RESEARCH ARTICLE OPEN ACCESS

Privacy Preserving and Detection of Packet Dropping Attacks in MANETS

Sonia Choudarygari, Penmatsa Naga Venkata Divya
Hyerbad – India

ABSTRACT
In mobile ad hoc networks providing privacy and maintaining the individual nodes is challenging because of node mobility and changing of topology in the networks. In this paper we are intended to provide the privacy and security to the data. Link errors and malicious packet droppings are the two sources for packet loss. Existing techniques uses cryptographic methods to record the forwarded packets to detect the packet loss but these are applicable only when the packets are highly selective. In this the link errors may not be significantly smaller than the packet dropping rate of the insider attack. So we proposed an accurate algorithm to detect the selective packet drops made by the insider attacks. We use a HLA (Homomorphic linear authenticator) based public auditing mechanism to detect the dropped packets. This algorithm is used to find the correlations between the packets. It provides a truthful and publicly verifiable decision statistics. We also use the ACF (auto-correlation function) to calculate the position of lost packets. This system with new HLA construction is collusion proof and incurs low communication cost.

Keywords:- Ad hoc networks, Link errors, packet dropping, secure routing, HLA, ACF, auditing.

I. INTRODUCTION

In multi-hop ad hoc networks nodes cooperate with each other for routing the information. They can send the sensitive data through the network. Under the network an attacker may exploit this cooperative nature of nodes and can make the attacks. This may cause the denial of service, packet droppings or any modification in the original content. Due to this type of attacks the user cannot send and receive the packets correctly. First the attacker act like a cooperative node in the route discovery process. Once being included in the route, he starts dropping the packets slowly. In most cases the malicious node simply stops forwarding the packets to the destination. Eventually such a Denial of Service attack can change the network by partitioning it into the topology. A malicious node that is a part of route can exploit its knowledge of network protocol and communication context to launch an attack. The persistent packet dropping can effectively degrade the performance of the network from the attackers point. First the continuous presence of the extremely high packet loss rate at the malicious node makes this type of attacks easy to be detected. Once the attack has been detected it is easy to remove the attacker.

II. ASSESSMENT ON PREVIOUS COLLECTION OF WORK

The related work can be classified into two following categories depending upon the weight of detection algorithm that gives to link errors relative to malicious packet droppings.

The first category assumes that the most of all the packets are lost due to the malicious dropping. In this case the impact of link errors is ignored. Most of the related work belongs to this category. The detection accuracy of malicious node can be done in some of the ways

1. The node will get a transmission point on sending the packets. It can lose its point whenever there is a packet loss.
2. Each node is taken care by the neighboring node so if any packet droppings occur then the neighboring node will monitor it. The malicious node is identified and removed from the network.
3. Some cryptographic methods are used to record the packet routing of forwarded messages.

The second category aims at the category where the malicious droppings are significantly higher than that caused by link errors. Here the impact of link errors is non-negligible. Certain knowledge on wireless channel is necessary here. The presence of malicious packet dropping attacks and link errors in the network will permanently disable the whole network topology. The existing system can detect and remove the attacks up to some extent and cannot remove completely.

All these methods are not performed well when the packet dropping is highly selective. Our study targets the challenging situation where link errors and malicious

dropping lead to comparable packet loss rates. The effort in the literature on this problem has been quite preliminary, and there is a few related works.

The most of the related works assumes that assumes that malicious dropping is the only source of packet dropping. In credit-system-based method, the malicious node may still receive enough credits by forwarding most of the packets that receives from the upstream nodes. In Bloom-filter scheme, it is able to provide a packet-forwarding proof. In reputation-based approach, the malicious node maintains the good reputation by forwarding most of packets to next node. As for the acknowledgement based method and all the methods of second category, counting the number of lost packets does not give sufficient information to detect the packet loss.

III. OBJECTIVE AND SCOPE

Our proposed project will detect and remove the malicious dropping rates and link errors. In order to detect the attack we are using the HLA mechanism to improve the network authentication rate and efficient detection of malicious node form the networks. Our proposed system forms a secure network with high throughput rate. The scope of the project is to maintain the same delay time in both the cases i.e, the packet dropping case and the normal case.

IV. PROBLEM STATEMENT

The goal of conflict model in the network degrades the performance by dropping the packets and some remain undetected. Here we address a problem of identifying the nodes on a route that drop the packets selectively and maliciously. The public auditor must perform the detection of that does not have knowledge of secrets held by the nodes on a particular route. The auditor must be able to construct a publicly-verifiable proof of the misbehavior of the node whenever a malicious node is identified. The construction must be collusion proof and privacy preserving that means it does not reveal the information that is transmitted on the route. In addition, the detection mechanism should incur low communication and storage overheads so that it can be applied to a wide variety of wireless networks.

