AUDITING BASED TECHNIQUE FOR IDENTIFICATION OF MALICIOUS PACKET DROPPING IN MANET

[1]K.Vanitha, [2]K.Anitha, [3]Dr.M.Mohamed Musthafa, [4]Dr.A.M.J.Zubair Rahaman

[1]Assistant Professor, [2]Assistant Professor, [3]Professor, [4]Professor
Computer Science and Engineering,
[1,3,4]Al-Ameen Engineering College,Erode,India
[2]CSI College of Engineering, Ketti

Abstract: MANET is multi hop ad-hoc networks and nodes in that can acts as sender or receiver or relay. Packet drooping is one of the main concerns and the packet loss can be occurred by link errors and malicious packet dropping. The main purpose of this work is to develop an accurate algorithm for detecting selective packet drops made by insider attackers and to improve the detection accuracy, to differentiate whether packet loss is caused due to link error or activity of the attacker by exploiting the correlations between lost packets and to detect packet dropping attacks in mobile environment. The packet dropping in this case is nearly equal to the normal link error because of which existing algorithm that are based on detecting the packet loss rate cannot find the exact cause of packet loss. Hence to improve the detection accuracy, the correlations between lost packets is identified. The technique called Homomorphism Linear Authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of packet loss information reported by nodes. This architecture is privacy preserving, collusion proof and incurs low communication and storage overheads. Hence to improve the detection accuracy, the correlations between the bitmap generated are calculated and lost packets are identified. The public auditing architecture is developed that detects and verifies the truthfulness of the packet loss information reported by nodes.

***Index Terms*: MANET, packet dropping, HLA, ACF, Auditing**

I. INTRODUCTION

The nodes are communicated with each other through wireless links in wireless ad-hoc networks. The nodes are dynamic in the ad-hoc network is generally called Mobile ad-hoc network (MANET) [17]. As MANET is infrastructure less network its topology changes every time and there is no central access point to control the nodes. All the nodes can either act as a relay or host. Nodes can communicate with other nodes through intermediate nodes where that intermediate nodes route the packets from or to other nodes in the network. The source and destination are within the communication range can directly communicate otherwise it must communicate through the intermediate node. During the communication, the cooperation of the nodes in the path is very important for successful packet delivery from source to destination. Wireless nodes which run on batteries and nodes may or may not cooperate in the communication because of its energy constraint. The node which receives and send packets will consume some energy, in order to preserve its energy, some nodes may not cooperate effectively in the network and simply drop the packets.[5,18]

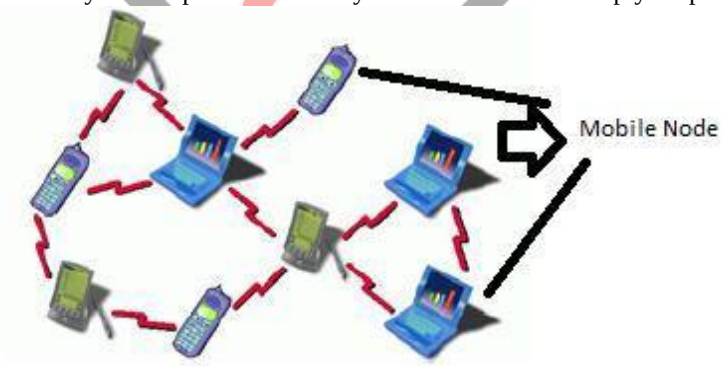

Figure1.MANET Example

The dropping of packet either by the failure of a link which is unintended or by the malicious node which is intended [5]. A malicious node may misbehave by agreeing to forward the packets and later failing to do so. After included in a route the node stop forwarding the Packet to the next node. Identifying the packet dropping by link error or by a malicious node is very important. Once the malicious node is identified that node taken from the routing table of the network. If the identification of packet drops by link error then selects the different route with the help of multipath routing algorithm. The figure 2 shows the malicious node packet dropping example.

