# Detection of Packet Dropping Attacks in MANET using Public Auditing

Ms. Smita A Patil
M.Tech (CNE), Dept of CSE
CMRIT
Bengaluru, India

Mr. Manoj Challa
Assoc. Prof, Dept of ISE
CMRIT
Bengaluru, India

***Abstract*— Mobile ad hoc network consists of mobile nodes. The packet loss in MANETs is caused either by link error or the malicious packet dropping. To detect the main reason behind the packet loss we use the correlation between the lost packets. Packet loss bitmaps are used to get the information about the packet loss. These bitmaps are collected from each and every node that are part of the route. Collecting of bitmaps from intermediate nodes is done by public auditor. Since the misbehaving nodes are present in the network, the modified Homomorphic Linear Authenticator (HLA) cryptographic signature is proposed to securely collect the bitmaps. The proposed system is privacy preserving, collusion proof, and has low communication, storage and computation overhead. The performance of the proposed system is calculated by using the detection accuracy rate.**

***Keywords*— *Packet drop, Insider attack case, Public auditing, Homomorphic linear authenticator***

## I. INTRODUCTION

MANET consists of cooperative nodes. Cooperative nodes relay packets to each other. An adversary will utilize the advantage of the cooperative nature of MANET and attack the nodes to obtain the information send through the network.

Adversary may attack in three ways. One is through dropping all the packets through the malicious node. Second is randomly dropping packets and the third is very important i.e., selective packet dropping. In the first type of attack, the malicious node will drop all the packets that it receives from its upstream node. This is the case of intense Denial-of-Service (DoS) attack. The malicious node will not allow the packets to reach the destination. This type of attack can be easily detected [21]. Malicious nodes make their presence very obvious. When there is no packet transmission taking place from the node it is considered as malicious node and removed from the routing table. If the malicious node is not detected, the MANET use the multi path routing algorithm [23],[24] to eliminate those black holes and take a new path for packet transmission. Second type is the random packet dropping. In this case, malicious node drops the packet every now and then. It is a periodic process of dropping the packets. It can be sometimes misinterpreted as the link error. Third type is the very important type of attack i.e., selective packet dropping attack. In this attack, malicious node will be highly selective while dropping the packets [17],[20],[21]. Insider attack case is the particular attack which we are interested in this paper. Insider attack case is where the malicious node is part of the network, gains the knowledge of network's communication background and then selectively drops the packet to degrade the performance. The selective packet drop rate is similar to that of link error.

The proposed mechanism mainly concentrates on the selective packet dropping i.e., insider attack case. The cause of the packet drop is detected and if it is because of the malicious node(s) then these node(s) is/are detected and removed from the routing table. The proposed mechanism is using the correlation between the packet losses. The packet loss bitmap holds the state of transmission of packet. If the packet is forwarded to downstream node, then the bitmap has value 1 or else 0. These bitmaps are maintained by all the nodes that are part of the path. The correlation of the bitmaps is carried out using the auto correlation function (ACF) [1]. Collection of packet loss bitmap s from each and every node that are part of the path is done by the public auditor. Auditing is usually performed in the cloud for security purpose. To find the misbehaving node the auditor is used. To reduce the overhead from the network the auditing is carried out by the public server. All the nodes should give the information on the packet loss bitmap, if not given that node is directly considered as misbehaving and eliminated from the network. The network consist of malicious nodes hence they try to give wrong information of packet transmission to downstream node. The proposed mechanism introduces a modified Homomorphic linear authenticator (HLA) [2], [3], [22] cryptographic signature to collect the packet loss bitmaps truthfully. The original HLA signature perform well if there is only one misbehaving node. If there are more than one misbehaving nodes are present, then there is a chance of collusion. For example, consider two misbehaving nodes present in MANET network. The upstream misbehaving node receives the packet but do not forward to the downstream node. As the downstream node is also a misbehaving node it forms the back channel to communicate with the upstream misbehaving node. And when these nodes are asked for packet loss bitmaps they send wrong information. Hence, the modified HLA signature is used to make the mechanism collusion proof.

## II. RELATED WORK

The conventional method is divide into two categories based on the study performed on occurrence of the packet loss. First category mainly concentrates on the packet loss due to the malicious packet drop. These conventional methods neglect the packet loss due to the link error.

