IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 52-57
www.iosrjournals.org

Detection Of Malicious Packet Dropping Attack In Wireless AD HOC Networks

Megha Vasu Mohan [1], Prof. Nagaraj K. Vernekar[2]
[1] (*Computer Engineering Department, Goa College of Engineering, Farmagudi, Goa, India)*
[2] *(Computer Engineering Department, Goa College of Engineering, Farmagudi, Goa, India)*

Abstract: *In wireless 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. Channel error and malicious packet dropping are two cause of packet drop in the wireless ad hoc network. 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. . The main aim is to find out whether the packet loss is due to connection error only or both connection and malicious drop. Conventional method does not achieve acceptable detection accuracy. In order to improve the detection accurately we are using entropy method to ensure whether the packets are lost due to connection error or malicious drop and to make sure that calculation of entropy is truthful, we develop a public auditing architecture called homomorphic linear authenticator (HLA) that allows the detector to prove the correctness of the lost packet information reported by intermediate nodes.*

Keywords: *Homomorphic linear authenticator (HLA), Entropy method, Malicious node detection, Packet dropping, Signature generation.*

I. Introduction

In a multi-hop wireless network, nodes cooperate in routing traffic. This cooperative nature is utilized by an invader to launch attacks. For example, the invader may first pretend to be a cooperative node in the path generation process. Once added in the path, packet dropping is done by invader. In the worst case, malicious node completely disturbs the path from source to destination by not forwarding packets from the upstream nodes. By this drastic Denial-of-Service (DoS) attack network becomes debilitated by fencing off the network topology. An insider attack is launched by the malicious node which is included in path by utilizing its knowledge of the network protocol and the communication context. Specifically, the malicious node may assess the prominence of various packets, and then drop the small amount that are conceive to be highly critical to the operation of 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.

The algorithm provides a truthful and publicly verifiable method to support the recognition technique. A bitmap is generated by intermediate nodes indicating the lost/received status of each packet in a sequence of consecutive packet transmissions. The auditor calculates packet loss per-hop bitmap easily constructing a bit-wise complement-XOR operation of two bitmaps. The main aim is to build the homomorphic linear authenticator (HLA) cryptographic method which is mostly a signature system so as to assure that the packet-loss bitmaps reported by individual nodes along the path are correct, i.e., reflects the actual status of each packet transmission. The construction of such a proof should be privacy preserving, i.e., it does not disclose the original information that is transmitted on path from source and destination. The detection method should obtain little communication and storage overheads, so that it can be applied to a large mixture of wireless networks.

1.1 Problem Statement

In a wireless network, the problem is to recognize the nodes on PSD that drop packets maliciously. The detection to be performed by a public auditor that does not have information of the secrets held by the nodes on PSD. When a malicious node is detected, the auditor should be able to build a publicly verifiable proof of the misconduct of that node.

1.2 Project Objective

The main objective is to detect the occurrence of selective packet drops and identifying the malicious node responsible for these drops. Entropy method is used to check whether the packets are lost due to link error or both malicious drop and link error. Ad hoc on-demand Distance Vector (AODV) Routing Protocol is used instead of DSR protocol**.**

II. Literature Survey

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.

Liu, Deng, Varshney and Balakrishnan[9] proposed a paper title "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs". To study routing misbehavior in MANETs (Mobile Ad Hoc Networks). In general, routing protocols for MANETs are planned based on the statement that all participating nodes are completely supportive. However, due to the open structure and hardly available battery-based energy, node misbehaviors may be real. One such routing misbehavior is that some self-interested nodes will participate in the route discovery and maintenance processes but decline to promote data packets. In this paper, the author proposes the 2ACK scheme that serves as an add-on method for routing schemes to find out routing misbehavior and to diminish their undesirable effect. The main proposal of the 2ACK scheme is to send two-hop acknowledgment packets in the reverse way of the routing path. In order to reduce additional routing overhead, only a part of the received data packets are acknowledged in the 2ACK scheme.

Marti, Giuli, Lai and Baker[4] proposed a paper titled "Mitigating Routing Misbehavior in Mobile Adhoc Network" where Reputation Based System is used to keep track of the quality of activities of other node in an adhoc network. Basically reputation is a sight formed on the basis of inspecting node performance. Reputation can be intended by direct inspection and/or indirect inspection of the nodes during route behavior, number of transmissions generated by the node, through acknowledgement communication and by overhearing node's communication by the adjacent nodes. This scheme that contains two main modules, termed watchdog and pathrater, to identify and diminish, respectively, routing misbehavior in MANETs. Nodes operate in a immoral mode wherein the watchdog module overhears the media to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of newly sent packets. A data packet is cleaned from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for a long time, the watchdog module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior recognition at the forwarding level as well as the link level.

Balakrishnan, Deng, and Varshney[3] proposed a paper title "TWOACK: Preventing selfishness in mobile ad hoc networks". Mobile ad hoc networks (MANETs) operate on the basic underlying assumption that all participating nodes fully work together in self-organizing functions. However, performing network functions consumes energy and other resources. Therefore, some network nodes may choose against cooperating with others. Providing these misbehaving nodes, with an motivation to cooperate has been an active research area recently. In this paper, they propose two network-layer acknowledgment-based schemes, termed the TWOACK

and the S-TWOACK schemes, which can be simply added-on to any source routing protocol. The TWOACK scheme detects such disobedient nodes, and then seeks to improve the problem by notifying the routing protocol to avoid them in future routes.