From the network model we can determine the nodes on the routing path that causes the packet loss. This is carried out by the auditor who doesn't know any secrets above the node. When a particularly malicious node is identified, auditor provides a publicly verifiable proof which should be privacy preserving and should be low communication and storage overheads.

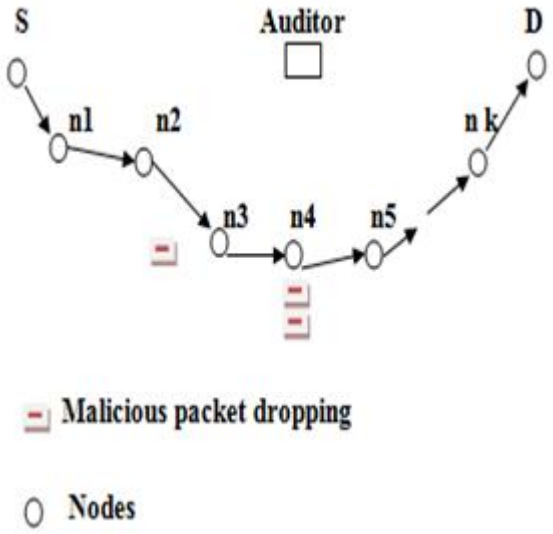

Fig1: Network Attack Model

V. PROPOSED SCHEME

In this proposed mechanism we are going to find the correlations between each lost packets. This can be achieved by auditing. The main challenge in our mechanism is how we can guarantee the packet loss bitmaps reported by individual nodes along the route are truthful. This can be done by using the HLA scheme which is basically a public auditing scheme that is widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients. The correlation of lost packets is calculated from the auto-correlation function.As shown in fig1, the source represented with S will send the nodes to the destination D. We are specifying the route. The intermediate nodes are represented with {n1, n2, n3….. nk}. The auditor is capable of identifying the traffic patterns and also to detect the lost packets. The packet loss can be either of the link errors or the node failure. Whenever the node failure occurs we will choose another neighboring node and send the packets to it. And in case of link error we will choose another link (path) and transmit the packets. Network coding has been shown to optimally use bandwidth in a network, maximizing information flow but the scheme is very inherently vulnerable to pollution attacks by malicious nodes in the network. A node which is malicious can quickly affect many receivers. The pollution of network packets spreads quickly since the output of

honest node is corrupted if at least one of the incoming packets is corrupted. The homomorphic property of the signatures allows nodes to sign any linear combination of the incoming packets without contacting the signing authority. In this scheme it is computationally infeasible for a node to sign a linear combination of the packets without disclosing what linear combination was used in the generation of the packet. In out model we are providing a threshold value let say x, if the value of x is less than the given threshold value then it is considered as a malicious node. And if the value is equal then we can say that the packet is reached successfully.

VI. System modules:

The system modules of proposed system includes the source , which is used to send the packets along with the destination address, the router which sets the threshold value to the given file and routes the packet to destination by measuring the shortest path between the source and destination, the auditor is responsible for identifying the traffic patterns and detect the malicious droppings to recover and resend the packets, the destination is the end user who receives the file without any lose of packets.

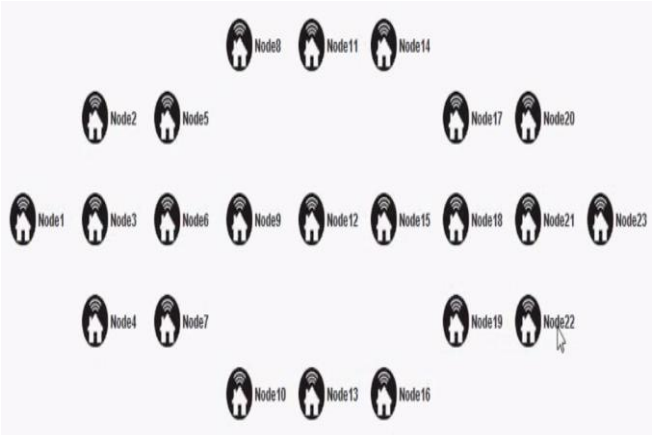

Fig2: Nodes in the ad hoc network

VII. SYSTEM DESIGN

In ad hoc networks many nodes are involved as shown in fig2, such that one cannot determine which node is malicious. The Auto correlation function is used to calculate the correlations between the nodes and can decide whether the attack is due to regular link errors or the combination of link and malicious droppings.