The first category is further grouped into four sub categories. The first one is based on the credit systems [8], [26], [9]. In the credit system, the nodes that transmit the packets to downstream node is given the credits. These credits are helpful for the nodes when they transmit their own packets. If the node is malicious then, it has low credit and never gets the opportunity to transmit its packets. The second sub category is based on the reputation systems [11], [7], [12], [15], [16], [10], [4]. In reputation system, nodes that transmit packets to its next node gets good reputation. If the node does not transmit packets to its next node, then it earns bad reputation. The information is propagated to all the nodes and the node that has bad reputation is avoided while routing process. The third sub category is hop-to-hop acknowledgement [14], [18], [19], [5], [6], [25] of the packet lost node which is responsible. Nodes which are responsible for packet loss are excluded. Fourth sub category is based on the cryptographic methods. For example, consider the work in [13] that uses Bloom filters. Bloom filter is the data structure that identifies whether an element is part of the set or not. Bloom filters in this paper helps to form proof for forwarding of the packets.

Second category is the combined effect of link error and malicious packet drop. But the malicious packet drop rate is very high compared to the link error packet loss rate. If the link error packet loss rate exceeds the malicious packet drop rate, then the above algorithms do not perform properly. Because the algorithms are developed considering the fact that malicious packet drop rate is higher than link error.

All the above conventional methods are mainly concentrating on the malicious packet drop attack. If the packet drop is highly selective then all the above algorithms do not work. As the selective packet drop rate is equivalent to the link error rate. In credit system, malicious nodes have enough credit since they have forwarded most of the packets. Similarly, in reputation system malicious node have enough reputation to transmit packets.

## III. PROPOSED SYSTEM

Architecture of the proposed system is as shown below in figure 1.

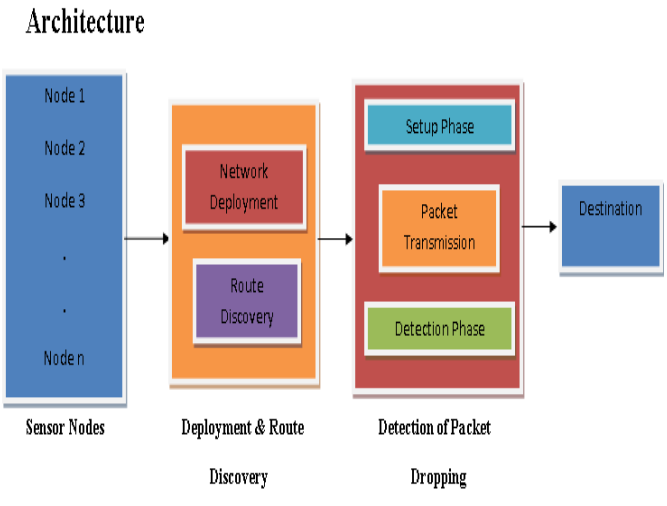


Fig. 1. Architecture of Proposed System.

The proposed system has the sensor nodes. The sensor nodes are deployed to create a MANET network. The parameters for network deployment are initialized such as number of nodes, routing protocol to be used, etc. The nodes are deployed in NAM (Network Animator) window. The beacon packets are transmitted to all the nodes present in the network. These packets are transmitted to find the neighbor nodes of each other. When beacon packets are sent to all nodes, the information is stored in the routing table. Using that table, routing protocols form path for packet transmission. The source sends packets to destination through this established path.

Consider an arbitrary path $P_{SD}$ in a MANET network, as shown in Figure 2. The source node $S$ continuously sends packets to the destination node $D$ through intermediate nodes $n1, \ldots, nK$, where $n_i$ is the upstream node of $n_{i+1}$, for $1 \le i \le K-1$. We assume that $S$ is aware of the route $P_{SD}$, as in Dynamic Source Routing (DSR). If DSR is not used, $S$ can identify the nodes in $P_{SD}$ by performing a traceroute operation.

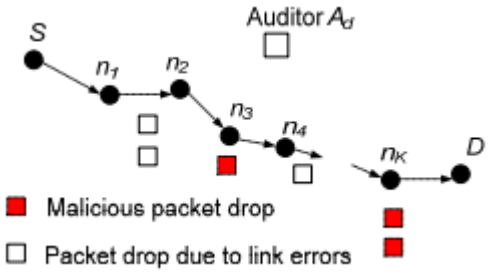


Fig. 2. Network and Attack model.

