International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

HLA Based Public Auditing Architecture for Wireless Ad hoc Networks

*YOUSUF ANEESA **B.RAJITHA

*M.TECH student , Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING
**Assistant Professor, Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING

ABSTRACT

There are two sources for packet loss i. e link error and malicious packet dropping. It is important to find whether the losses are due to link errors only or is due to both link error and malicious packet drop. Here, I am mainly interested in the insider attack case where malicious nodes drops packets selectively to degrade the network performance. Packet dropping rate in the insider attack case is nearly equal to normal link error because of which existing algorithms cannot find the exact cause of the packet loss. I am going to find the correlation between lost packets and to ensure that these correlations are accurate i am going to use Homomorphism Linear Authenticator (HLA) based public auditing mechanism.

Keywords— Packet loss, Truthful detection, Homomorphism Linear Authenticator, Malicious node, Cryptography.

1. INTRODUCTION

In a multi-hop wireless network, nodes help to transfer packets from source to destination. Malicious node when added into a network, first it works in a cooperative way when finding the route from source to destination and when added into the rout e, the node starts to drop the packets i.e it stops forwarding almost all the packets t hat are received from its upstream node. This type of dropping is called as persistent packet dropping. This type of dropping completely lowers the performance of the network. It is easy to find this type of dropping because here most of the packets are dropped. There is another type in the packet dropping which is called as selective

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

packet dropping. Here attacker node calculates the importance of various packets and will drop only those packets that are very important. This also lowers the performance of the network as in persistent attack case. Here the probability of getting detected is very low when compared to persistent packet dropping. In this paper I am mainly interested in finding this type of dropping. It is very difficult to detect the position of selective packet dropping and also to identify whether the packet loss is intentional or unintentional. Intentional packet dropping is because of attacker's node and unintentional packet dropping is because of harsh channel conditions. Usually link errors exist in the open environment so the attacker will make use of harsh channel condition to drop the small amount of packets. Here just by observing packet loss it is not possible to find the real culprit for the packet loss. The packet dropp ing rate should be greater than the link error for the accurate detection. In this paper accurate algorithm is developed to detect the malicious packet drop. Here detection accuracy is very high which is achieved by finding the correlation of lost packets which is obtained by using the bitmap of packet reception provided by each node. By finding correlation between lost packets we can find whether packet loss is only because of link error or is the effect of combination of both link error and malicious packet drop bec ause both correlation gives different patterns for packet loss as shown in figure 1.In the figure the simulation of autocorrelation of two different packet loss process is given. The packet loss in one process is caused by 10% of link error and in another process packet loss is caused by 10% of link error and 10% of malicious packet dropping.

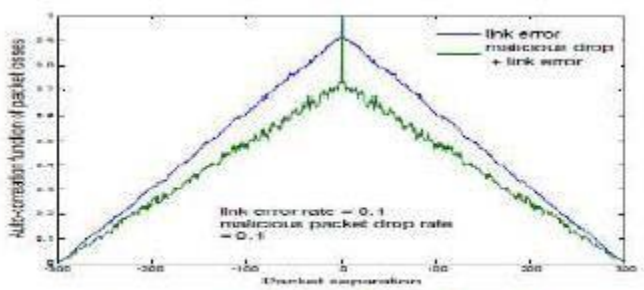

Fig.1 comparison of correlation of lost packets

To find whether the information provided by each node is true or not, i make use of HLA cryptographic primitive in which we will first generate the signatures and those signatures are added attached to the packet and sent to the destination. If any node in the network is dropping the packet then it will

lose the signature and at the time of verification the node could not send the signature to the auditor hence the malicious node can be easily detected. There is another advantage in this method that instead of adding one signature to one packet we can make a block of packets and put the signatur e to this block. By doing thiswe can reduce the overhead. This mechanism provides some extra features which include privacy preservation and low overheads between the intermediate nodes. Privacy preservation means the auditor cannot get the information sent through the packets.