The HLA mechanism is used to detect the packet loses efficiently. In this mechanism we are finding the HLA signatures to each and every node along with the file. The HLA is used to find size of the given file. The HLA measures the size of the file along with the bandwidth or a threshold value. It selects the shortest distance between the neighboring nodes. Whenever we lose the packets due to malicious node the auditor can detect the traffic patterns and can recover by sending it again. It will stop the malicious node entering into the network.

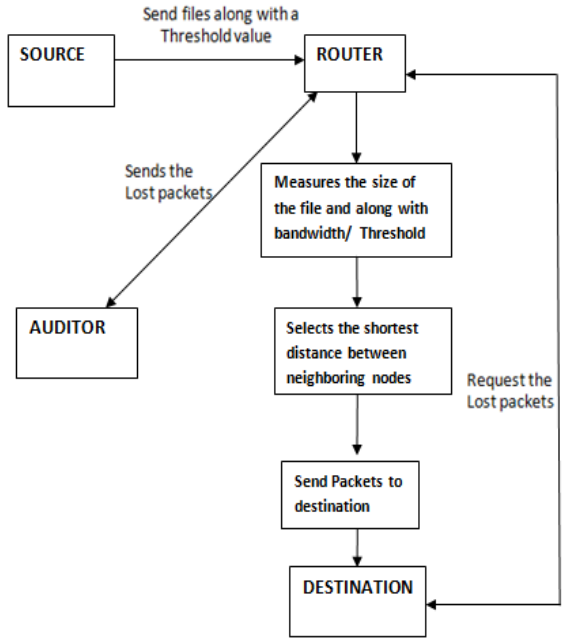

Fig3: DFD Diagram To Detect packet Dropping Attacks

VIII. SCREEN SHOTS

Step1: Fig4 describes the source node from which the data need to be sent. Here we need to browse the file to send and then intialise all the nodes. Now we can send data packets to the final destination. Even if any data get lost we can recover it.

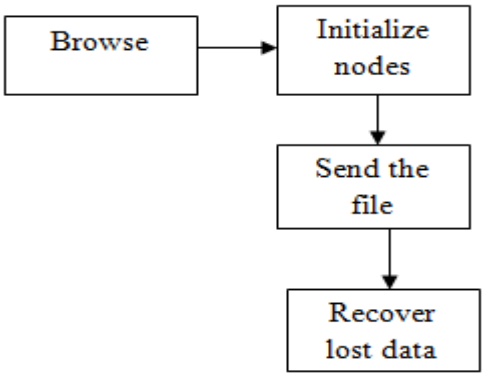

Fig4: Source Node

Step2: This figure shows the route path between the source and destination. This is a normal case when no attacker is involved in the route and the data is sent successfully to the destination by choosing the shortest path between them using the HLA mechanism.

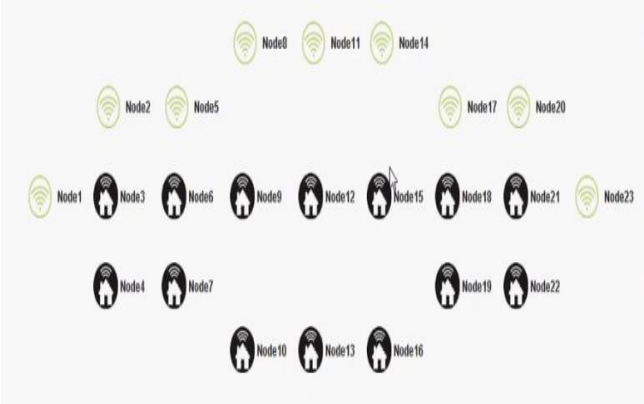

Fig5: Route from Source To Destination

Step3: In this we are making the threshold energy to zero such that the node will not receive the data. This node is called attacker node in this case.

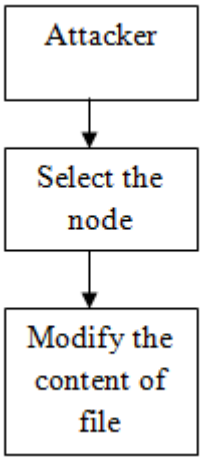

Fig6: Packet Dropper

Step4: In the figure, malicious nodes are taking place wherein one node the threshold value is less than the file size and in other node the malicious data has been entered by the attacker. This will be taken care by the Auditor. Once the node gets attacked, the auditor will make sure that the nodes which are malicious gets blocked next time. Such that the packet droppings may not occur and malicious node can be removed from the route.