Our architecture consists of four phases: setup phase, packet transmission phase, audit phase, and detection phase.

### A. Setup Phase

The setup phase comes into action right after the route discovery process but before the packet transmission phase. Source node use the symmetric key crypto system and symmetric keys. Source node safely transmits decryption key and symmetric key to all intermediate nodes. Key distribution is carried out by the RSA algorithm. Source node also inform all the nodes of two hash functions. Source node has to arrange HLA keys.

### B. Packet Transmission Phase

In this phase source node transmits the packet along the path $P_{SD}$. The packets are first hashed using hash function and then sent to all intermediate nodes along with HLA signatures. The one way chained encryption is used for transmission of packets and keys. One way chained encryption prevents upstream node to decipher signatures that are meant for downstream nodes. Message Authentication Code (MAC) is computed using another hash function. First the packet is grouped with HLA signature and then encrypted. Then the encrypted message is concatenated with the MAC key to form a new packet. When the first node receives the new packet, it extracts original packet, HLA signature and MAC key. After that the node stores the data in proof of reception database. When the auditor is

investigating, nodes send the data from proof of reception as a proof for forwarding the packets to next node.

### C. Audit Phase

This phase is activated when the source node sends the Attack detection request (ADR) message to the audit. In ADR message it includes packet sequence number, node ID's, HLA public key. Auditor sends the challenge vector to all the intermediate nodes. On the basis of the proof of reception database nodes will send the packet reception bitmaps. The value is 1 if received otherwise 0. Auditor checks for the validity of data. If bitmap equals to the data then it is accepted otherwise, the node is rejected and considered as malicious node. In this phase it only verifies if the node is understating i.e., gives the wrong information about receiving packet when in actual it has not received the packet.

### D. Detection Phase

The auditor does the following functions in detection phase.

- Detect any overstatement of packet loss i.e., informing not reception of packet but in actual it has received.
- Constructing a packet-loss bitmap for each node.
- Calculating the autocorrelation function for the packet loss on each node.
- Decide whether malicious behavior is present.

## IV. RESULTS

In the performance section, the detection accuracy of the proposed system that uses maximum likelihood algorithm and proposed system algorithm are considered. Here the two types of malicious packet dropping are examined i.e., random dropping and selective dropping. Figure 3, 4 and 5 shows the random packet drop case. Figure 6, 7 and 8 shows the selective packet drop case. Random dropping has the probability of packet drop $P_M$. In selective packet drop attack, attackers drop packets of certain sequence number.

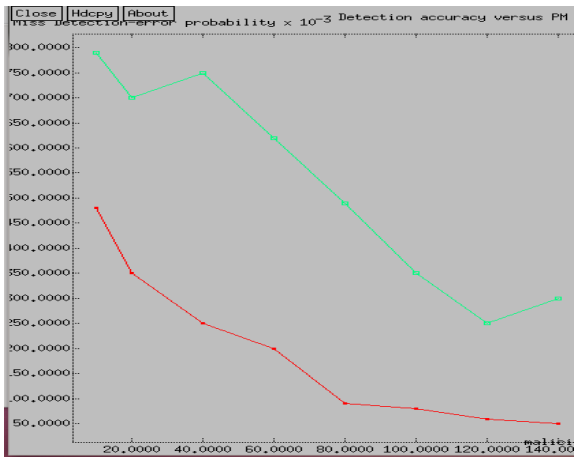


Fig. 3. Overall detection-error probability(random packet-drop case).

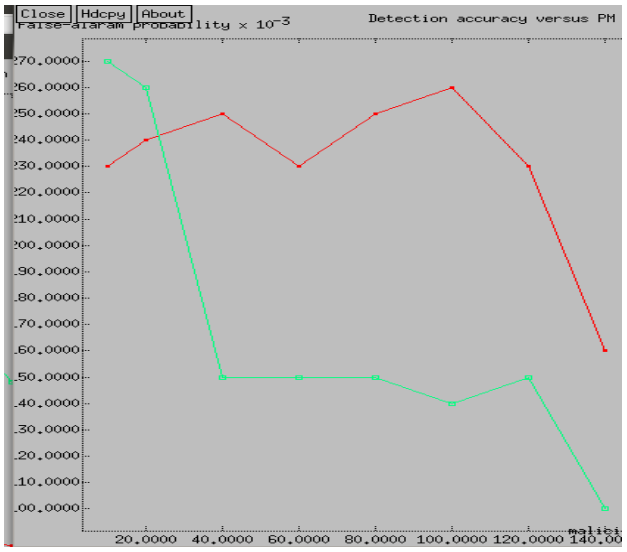


Fig. 4. Miss-detection probability(random packet-drop case).