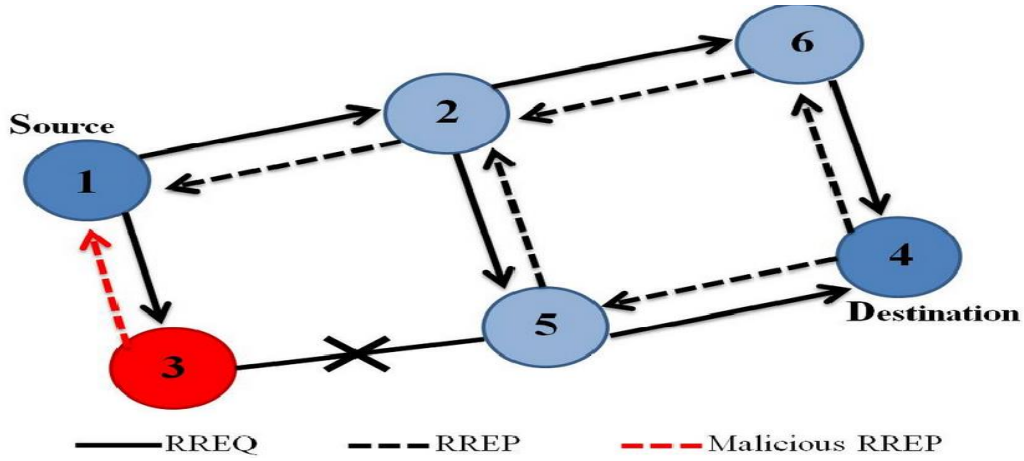

Figure2.Example of Malicious node packet dropping

In this paper first, we discuss what are the available techniques for identifying the malicious node and second how our proposed method will help in identifying the malicious node.

II. RELATED WORKS

The cooperation of nodes is very important aspects of MANET for transferring the packet from source to destination. The packet drops due to link error or malicious packet drop. Here how the different approach used to identify malicious nodes such as credit systems, reputation-based system, hop to hop Acknowledgement and cryptographic primitive method. For the credit based system [11], [12] each node receives credit for transmitting a large number of packets to other node and that credit will help to send its own packet. The incentives are given to the node those who behave well during the communication. It is hard to find malicious node packet dropping if node performs selective packet dropping. Malicious node gets intensive for receiving packet forwarding from upstream nodes. So the credit is added for malicious nodes which help to maintain its trust level high. For the reputation method [13], each node has to maintain its good reputation in order to participate in the communication. Any node with the bad reputation not able to participate in the communication network. It depends on the neighbour node to monitor and identify the misbehaving nodes. The information contains the reputation is sending periodically throughout the network and this will help the node in select the routes which not containing malicious nodes. A node with high packet drops is given bad reputation by its neighbour nodes. In this method malicious node maintaining its reputation by simply forwarding the packets to its next node. For the Hop to Hop Acknowledgement any node with the high rate of packet loss which is excluded from the network and eliminated from route section This kind of research is found in [14], [15], and [16]. In [8], the author proposed an anomaly-based IDS system on an enhanced windowing method to carry out the collection and analysis of selective drop attack. This method leads to some miss calculation and detection accuracy. A Record and Trust-Based Detection (RTBD) technique was proposed in [9] which lead to low performance evaluation when the trust is created based on credit system. In [10] the author proposed an intrusion detection system which removes the fake nodes but does not contain any authentication method for privacy purpose.

III. PROPOSED WORK

In MANET the packets are transmitted from source to destination through the intermediate node and few packets are lost due to link failure or dropping by the malicious node. In our proposed model the auditor node is independent of the routing path is the responsibility of detecting the reason for packet loss. The packet loss calculated at the destination node and sends the suspected list to the source node. The Source node sends an attack detection request (ADR) to the auditor. Autocorrelation function (ACF) calculates the correlation between the positions of last packets of the bitmap generated by each node. The bitmap is described the lost and received status of each packet in a sequence of consecutive packet transmission.

PROCESS OF PROPOSED WORK:

Step1:

The distribution of the symmetric keys to all nodes and the hash function is carried out by source Node. The packets are transmitted along with the signature in order to preserve privacy.

Step2:

The status of packet transmission is stored at the database at every intermediate node. This will help to generate a bitmap.

Step3:

The destination node notices the occurrences of packet loss and intimate to the source node.

Step4:

The source node verifies the intermediate node randomly and creates the suspect list.

Step5:

The source node sends the request to nearest auditor node to detect an attack.

Step6:

The auditor node verifies the bitmap at a suspected intermediate node and then autocorrelation function calculated and detect the malicious node.

PHASES OF PROPOSED WORK:

DISTRIBUTION OF KEY:

The source node decide on a encrypt key and decrypt key Consider the path from source to destination as P_{SD}. The source node S makes decision on a symmetric-key crypto-system (encryptkey, decrypt key) and K symmetric keys $key_1, \ldots, key_k$. The source node distributes the decrypt key and a symmetric key key_j to its neighbor nodes n_j which exists in the path. RSA is used for key distribution. Using the public key of the intermediate nodes n_j where j=1 to k, the source node encrypts and sends the cipher text to nj. After receiving the packet, the intermediate nodes decrypt the cipher text using its private key and extract the decrypt key and symmetric key key_j. The source node also announces two hash functions to all nodes in the path which can be used for authentication purpose.

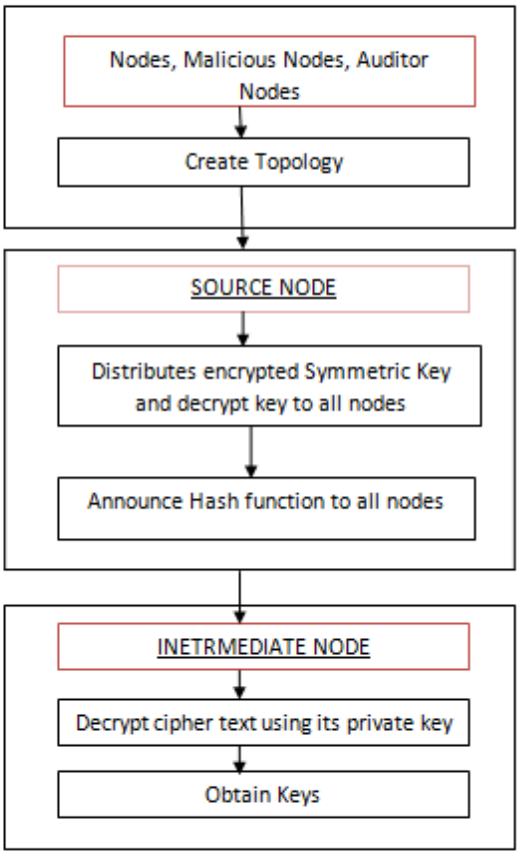

Figure3.Distribution of Keys

PACKET TRANSMISSION:

The Packet is transmitted by source node after the key distribution. Consider packeti send by the source node S, where "i' is the sequence number to identify uniquely among the packets. Source node S computes the hash function of the packet Pi as r_i=H1 (Pi). S then generates an extended HLA signature for node n_j as shown in equation [(1).

$$S_{ji}=[H2(i||j)u^{ri}]^x, \text{for } j=1,\ldots,k, \quad (1)$$

Here a one way chained encryption is used, it prevents an upstream node from deciphering the signature send to downstream nodes. By using this one way encryption, the S_{ji} is sent along with Pi. S also iteratively computes the following parameters as in equation (2).

$$\begin{aligned} &K_i = \text{encryptkeyK}(S_{Ki}),\\ &T_{ki}=Ki||MAC_{keyK}(K_i), \quad (2)\\ &.\\ &.\\ &.\\ &T_{ji} = Sji||MAC_{keyj}(S_{ji}), \end{aligned}$$

Where Message Authentication Code (MAC) is computed according to the hash function H. S puts Pi and Ti in one packet and sends it to node n1.n1 receives the packet from S and extracts Pi and Ti. Then n1 verifies the integrity of 1i by testing the equality as shown in equation (3)

MAC_{key1} (1i)=(1i). (3)

If the result of the test is true, then n1 decrypts 1i as shown in equation (4).

Decryptkey1 (1i)=$s_{1i}||T_{2i}$. (4)

If the test of equality fails, then n_1 stores loss of P_i in the proof of reception database. Once if the test is proved to be true then n_1 stores r_i and s_{1i} in its proof of reception database. Each node after receiving the packet stores the data of reception in the database maintained by each node individually. The data is stored as FIFO manner. This proof is used for auditing later. Then n_1 puts P_i and T_{2i} in one packet and transmitted to n2. The above process is repeated at every intermediate node n_j. The last intermediate node n_k, only forwards Pi to the destination D.

