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

SECURE AUDITING AND TRUTHFUL DETECTION IN WANET

*S.K. Abincy**R.Bhavana Selvi***M.Dharani
Vins Christian Women's College Of Engineering
abincysk26@gmail.com,bhavanravir@gmail.com,madharanii@gmail.com

***ABSTRACT* - A homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. To reduce the computation overhead, a packet-block-based mechanism is proposed, which allows one to trade detection accuracy for lower computation complexity.**

Keywords—Packet dropping, secure routing, attack detection, homomorphic linear signature, auditing.

I. INTRODUCTION

In a multi-hop wireless network intermediate nodes are used to send the packet from source to destination they are considered as cooperative nodes. Insider attack- In the route discovery process adversary node pretends as a cooperative node and drops the packet. The malicious node has the capability to evaluate and drop highly sensitive packet which affect the operation of the network. Link error between the nodes also cause packet drop.

To overcome the above problems we introduce an accurate algorithm auto-correlation and an auditor HLA (Homomorphic Linear Authenticator) for truthful detection. Bitmap—lost/received status of each packet in transmission is described by bit map. Correlation between the lost packets decides whether the packet loss is due to link error or combination of link error and the malicious drop. HLA is a public auditor which is basically a signature scheme and it is efficient and promising algorithm for detecting the malicious node.

This construction is privacy preserving, collusion proof, and incurs low communication and storage overhead.

Privacy preserving: HLA should not able to access the content of the packet when auditing the node in the network. Only the packet delivery information from the nodes must be accessed by the HLA not the content.

Collusion proof: Content of the packet can't access by the adversary even though the adversary is collude with malicious node in the path. Construction is secure because there is no collusion between the attackers (i.e.) the information about the HLA signature is not given to the attacker by malicious node even it is collude with each other in the network.

Low communication and storage overhead: This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue. Last, to significantly reduce the computation overhead of the baseline constructions so that they can be used in computation-constrained mobile devices, a packet-block-based algorithm is proposed to achieves scalable signature generation and detection. This mechanism allows one to trade detection accuracy for lower computation complexity.

II. RELATED WORKS

Related works are classified into two categories. In the first one the packet lost is due to malicious dropping and it ignores link errors. It is classified into four sub-categories.

a. Credit system— a node that relay packet for other nodes receive credit from credit system and it use that credit to send its own packet. But the malicious node can't send its own packet due to the absence of credit.
b. Reputation system—Identification of malicious node is depending on the neighbouring node.
c. Acknowledgement based—Hop-to-hop acknowledgement locates the hop where packets are lost and remove that hop.
d. Cryptographic method—Bloom filter used to identify the hop that drop the packet.

In the second category the packet loss is due to malicious dropping and link error but the loss of packet by malicious dropping is higher than the link error.

III. System models and problem statement

A. Network and channel model

The source selects the route by Dynamic Source Routing or trace route operation to send packet to the destination. A common key is used by all the cooperative nodes for encryption and decryption at the routing process. Source sends the

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

encrypted hello packet to one of the neighbouring node and the node that receive the packet will decrypt the packet by common key and send to the source, if it is same then the source send the original packet to the next node. Likewise each node tests the neighbouring node to select the route to destination.

Advanced Encryption Standard (AES) is a symmetric encryption standard used to encrypt and decrypt the original packet by source and destination. Four stages are takes place in AES that are,

Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

B. Adversarial model

Malicious nodes are the main reason for packet dropping and it has the capability to hide from the auditor by the help of covert channel. Covert channel—channel that used to send the packet between malicious nodes.

C. Problem statement

Dropping of packet is the problem in network to overcome this auditor is used. Initially the auditor doesn't have the idea about nodes. When auditor receive request from source it enquire the nodes in the route about the transmission but the information in the packet should not be viewed by the auditor it must be privacy preserved.

IV. PROPOSED DETECTION SCHEME

A. Overview

Correlation between the lost packets is used to find out whether packet loss is due link error or the combination of the link error and malicious dropping. 0 and 1 are bits used to denote the loss and receive state of the packet. 0 denotes that the packet is loosed and 1 denotes that the packet is received. Bitmap is used by the auto-correlation function to get the detail from each node about the loss/receive state of packet.

B. Scheme details

1. Setup phase

Before transmitting the packet it must be encrypted. AES algorithm is used to encrypt the packet which is used by source and in destination side the packet is decrypted by means of same algorithm. There are basically ten rounds in AES each round consists of four stages (SubBytes, ShiftRows, MixColumns and AddRoundKey). Both source and destination side first stage is add round key. In all the four stages only the add round key stage uses the key. In tenth round of encryption and decryption mix column stage does not take place. Each add round key consists of 128bit (4 words).

2. Packet transmission phase

Encrypted packet is transmitted from the source to destination by the help of intermediate node. A common key is used by all the cooperative nodes for encryption and decryption at the routing process. Source sends the encrypted hello packet to one of the neighboring node and the node that receive the packet will decrypt the packet by common key and send to the source, if it is same then the source send the original packet to the next node. Likewise each node tests the neighboring node to select the route to destination.

3. Audit phase

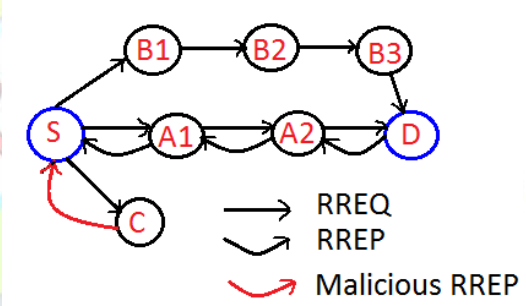

Fig. Independent auditing

An independent auditor Ad in the network it is independent in the sense that it is not associated with any node in P_{SD}. The auditor is responsible for detecting malicious nodes on demand. S encrypts the packets and sent through the route to destination. Destination after receiving packets can verify the packet and after verification it can decrypt the packets. Assume 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. Ad needs to collect certain information from the nodes on route P_{SD}. Adhoc On Demand Vector (AODV) protocol is used for the direct communication between source and destination.

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 request from source to auditor consists of id of nodes in the path, ordered in the downstream direction, source's public key information, sequence numbers of packet recently sent by source, and the sequence number of the packets that were received by destination.

The source broadcasts a RREQ message with unique identifier to all its one hop neighbors. Each receiver rebroadcasts this message to its one hop neighbors until it reaches the destination. RREP message back to its neighbor which relayed the RREQ. C is a malicious node intending to drop packets from S to D. S first broadcasts RREQ packet to its neighbors. Each neighboring node continues to rebroadcast this message. The malicious node C lies to S claiming it has the shortest path to D and sends a RREP packet to S.

4. Detection phase

HLA is the auditor used to detect the node that loss the packet. Auto-correlation is the concept used by the HLA to detect which node is the malicious node. When the destination thinks that there is a problem in receiving packet (i.e.) if it not receives the packet at specified time then it send message to the source about the problem and source sent packet to HLA. HLA check each node in the route by asking about the packet delivery details and which is privacy preserving (i.e.) only the detail of packet delivery is viewed by the HLA not the content inside the packet.

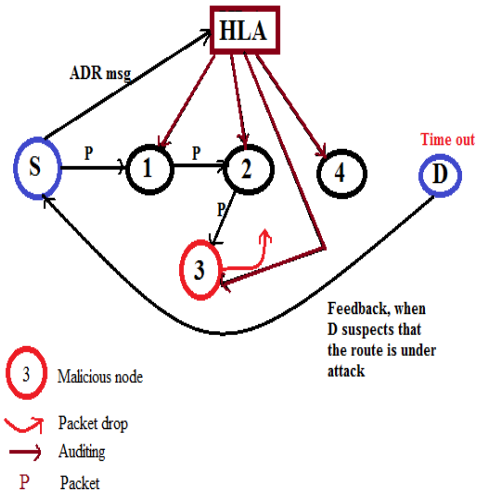

Fig. Detection phase

C. Security analysis

HLA is publically verifiable and privacy preserving (i.e.) to verify a nodes response the auditor does not require the secret key of HLA. Christo Ananth et al. [8] 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.Source distribute HLA signature to the nodes on the path this indicates the upstream node can't get the copy of the HLA signature of the downstream node.

D. Overhead analysis

1. Computation requirements

In source node and public auditor computation takes place but here in the public auditor side computation overhead does not takes place much because it is a dedicated service provider. But in source node computation overhead takes place because source has to generate HLA signature for all the nodes for each data packet. To overcome this block-based HLA signature and detection mechanism is used.

2. Communication overhead

Communication overhead takes place in packet transmission and auditing phase. In packet transmission phase communication overhead for transmitting a packet is 44L bytes and in auditing phase 320+M bits.

3. Storage overhead

The storage overhead at each node is 320M+56 bits, or 40M+7 bytes. Here the intermediate node just sends the packet from one node to another and it doesn't store the packet data so the storage overhead gets reduced.

V. REDUCING COMPUTATION OVERHEAD

Block-Based HLA signature generation and detection

To reduce the computation overhead, Block-Based HLA signature is used. The source generates the HLA signature for each packet and each node this leads to computation overhead. To reduce this

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 some set of packets are consider as block and for each block the HLA signature is generated, this reduce the computation overhead.

For detection purpose bit map concept is used. From each block bit map detail is received by the HLA in which 1 represent that the block is received and 0 represent the block is not received yet.

VI. CONCLUSION

HLA is used to detect the nodes that cause the packet drop. Auto-correlation concept is used by HLA to detect the malicious nodes. Packet dropping is due to link error or the combination of link error and malicious dropping is also identified by HLA. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead , a packet-block-based mechanism is proposed, which allows one to trade detection accuracy for lower computation complexity.

REFERENCES

[1] 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

[2] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, ―An acknowledgement- based approach for the detection of routing misbehaviour in MANETs,‖ IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

[3] W. Kozma Jr. and L. Lazos, ―Dealing with liars: Misbehavior identification via Renyi-Ulam games,‖ presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.

[4] Y. Zhang, L. Lazos, and W. Kozma, ―AMD: Audit-based misbehaviour detection in wireless ad hoc networks,‖ IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.

[5] Proano and L. Lazos, ―Selective jamming attacks in wireless networks,‖ in Proc. IEEE ICC Conf., 2010, pp. 1–6.

[6] T. Shu, M. Krunz, and S. Liu, ―Secure data collection in wireless sensor networks using randomized dispersive routes,‖ IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[7] 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] 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).

[9] 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.

[10] R. Rao and G. Kesidis, ―Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited,‖ in Proc. IEEE GLOBECOM Conf., 2003, pp. 2957–2961.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, ―The feasibility of launching and detecting jamming attacks in wireless networks,‖ in Proc. ACM MobiHoc Conf., 2005, pp. 46–57.

[12] T. Shu, S. Liu, and M. Krunz, ―Secure data collection in wireless sensor networks using randomized dispersive routes,‖ in Proc. IEEE INFOCOM Conf., 2009, pp. 2846–2850.

[13] H. Shacham and B. Waters, ―Compact proofs of retrievability,‖ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Dec. 2008, pp. 90–107.

[14] G. Noubir and G. Lin, ―Low-power DoS attacks in data wireless lans and countermeasures,‖ ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, no. 3, pp. 29–30, Jul. 2003.

[15] 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.

[16] V. N. Padmanabhan and D. R. Simon, ―Secure traceroute to detect faulty or malicious routing,‖ in Proc. ACM SIGCOMM Conf., 2003, pp. 77–82.

[17] P. Papadimitratos and Z. Haas, ―Secure message transmission in mobile ad hoc networks,‖ Ad Hoc Netw., vol. 1, no. 1, pp. 193–209, 2003.