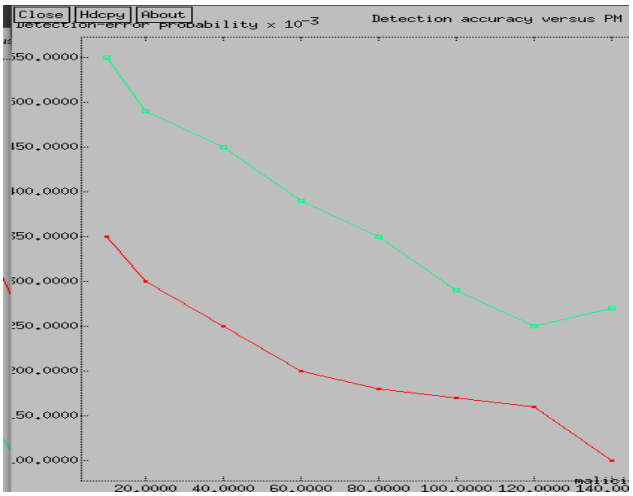


Fig. 5. False-alarm probability(random packet-drop case).

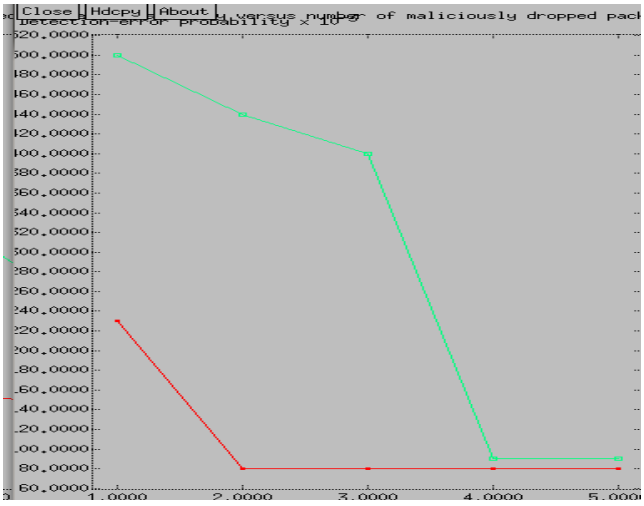


Fig. 6. Overall detection-error probability(selective packet-drop case).

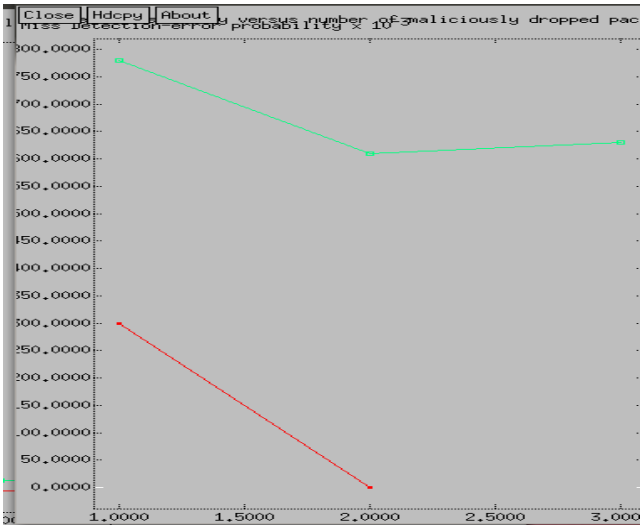


Fig. 7. Miss-detection probability(selective packet-drop case).