2. EXISTING SYSTEM

The existing system can be broadly classified into two categories. The first category is having those systems that has high malicious dropping rate where almost all packets are dropped because of malicious packet dropping. Here the link errors are neglected. This category is classified into four sub-categories where each sub-category works depending upon some system.

The four systems for four sub-categories are as follows

1) Credit system

2) Reputation system

3) End-to-end or hop-to-hop acknowledgement

4) Usage of cryptographic primitive methods

All the systems works as follows:

1) Credit system: In this type of system, a node receives credit by sending packets for other nodes. These credits are used by nodes to send its own packets. If a malicious node is continuously dropping the packets then it will lose credits and it cannot send its own traffic.

2) Reputation system: Here the system depends on neighbour nodes to identify the malicious node. A node which drops most of the packets will get a bad reputation by its neighbour node. This information is passed to all the nodes in the network and is used to select routes for the next packet transmission. A high packet dropping node is eliminated from the routes.

3) End-to-end or hop-to-hop acknowledgement: Here end-to-end or hop-to-hop acknowledgements are used to find the hops where packet loss is present. A hop that high packet dropping rate is eliminated from the route.

4) Usage of cryptographic primitive methods: This type is used to construct the proofs for the forwarding of received packet at each node.

The second category is having high malicious packet dropping rate than the link errors, but here effect of link error is not neglected. Here source traffic rate and estimated received rate are calculated and are compared with each other. If the difference between these two is within a range then packet dropping is becau se of link errors and if the range is high then packet dropping is because of malicious node. There is another method to find the malicious node which is called as Maximum-Likelihood algorithm. Here a hypothesis test is considered known as binary hypothesis test and here two hypothesis are considered. One is the hypothesis for the absence of malicious node in the link which is represented as H0 (loss of packets because of link errors) and another one is the hypothesis for the presence of malicious node in the link which is represented as H1 (loss of packet is because of both link error and malicious drop). Let z be the number of packet loss found during some interval of time t then, z = x for H0 where malicious nodes are absent z = x+y for H1 where malicious nodes are present where x and y are the number of packets lost because of link error and malicious drop respectively. Here x and y are random variables. The probability density function (pdf) of z conditioned on H0 and H1 can be given by h0(z) and h1(z) respectively as shown in figure 2(a) and 2(b). Considering the probabilities of H0 and H1 as 0.5 i. e Pr(H0)=0.5 and Pr(H1)=0.5 because the auditor is having no prior knowledge of distribution of H0 and H1. There are two other parameters called as probability of false alarm(Pfa) and probability of miss detection(Pmd). By considering both parameters the detection error can be calculated as Pde = 0.5(Pfa+Pmd) is the maximum likelihood(ML) algorithm if $z \leq$ zth, H0 will be accepted otherwise, H1 will be accepted Here zth is called as threshold which is obtained by the equation h0(zth)=h1(zth). The shaded regions for pfa and pmd are shown in figure 2(b). The disadvantage of this algorithm is for the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

smaller mean of y where h0(z) and h1(z) are not separated sufficiently. Because of this Pfa and Pmd is large leading to a large detection error. This means that when there is selective packet dropping, it is very difficult to find the malicious node.

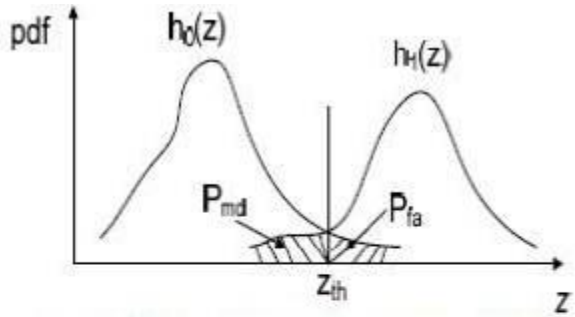

Fig.2 (a).mean of y is very large than mean of x

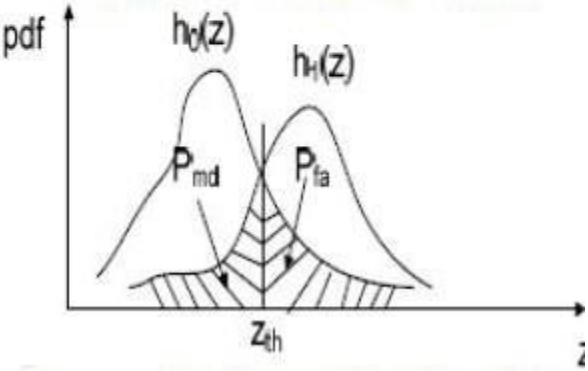

Fig.2 (b).mean of y is comparable with mean of x

Disadvantages of the existing system:

- In the credit system method, a malicious node will receive good number of credits by sending most of the packets that it receives from upstream nodes.
- In the reputation-based method, the malicious node is capable of maintaining a very good reputation by forwarding most of the packets to its neighbour node.
- The correctness of the packet forwarding proof of bloom filter is just probabilistic and it can have some errors.
- In the acknowledgement-based method and in all the methods in the second category, just by counting the number of packet loss we can find the real culprit which is causing packet loss.

3. PROPOSED SYSTEM

Consider a multi-hop network which is having an arbitrary path PSD as shown in figure 3. The source node sends the packets through intermediate nodes to the destination node. In each hop, the sending node is called as an upstream node of an receiving node. The packets are transmitted from source to destination and a bitmap is obtained for each node as (a1,a2….am) where aj=0 or 1. If the packet is successfully transmitted then aj=1 and if the packet is not transmitted the value of aj is considered as

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

0. By using this bitmap we can find the correlation between the lost packets. From this correlation we can find the malicious node

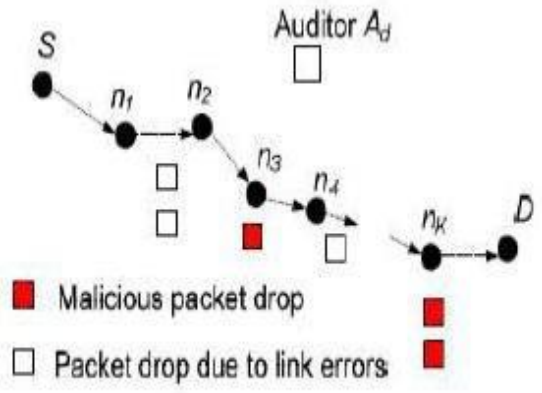

Fig.3 Network and attack model

There is an auditor in the network which is independent. The meaning of independent is that it is not related with any of the nodes in the network and it doesn't know about the secrets associated with the nodes. Here auditor is capable of detecting attacker's node when it gets request from the source. After sending all the packets from source to destination, the destination sends a feedback to source about the route i.e whether the route is under attack or not by considering some parameters. After getting feedback, if the route seems to be under attack then source will send the attack detection request (ADR) to auditor. Now auditor starts investigation to find malicious node. The auditor requests certain information from the intermediate nodes. Here normal nodes reply with correct information and the malicious node try to cheat. Here each and every node must reply for the auditor request otherwise the node is considered to be misbehaving.

The main challenge here is for the guaranty of the information sent by the nodes to the auditor. The attacker usually sends the wrong information not to get detected. Sometimes the malicious node may drop the pa cket and will send that that the packet is transmitted. To overcome this problem we are using Homomorphic linear au thenticator (HLA) a cryptographic method which is used in cloud computing. In this type of scheme, source is allowed to generate the HLA signatures s 1,…,sM for M messages r1,…,rM. The source sends these signatures s i's and packets ri's along the route. The node will create a valid HLA signature if and only if it has received all the signatures. Since s i's and ri's are sent together, the reception of signatures ensure that all the packets are transmitted without getting dropped. In this way we can truthfully detect the malicious node.

This mechanism includes 4 phases

1) Setup phase: After the establishment of route, this phase takes place. It is before any packet is transmitted to the route. Source makes use some symmetric key cryptosystem to generate encryption, decryption and K number of symmetric keys for K intermediate nodes. Source uses encryption and decryption method to provide symmetric keys to the nodes.

2) Packet transmission phase: After the completion of setup phase, source generates signatures and add these signatures to the packets and send to the route. Each node stores signature for the proof of reception in its database for the future purpose.

3) Audit phase: This phase comes into picture when auditor receives ADR message from the source. Each node sends the bitmap of packet received and also the signature and it compares the signatures with the stored signatures. If it is correct then it will prove that node has received all the packets. Here node cannot tell that it has received a packet when it does not receive it.

4) Detection phase: The auditor goes for this phase after receiving reply from the nodes. First it checks for the overstatement of packet loss using the bitmap sent by the nodes. In the beginning per hop packet loss bitmap is calculated from one node to other node by applying the complement of XOR operation for the bitmap of two successive nodes. At last it calculates the autocorrelation to find whether there is malicious node in the network or not.

Advantages:

- High detection accuracy.
- Privacy Preserving: The public auditor should not be able to decern the content of a packet delivered on the route through auditing information submitted by individual hops.

Disadvantages:

- Due to signature generation overhead may be high.
- Data confidentiality will raise the issue in this work.

4. CONCLUSION AND FUTURE WORK

In this paper it can be seen that conventional method cannot provide satisfactory result when there is selective packet dropping. For the correct calculation of correlation

between lost packets, it is important to get truthful information about packet loss. So I propose an HLA based auditing mechanism that provides the truthfulness for the packet loss information provided by the intermediate nodes in the network. For the future work we can use different methods to generate keys for the generation of signatures to reduce the overhead and we can use some encryption method to obtain the data confidentiality. We can add one signature to the block of packets to the instead of adding one signature to one packet to reduce the overhead.

REFERENCES

[1] Tao Shu and Marwan Krunz "*Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks*" *IEEE Transactions on Mobile Computing DOI:10.1109/TMC.2014*

[2] K. Balakrishnan, J. Deng, and P. K. Varshney "*TWOACK: preventing selfishness in mobile ad hoc networks*" In *Proceedings of the IEEE WCNC Conference*, 2005.

[3] G. Ateniese, S. Kamara, and J. Katz " *Proofs of storage from homomorphic identification protocols*" In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2009.

[4] Q. He, D. Wu, and P. Khosla "*Sori: a secure and objective reputation based incentive scheme for ad hoc networks*" In *Proceedings of the IEEE WCNC Conference*, 2004.

[5] S. Zhong, J. Chen, and Y. R. Yang. "Sprite: a simple cheat -proof, credit based system for mobile ad-hoc networks" In *Proceedings of the IEEE INFOCOM Conference, pages* 1987–1997, 2003.

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

[7] 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.

[8] 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*

network s." In *Proceedings of the IEEE ICC Conference*, 2009.

[9] W. Kozma Jr. and L. Lazos. *"Dealing with liars: misbehavior identification via Renyi-Ulam games*." In *Proceedings of the International ICST Conference on Security and Privacy in Communication Networks (SecureComm)* , 2009.

[10] A. Proano and L. Lazos . *"Pack et-hiding methods for preventing selective jamming attack s." IEEE Transactions on Dependable and Secure Computing*, 9(1):101–114, 2012.

AUTHOR 1 :-

*Yousuf Aneesa completed her B tech in Jaya Institute of Technology and Science for Women in 2014 and pursuing M-Tech in Vaagdevi College of Engineering

AUTHOR 2:-

**B.Rajitha is working as Assistant Professor in Dept of CSE, Vaagdevi College of Engineering