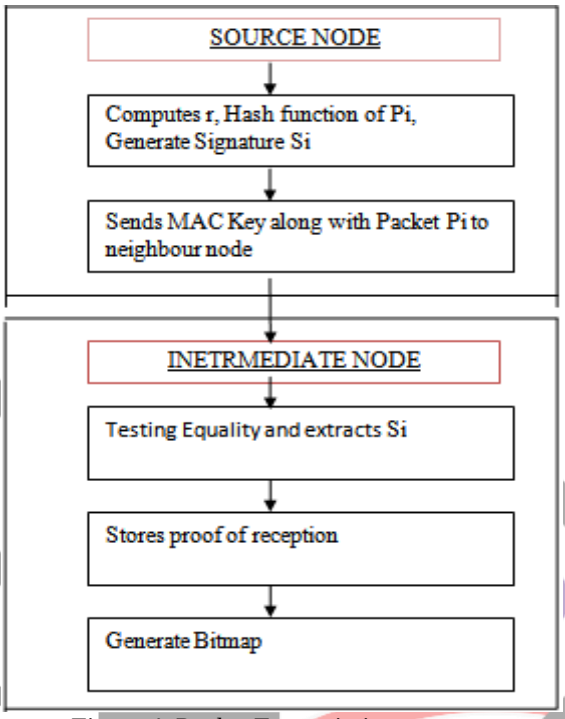

Figure 4. Packet Transmission

VERIFICATION OF PACKET LOSS:

Verification of packet loss done in the destination node. The Algorithm verifies the packet loss and generates the suspected node list. The actual number of packet received from the previous node is less than the number of packet sent from source node then the destination node sends the packet loss message to source node.

The source node first discovery the suspected node by sending a request to the intermediate node at random. The intermediate node sends the number of packets it received to the source node based on the request. The source node verifies at which node there is a change in the number of packets. If any variation in number of packets received in any node then its neighbour node is added to the suspected list. After creating the suspected list attack detection request send to the nearest auditor node for auditing.

Algorithm:

If source node S
    Intimate to the destination, the count of data packets in a block of data send one block of data through the path selected through route discovery process
Else if destination node D
    Compare the data packets received with the data count intimated by the source.
Calculate the probability of packets received at the destination node as PD.
If PD < TPL (the value of TPL is between 0 and 0.2)
    Send positive acknowledgement back to source node.
Else
    Creates the suspected node list
    Initiate Attack Discovery Process
End if

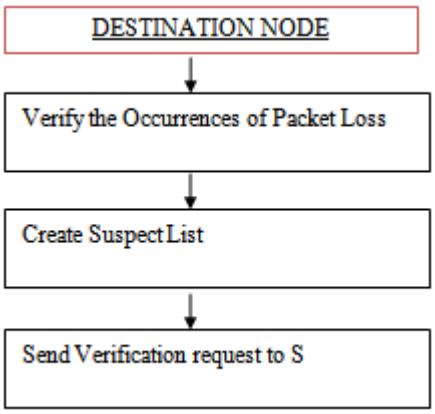

Figure5. Verification of Packet loss

AUDITING:

The public auditor received Attack detection request (ADR) from the source node. An improved auditing method is discussed to improve the attack detection accuracy. This request contains the id of the nodes in the path P_{SD}. The sequence number of packet received is stored in the database at each node. The auditor node submits a challenge vector to each node in the path. Based on this proof of reception stored in the database, the bit map b_j is generated by node nj. Here the j = (b_{j1}, . . . , b_{jM}) where b_{ji}=1 if the packet is received at that particular node and b_{ji}=0 if the packet is not received at the particular node. The auditor node is also provided with the information about sequence number of the packets sent from source node and also the sequence number of the subset of these packets that were received by destination node.

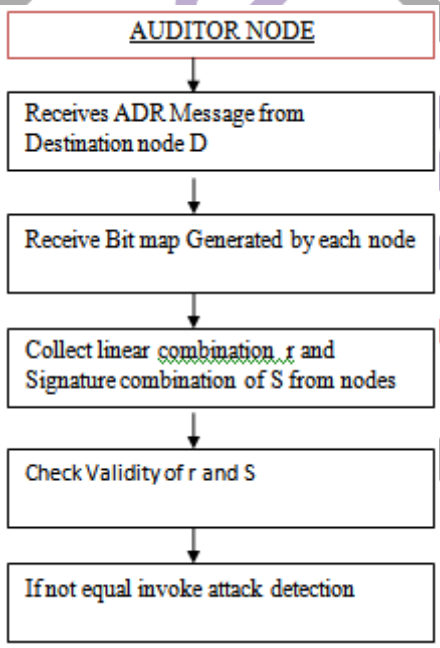

Figure6. Auditing

ATTACK DETECTION:

