent packets by S. Depending simultaneous this information the node n_j generates the packet reception bitmap b_j = (b_{ji}……b_{jm}). Where b_{ji}=1 if P has been collected by and b_{ji}=0. Node nj calculates n_j= Σim=, bji#0 $c_{ji}r_i$ and the HLA signature S_j=Π_i=1, Sjibji#0 c_{ji}……. [2] Node n submits b_j, r (j) and S (j) to Ad as a proof of packet it is collected.

6.2.1.3 Receiver

The packets sent by the sender are gathered by the receiver. If the receiver doesn't receive the packet it sends an information message to the sender.

7 CONCLUSION

In this paper correlation of lost packet is correctly computed. To ensure the truthfulness of instruction send by the nodes HLA placed auditing architecture is used to present privacy preserving collision avoidance and low communication storage uppers. Development to productive surroundings will be studied in our future work.

REFERENCES

[**1**] 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.

[2] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[3] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
ET)
Vol. 3, Special Issue 2, March 2016

[4] A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.

[6] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z.Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[7] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput., vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012.

[8] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept