Signature based Detection of Dropping Attacks in a Wireless Ad Hoc Networks

Sangeetha M S
M. Tech Student
Department of Computer Science and Engineering
Sarabhai Institute of Science and technology
Vellanad, Trivandrum, India

Sumitha Valsalam
Assistant Professor
Department of Computer Science and Engineering
Sarabhai Institute of Science and technology
Vellanad, Trivandrum, India

***Abstract*—In a multi-hop wireless ad hoc network link error and malicious packet dropping are two sources for packet losses. It is very important to find whether the losses are due to link errors only or is due to both link error and malicious packet drop i.e. the cause of packet loss. In this work the importance is given to the insider attack case where malicious nodes drops packets to degrade the network performance. Packet dropping rate in the insider attack case is approximately equal to normal link error because of which existing algorithms cannot find the exact cause of the packet loss. Thus truthful detection of packet dropping attack is very important. Thus in here the correlation between lost packets are found and to ensure that these correlations are correct an accurate public auditing mechanism called Homomorphic Linear Authenticator (HLA) is used which allows the detector to verify whether the packet loss information reported by various nodes are true or not. The proposed mechanisms achieve more detection accuracy than conventional methods. As an enhancement dynamic routing to provide secure communication between nodes and classification of packets to classify the packets is proposed to be implemented.**

Keywords—Malicious packet drop;homomorphic linear authenticator;auditing

I. INTRODUCTION

A wireless ad hoc network is characterized by the spontaneous self organization of a collection of nodes into a multi hop network in the absence of a particular infrastructure. In here nodes in the network rely on other nodes to forward and route data packets to the destination. The nodes in an ad hoc network communicate using wireless links where by nature vulnerable to channel errors and interference that may corrupt some or many data packets. In a malicious packet drop attack the malicious node first pretend to be a cooperative node in the route discovery process, after becoming the part of the route it can exploit the knowledge of the network protocol and the communication context to launch insider attack.

In many case the malicious node stops forwarding every packet received from upstream nodes and completely disrupting the route between source and destination. So it is very important to find the cause of the packet loss. Detecting malicious selective packet dropping is extremely challenging in a highly dynamic wireless environment. The difficulty comes when it is needed to not only detect the location where the packet drop took place, but also identify whether the drop is intentional or not. Specifically, because of the open nature of the wireless network. As a result, a packet drop in the route could be caused due to harsh channel conditions. In this case, observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss, because the packet drop rate by the malicious node is approximately comparable to that of wireless link errors. Clearly, deciding whether a packet drop is intentional or unintentional is a challenging problem.

In here an accurate algorithm is being developed for detecting the selective packet drops made by malicious nodes. The high detection accuracy is achieved by exploiting the correlation between the lost packets by using a bit map reported by nodes. Some malicious nodes which is a part of the network may give false information regarding the packet reception so auditing of such information for truthful verification is required. So a public auditing mechanism called Homomorphic Linear Authenticator (HLA) cryptographic primitive is being used..

The remaining paper is organized as follows. Section II discusses related works .In section III, the proposed system has been described which includes architectural design. Section IV includes implementation details of the proposed system. Section V summarizes the contents of the paper.

II. RELATED WORKS

In recent years many works has been done in the area of detecting packet drop attack in a wireless ad hoc networks. In [2] a reputation-based scheme named Watchdog that helps to detect misbehaving nodes and enhance the throughput of network with the presence of malicious nodes was proposed. The Watchdog scheme consisted of two different parts: they are Watchdog and Path rater. Watchdog serves as an ID for MANETs and it is responsible for detecting the misbehaving malicious node in the network. Watchdog detects the malicious misbehaving by listening to its next hop's transmission. Whenever a node's failure counter exceeds the predefined threshold value, the Watchdog node informs it as misbehaving node. In this case, the path rater will cooperate with the routing protocols to avoid the reported nodes in future transmission.

In [3] the authors proposed two network layer acknowledgment based scheme termed the TWOACK and the S-TWOACK schemes, which can be added on to any source routing protocol. When a node forwards a packet the nodes routing agent verifies whether the packet forwarded is successfully received by the node that is two hop away from

the source route by using a acknowledgment packet called TWOACK packet. A node acknowledge the receipt of a data packet by sending back a two-hop TWOACK packet through the path. If the sender of a data packet does not receive a TWOACK packet corresponding to a particular data packet that was sent out, the next hop forwarding link is claimed to be misbehaving and the forwarding route broken. The Selective-TWOACK (S-TWOACK) scheme is a derivative of TWOACK scheme.In the S-TWOACK scheme, instead of sending TWOACK packet for every packet that is received when a data packet is received, a node waits until a certain number of data packets arrive. The node then sends back one TWOACK packet for multiple data packets that it has received.