Auditor enters into detection phase after it receives bitmap. Auditor constructs packet loss bitmap at each node to detect is there is any overstatement of packet loss and checks the consistency of the bitmaps. If there is no exaggeration of packet loss, then the set of packets received at node j+1 should be a subset of the packets received at node j. If any node which truthfully reports its packet reception bitmap is considered as normal node else it consider as malicious node. Hence bitmap of a malicious node will disagree with with the bitmap of a normal downstream node. There will always be at least one downstream node i.e. destination node. So Ad only sequentially scans bitmap reported by intermediate node and the report from D to identify nodes that are overstating their packet losses. After checking for the consistency of bitmaps, Ad starts constructing the per-hop packet-loss bitmap j from j-1 and 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 mj. The packets that were not received by the upstream node will be marked as “not lost” for the underlying hop. Denoting the “lost” packet by 0 and “not lost” by 1, j can be easily constructed by conducting a bit-wise complement-XOR operation of j-1 and j.

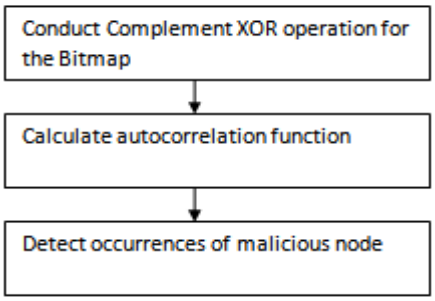

Figure7. Attack Detection

IV. CONCLUSION

In this paper we proposed a method based on Auditing using HLA in order to identify packet loss and find the reason for packet loss. It examines the reason whether the packet drop is either link failure or malicious attacks. In also helped in finding the actual cause of the packet drop. To identify the packet loss is purely due to link errors or combines effect of ink error and malicious drop by detecting the correlations between lost packets. In future the detection mechanism can be tested in various protocols and network environment and compare their performance. As a first step, this analysis mainly highlight the fundamental features of the problem, such as the untruthfulness nature of the attackers, the privacy-preserving requirement for the auditing process, and the randomness of packet losses, but ignore the particular behaviour of various protocols that may be used at different layers of the protocol stack.

REFERENCES

[1] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation- based incentive scheme for ad hoc networks," in Proc. IEEEWireless Commun. Netw. Conf., 2004, pp. 825–830.

[2] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

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

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. ACM MobiComConf., 2000, pp. 255–265.

[5] Vanitha, K & Zubair Rahaman, AMJ, 'Efficient Analysis of Malicious Packet Dropping and Privacy in MANET using FHM', Asian Journal of Research in Social Sciences and Humanities, vol.7, no. 1, January 2017, pp. 551-562

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

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

[8] G Rajarajan and L. Ganesan"A Hybrid Approach to Protect Network Components from Distributed Denial of Service Attacks", Advances in Natural and Applied Sciences,2016,10(1):117-122

[9] Lilly Roseline Mary J and Buvana M," Secure and Efficient Data Gathering Using Trust Management Scheme and Intrusion Detection System in Wireless Sensor Network", Advances in Natural and Applied Sciences,2016, 10(1):123-129.

[10] Nilesh N. Dangare and RS Mangrulkar,"Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network". Elsevier, 2016, 78:342-349.

[11] teniese,G S. Kamara, and Katz.J. "Proofs of storage from homomorphic identification protocols", in Proc. Int. Conf. Theory Appl.Cryptol Inf Security,2009,pp.319–333.

[12] Awerbuch B, R Curtmola, Holmer D, Nita-Rotaru C, and Rubens H.ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Trans. Inform.Syst. Security, 2008,10(4):1–35.

[13] W.Galuba P. Papadimitratos, M. Poturalski, K. Aberer, Z.Despotovic, and W. Kellerer.Castor: Scalable secure routing for ad hoc networks. Proc. IEEE INFOCOM, 2010 pp. 1 –9.

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

[15] V. N. Padmanabhan and D. R. Simon, "Secure trace route to detect faulty or malicious routing," in Proc. ACM SIGCOMM Conf., 2003, pp. 77–82.

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

[17] K.Vanitha and Dr.A.M.J.Md Zubair Rahman," An Efficient Analysis of Black Hole Attack On AODV Routing Protocol In Mobile Adhoc Networks" International Journal of Applied Engineering Research,vol.10,no38,2015, 28386- 28390.

[18] K.Vanitha, K.Anitha, Dr.A.M.J.MdZubair Rahaman, Dr.M.Mohamed Musthafa,"Analysis of Cryptographic Techniques in Network Security", Journal of Applied Science and Computations, Vol. 5 Issue 8, 2018, Page No: 155-163.