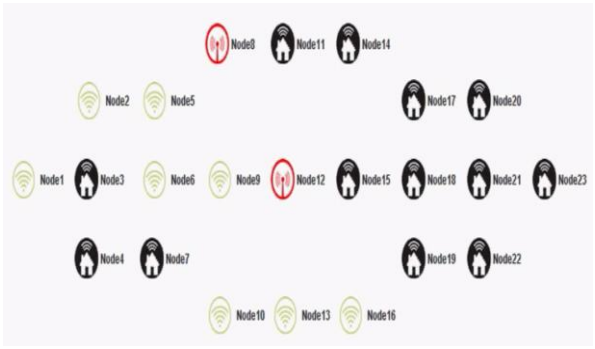

Fig7: Malicious Nodes

Step5: This figure shows the recovery process where the data which is been lost is recovered and then sent again by selecting the shortest distance between the nodes.

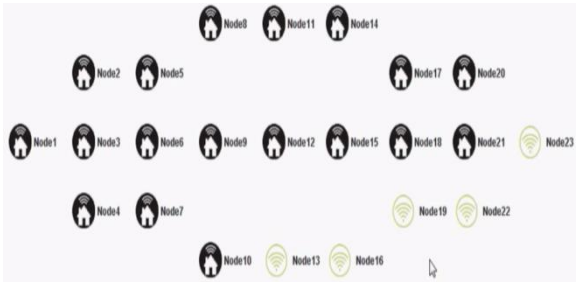

Fig8: Recovery Process

Step6: The below figure shows after all the transactions of data from source to the destination. Here the time delay is calculated in both the cases i.e, both the normal case without attacking and n the case of packet droppings. By using this scheme we can get the average delay time.

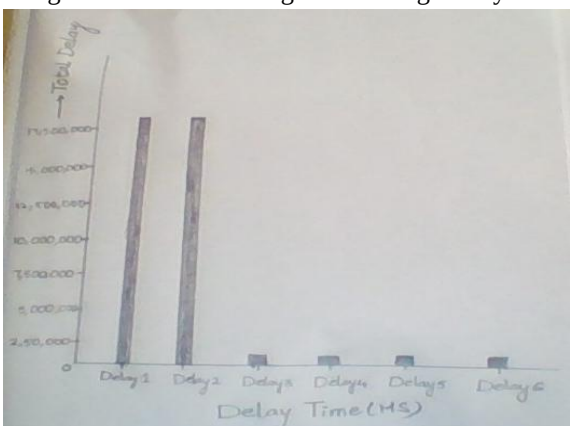

Fig9: Different Transactions Upload Delay Details

IX. 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.

ACKNOWLEDGMENT

I thank my college Marri Laxman reddy institute of technology and management who greatly assisted in the success of the project. I express my thanks and gratitude to Abdul Basith Khateeb sir, Head of the Department of CSE and my guide Mrs. PNV DIVYA Assistant Professor for their encouragement, support and guidance in presenting this paper.

REFERENCES

[1] 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.

[2] W. Kozma Jr., and L. Lazos, “REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.

[3] J. N. Arauz, 802.11 Markov channel modeling, 2004 C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores,"Proc. ACM Conf. Comput. and Commun. Secur., pp. 598-610., 2007.

[4] J. Crowcroft, R. Gibbens, F. Kelly and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks", First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., 2003.

[5] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks,"Proc. IEEE WCNC Conf., pp. 1510-1515., 2003.

[6] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks,” in Proc. IEEE INFOCOM Conf., 2003, pp. 1987–1997.

[7] 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.

[8] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable data possession at untrustedstores,” in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007,pp. 598–610.

[9] 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.

[10] D. B. Johnson, D. A. Maltz, and J. Broch, “DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks,” in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[11] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad-hoc routing service in adversarial environments,” Wireless Pers. Commun., Special Issue Secur. Next Generation Commun., vol. 29, no. 3, pp. 367–388, 2004.

AUTHORS PROFILe

CH. SONIA pursuing B.Tech degree in Computer science from the Jawaharlal Nehru Technological University (JNTU) , Hyderabad, India.

P.N.V DIVYA completed her M.Tech in St.Martins Engineering College, Hyderabad. She is presently working in CSE Dept as an Assistant Professor in Marri Laxman Reddy Institute of technology and management, Hyderabad.