In [4] the authors proposed a novel misbehaviour identification scheme called REAct. It investigates the problem of uniquely identifying the set of misbehaving nodes who refuse to forward packets. The identification of misbehaving nodes is based on a series of random audits triggered upon a performance drop is done in REAct. The source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioural proofs provided by nodes. Proofs are constructed using Bloom filters which are storage efficient membership structures, thus significantly reducing the communication overhead for misbehaviour detection.

In [5] the authors proposed a new method to prevent the selective jamming attack in a internal thread model. The wormhole which will generate an alarm to indicate the presence of jammer and sent IP address of jammer node to all other nodes in the network being used. Messages can be send through the network even though a jammer is present by using packet hiding. The technique called Strong Hiding Commitment Scheme (SHCS) is used for this. This technique is based on symmetric cryptography. First, the sender s has a packet 'P' for a particular receiver r. First step in SHCS is applying a permutation on packet P. Then encrypt the corresponding permuted packet with a random key. Here the Advanced Encryption Standard (AES) technique can be applied. Now the encrypted value is broadcast to all nodes. Thus an attacker within the wireless network can't identify the source of incoming packet, because the packet is encrypted. Here, the wormhole becomes the access point in a network region whenever it finds out any node that violates the rules in a particular network region. Such node is then considered as a jammer node Wormhole sends IP address of jammer to all other nodes. Thus the prevention of the jamming activity of the jammer is done by wormhole, by encrypting the source ID of message along with the message packet. By doing so jammer is unable to identify its target node and the sender node can forward its message safely through jammer node itself.

In [6] the authors proposed a comprehensive system named Audit-based Misbehavior Detection (AMD) system.The AMD system was developed for detecting and isolating misbehaving nodes. In AMD misbehaving nodes are isolated by implementing a reputation based system. Nodes with low reputation values are not included in the routing paths, thus being unable to drop transit traffic. The reputation module is responsible for managing and computing the reputation of the nodes. A decentralized approach in which each node maintains its own view of the reputation of other nodes is used. Such implementation alleviates the communication overhead for transmitting to a centralized location, and readily translates to the distributed nature of ad hoc networks. Moreover, it allows nodes to hold their own reputation metrics for their peers depending on their direct and indirect interactions. Once the source has converged to a misbehaving link it can no longer proceed to identify the misbehaving node. To isolate the misbehaving node, the ideas of path division and path expansion is being used.

The work proposed by this paper is to create a auditing mechanism based on Homomorphic linear authenticator(HLA) cryptographic primitive in order to verify the truthfulness of the reported information. And to provide a non predefined routing a routing protocol is used to provide more security.

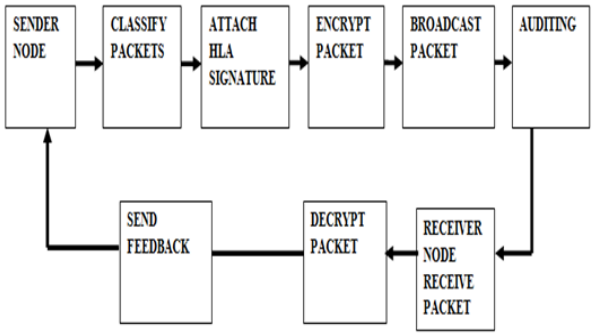

Figure 1: Architecture design of truthful detection of dropping attack

In here the sender node first classify the packets to be send and before sending the packets the sender create HLA signature for each packet and attach it to each packet and then encrypt it. Then these packet is send along the route. At the receiver side the receiver will decrypt the packet received and it will send the feedback to the sender. And if it report that the route is under attack then the sender will send a ADR request to the auditor and auditor will perform some testing to find the malicious node in the network.

IV. IMPLEMENTATION

Homomorphic linear authenticator[1] is being used here in order to provide a truthful verification for the packet reception status reported by individual nodes. And ALERT routing protocol is being used for routing.

4.1.Packet monitoring

Packet monitoring takes place after network monitoring. Network monitoring refers to the practice of overseeing the operation of a computer network using specialized management software tools. Packet monitoring is done to monitor the packets in the network and to classify them.

4.2.Packet transmission

In here the source node continuously sends packets to the destination node D through intermediate nodes ni....nk, where n is the upstream node of n+1,for 1<=i<=k-1.Before sending the packet S decides on a symmetric crypto system (encrypt key,decrypt key) and k symmetric keys key1 .....key k where encrypt key and decrypt key are the keyed encryption and decryption functions. S securely distribute decrypt key and a symmetric key key j to the node nj on the path.

Key distribution may be based on a public key crypto system such as RSA: S encrypts key using the public key to obtain key j. S also announces two hash functions to all nodes in the path.Besides the symmetric key distribution S also needs to set up its HLA keys.Then S transmits packets to the path according to the fllowing steps:

Before sending out a packet Pi,S computes r i=H 1(P i) and generates the HLA signatures of r i for node nj as follows:

$$sji = [H2(i||j)u^{ri}]^{x}, \text{ for j= 1.....K}$$

Where || denotes concatenation

These signatures are sent together with P i to the route by using one way chained encryption ,after getting Sji for j= 1….k ,S iteratively computes the following:

$$s\tilde{}Ki = encrypt\ (s\ Ki)$$
$$\tau\ Ki = s\tilde{}Ki\ ||MAC\ keyK(s\tilde{}Ki)$$
$$s\tilde{}K-1i = encrypt\ keyK-1(s\ K-1i||\tau\ Ki)$$
$$\tau\ K-1i = s\tilde{}K-1i||MAC\ keyK-1(s\tilde{}K-1i)$$

.

.

.

.

$$s\tilde{}ji = encrypt\ keyj\ (s\ ji\ ||\tau\ j+1)$$
$$\tau ji = s\tilde{}ji\ ||MAC\ keyj(s\tilde{}ji)$$

.

.

.

$$s\tilde{}1i = encrypt\ key1(s1i||\tau 2i)$$
$$\tau 1i = s\tilde{}1i||MAC\ key1(s\tilde{}1i)$$

Here the MAC in each stage j is computed according to the hash function. After getting τ 1i, S puts Pi || τ 1i into one packet and sends it to node n1.W hen node n 1 receives the packet from S, it extracts Pi,$s\tilde{}1i$ and MAC key1($s\tilde{}1i$) from the received packet. Then n1 verifies the integrity of $s\tilde{}1i$ by testing the following equality:

$$MAC\ key1(s\tilde{}1i = H^{MAC}_{key1}(s\tilde{}1i)$$

If the test is true then n 1 decrypts $s\tilde{}1i$ as follows:

$$decrypt\ key1(s\tilde{}1i) = s1i||\tau 2i$$

Then n1 extracts s1i and τ 2i from the decrypted text. It stores r i = H 1(P i) and s1i in its proof of reception database for future use. Finally n1 assembles Pi || τ 2i and relays this packet to node n2.If the above equality test fails n1 marks the loss of Pi in its proof of reception database and do not relay packet to n2 .The above process is repeated at every intermediate node n j, j=1….K. As a result, node nj obtains r i and its HLA signature s ji for every packet Pi that the node has received and it relays Pi || τ j+1i to the next hop on the route. In the last hop i.e., node n k only forwards Pi to the destination D here one way chained encryption is being used. Here the verification of Pi also occurs if it fails then node n1 should also stop forwarding the packets and should mark it accordingly in its proof of reception database.

4.3 Auditing

In here the auditing is done by the independent auditor Ad when it receives an ADR message from the S.S send a ADR message to the auditor only when it gets a feedback from the destination. Ad conducts the auditing process as follows: Ad submits a random challenge vector $c\vec{}j = (cj1 \ldots . cjM)$ to node nj, j=1….k.Let P1…..PM denotes the sequence number of the packets recorded in the current proof of reception database. PM the most recent packet sent by S.Based on the information in this database node nj generates a packet reception bitmap $b\vec{}j = (bj1..bjM)$ if b ji= 1 then it denotes that the packet has been received by nj and b ji = 0 otherwise. Node n j calculates the linear combination $r^{(j)} = \sum_{i=1}^{M} bji \neq 0\ c\ ji\ ri$ and HLA signature for the combination as follows:

$$s^{(j)} = \prod_{i=1, b\neq 0} s_{ji}^{cji}$$

Node nj submits $b\vec{}j$, $r^{(j)}$ and $s^{(j)}$ to Ad as proof of the packet it has received. Then Ad checks the validity of $r^{(j)}$ and $s^{(j)}$ by testing the following equality:

$$e(s^{(j)}, g) = e(\prod_{i=1,bji\neq 0}^{M} H2(i||j)^{cji} u^{r(j)}, v)$$

If the equality holds then Ad accepts that node nj received the packets as given in $b\vec{}j$.Otherwise Ad rejects $b\vec{}j$ and judges that not all packets claimed in the bitmap are actually received by nj, so n j is a malicious node.

4.4 Packet drop detection.

The auditor enters the detection phase after receiving and auditing the reply to its challenges from all nodes on the path. The main tasks of auditor in here include detecting any overstatement of packet loss at each hop, calculating the autocorrelation function for the packet loss on each hop, deciding whether malicious behavior is present or not.

First the consistency of the bitmaps for any possible overstatement is being checked, if there is no overstatement of packet loss, then the set of packets received at node j + 1 should be a subset of the packets received at node j, for j = 1.....K-1. Because a normal node always truthfully reports its packet reception, the packet-reception bitmap of a malicious node that overstates its packet loss must contradict with the bitmap of a normal downstream node. There is

always at least one normal downstream node, i.e., the destination D. So Ad only needs to sequentially scan the bitmap and the report from D to identify nodes that are overstating their packet losses.

After checking for the consistency of b^j ,Ad starts constructing the per-hop packet-loss bitmap mj from $b^{\rightarrow}j-1$ and $b^{\rightarrow}j$.This is done sequentially starting from the first hop from S. In each step only packets that are lost in the current hop will be accounted for in m j. The packets that were not received by upstream node will be marked as not lost for underlying hop. Denoting the lost packets by 0 and not lost by 1. $m^{\rightarrow}j$ can be calculated by conducting a bit wise complement XOR operation of $b^{\rightarrow}j-1$ and $b^{\rightarrow}$.

The auditor calculates the autocorrelation function ϒj for each sequence $m^{\rightarrow}j=(m\,j1\ldots\ldots mjM)$ from j=1…k as follows:

$$\text{?j(i)} = \frac{\left(\sum_{k=1}^{M-i} mjk\ mjk+1\right)}{M-i}\text{,For i=0.....M-1,j=1.....K}$$

The auditor then calculates the relative difference between ϒj and the ACF of the wireless channel *f*c as follows:

$$\in j = \sum_{i=0}^{M-1}(|\ \text{ϒj(i)-}\ f\text{c(i)}|\ )\ /\ f\text{c(i)}$$

The relative difference $\in j$ is then used as the decision statistics to decide whether or not the packet loss over the hop is caused by malicious dropIn such situation the malicious node will be marked and excluded from the route to mitigate its damages.

4.5 Routing

In here the ALERT routing protocol is used to provide unpredictable routing path, i.e; the routes will not be predefined. First the given network area is divided into two as horizontal or vertical zones. Then again split every partition into two zones as horizontally or vertically. This process called as hierarchical zone partition. After a node is randomly selected in each zone at each step as an intermediate relay node in this way unpredictable routing path is created dynamically. For successful routing between source and destination some information is needed, which is embed in the packet by source and each packet forwarder node. In the destination zone data will be holded only by receiver node other nodes will release the data.

V .CONCLUSION

This paper is based on homorphic linear authenticator.This auditing mechanism helps in verifying the truthfulness of reception status reported by individual nodes and helps in correctly identifying the malicious node in the network.And ALERT routing protocol is being used to provide secure routing.

VI.ACKNOWLEDGMENT

I would like to express my sincere gratitude to Dr. C.G. Sukumaran Nair (HOD), Associate Professor, Ms. Sudha S.K. and Assistant Professor, Mrs. Sumitha Valsalam., Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, for their valuable guidance.

VII.REFERENCES

[1] Tao Shu and Marwan Krunz "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless AdHoc Networks" IEEE Transactions on Mobile Computing Vol.14,No.4 April 2015
[2] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), August 2000
[3] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137– 2142
[4] 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
[5] Divya Ann Luke, Dr. Jayasudha. J .S," SELECTIVE JAMMING ATTACK PREVENTION BASED ON PACKET HIDING METHODS AND WORMHOLES" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014
[6] Yu Zhang, Loukas Lazos, Member, IEEE, and William Jr. Kozma" AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks" IEEE Transactions on Mobile computing Volume: PP, 2013
[7] A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.
[8] Weichao Wang ,Bharat Bhargava Mark Linderman," Defending against Collaborative Packet Drop Attacks on MANETs",2009