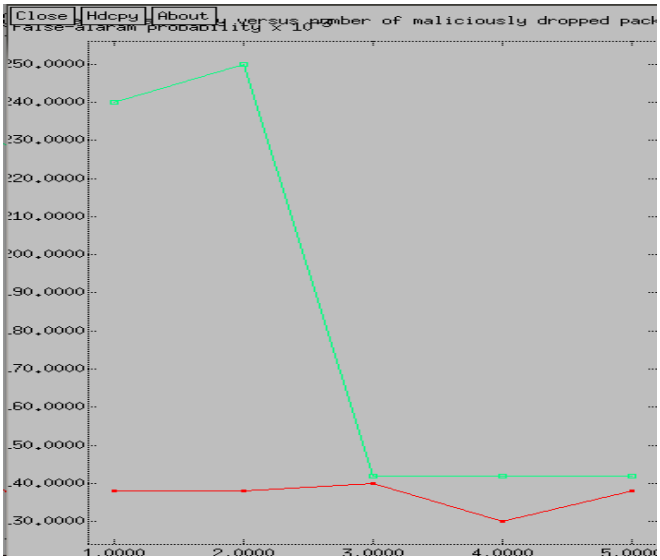


Fig. 8. False-alarm probability(selective packet-drop case).

## V. CONCLUSION

The conventional method is divide into two categories based on the study performed on occurrence of the packet loss. First category mainly concentrates on the packet loss due to the malicious packet drop. These conventional methods neglect the packet loss due to the link error. The packet loss in MANETs is caused either by link error or the malicious packet dropping. The proposed system truthfully detects the main reason behind the packet loss by using the correlation between the lost packets. Packet loss bitmaps are used to get the information about the packet loss. These bitmaps are collected from each and every node that are part of the path $P_{SD}$. Collecting of bitmaps from intermediate nodes is done by public auditor. Since the misbehaving nodes are present in the network, the modified Homomorphic Linear Authenticator (HLA) cryptographic signature is proposed to securely collect the bitmaps. The proposed system is privacy preserving, collusion proof, and has low communication, storage and computation overhead. The performance of the proposed system has the detection accuracy rate very high compared with conventional method i.e., maximum likelihood algorithm. The performance is measured using two cases one is random drop and the other one is selective drop. In both the cases the detection accuracy of proposed system is higher than conventional method.

## REFERENCES

[1] J. N. Arauz. 802.11 Markov channel modeling. Ph.D. Dissertation, School of Information Science, University of Pittsburgh, 2004.

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 598–610, Oct. 2007.

[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] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM TISSEC, 10(4), 2008.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008.

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

[7] S. Buchegger and J. Y. L. Boudec. Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the ACM MobiHoc Conference, 2002.

[8] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5):579–592, Oct. 2003.

[9] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring. Modelling incentives for collaboration in mobile ad hoc networks. In Proceedings of WiOpt, 2003.

[10] J. Eriksson, M. Faloutsos, and S. Krishnamurthy. Routing amid colluding attackers. 2007.

[11] 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.

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

[13] 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.

[14] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgement-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536– 550, May 2006.

[15] Y. Liu and Y. R. Yang. Reputation propagation and agreement in mobile ad-hoc networks. In Proceedings of the IEEE WCNC Conference, pages 1510–1515, 2003.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the ACM MobiCom Conference, pages 255–265, 2000.

[17] G. Noubir and G. Lin. Low-power DoS attacks in data wireles lans and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, July 2003.

[18] V. N. Padmanabhan and D. R. Simon. Secure traceroute to detect faulty or malicious routing. In Proceedings of the ACM SIGCOMM Conference, 2003.

[19] P. Papadimitratos and Z. Haas. Secure message transmission in mobile ad hoc networks. Ad Hoc Networks, 1(1):193–209, 2003.

[20] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.

[21] A. Proano and L. Lazos. Packet-hiding methods for preventing selective jamming attacks. IEEE Transactions on Dependable and Secure Computing, 9(1):101–114, 2012.

[22] H. Shacham and B. Waters. Compact proofs of retrievability. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Dec. 2008.

[23] T. Shu, M. Krunz, and S. Liu. Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE Transactions on Mobile Computing, 9(7):941–954, 2010.

[24] T. Shu, S. Liu, and M. Krunz. Secure data collection in wireless sensor networks using randomized dispersive routes. In Proceedings of the IEEE INFOCOM Conference, pages 2846–2850, 2009.

[25] Y. Xue and K. Nahrstedt. Providing fault-tolerant ad-hoc routing service in adversarial environments. Wireless Personal Communications, Special Issue on Security for Next Generation Communications, 29(3):367–388, 2004.

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