III. Proposed System

3.1 Overview

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 for detecting selective packet dropping attack made by malicious node.The high detection accuracy is achieved by using entropy method to detect malicious behavior. In Fig 1 indicates source, destination and three intermediate nodes where packet is transmitted and malicious node drops selective packets along with link error due to which some packets are dropped.

Each intermediate node sends an acknowledgment to the source after receiving the key during key transmission phase. Each intermediate node provides a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions to the auditor.

3.2 System Architecture

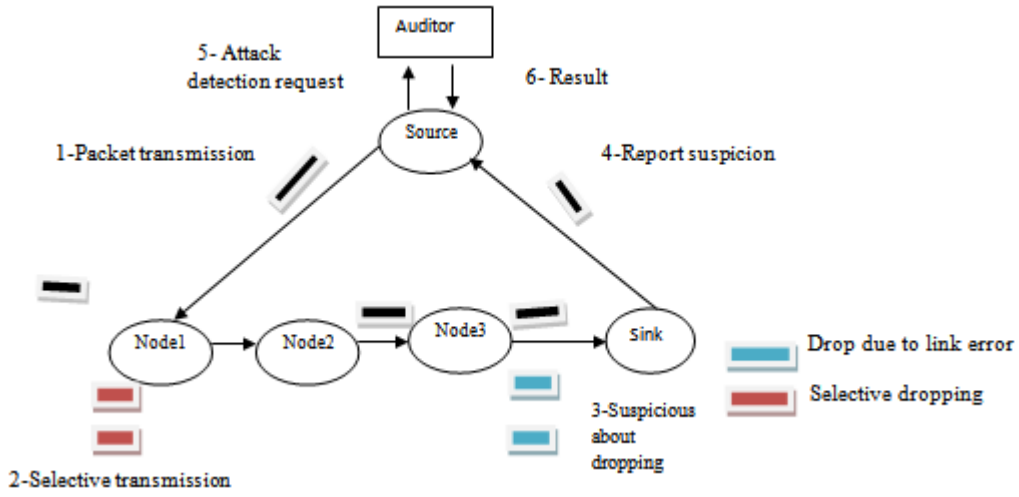

Fig 1: Packet transmission from source to destination

3.3 Modules

3.3.1 Setup phase

The source selects the route by Ad hoc On-demand Distance Vector (AODV) Routing Protocol. In this phase, S decides on a symmetric-key crypto-system (encryptkey; decryptkey) and K symmetric keys key1; . . . ; keyK, where encryptkey and decryptkey are the keyed encryption and decryption functions, respectively. S securely distributes decryptkey and a symmetric key keyj to node nj on PSD, for j = 1; . . .;K.

3.3.2 Packet Transmission Phase

After completing the setup phase, S enters the packet transmission phase. It generates the HLA signatures for each packet. S transmits packets to PSD according to the following steps.

Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes ri = H1(Pi) and generates the HLA signatures of ri for node nj , as follows:

$$sji = [H_2(i||j)u^{ri}]^x, \text{ for } j = 1, \ldots, K \quad (1)$$

These signatures are then sent together with Packet to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes.

3.3.3 Audit Phase

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1,. . . , nK, S's HLA public key information, the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Ad submits a random challenge vector $\vec{}cj$ = (cj1, . . . , cjM) to node nj , j = 1, . . . ,K, node nj generates a packet-reception bitmap $\vec{}bj$ = (bj1, . . . , bjM),

where bji = 1 if Pi has been received by nj , and bji = 0 otherwise. Node nj then calculates the linear combination:

$$r^{(j)} = \sum_{i=1, b_{ji}\neq 0}^{M} c_{ji} r_i \quad (2)$$

Each intermediate node calculates HLA signature for all the packets together:

$$s^{(j)} = \prod_{i=1, b_{ji}\neq 0} s_{ji}^{cji} \quad (3)$$

Node nj submits $\vec{}$bj , $r^{(j)}$and $s^{(j)}$ to Ad, as proof of the packets it has received.

$$e\left(s^{(j)}, g\right) = e\left(\prod_{i=1, b_{ji}\neq 0}^{M} H_2(i||j)^{c_{ji}} u^{r(j)}, v\right) \quad (4)$$

If the equality holds of (4) then Ad accepts that node nj received the packets as reflected in $\vec{}$bj.

3.3.5 Detecting Phase

The public auditor A_d enters the detection phase after receiving and auditing the reply to its challenge from all nodes on P_{SD}. The main tasks of A_d in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the entropy value for the packet loss on each hop, and deciding whether malicious behavior is present or not.

The auditor calculates packet loss per-hop bitmap $\vec{}$mj = (mj1, . . . ,mjM) where j=1,2…….K where K is the total number of intermediate nodes. Then auditor calculates entropy method [10] for each sequence $\vec{}$mj = (mj1,…. ..,mjM), j = 1, . . . ,K, as follows:

$$E_j = -\sum_{i=0}^{M-1} m_j(i) \log_2 m_j(i) \quad (5)$$

The entropy method Ej is then used as the decision statistic to decide whether or not the packet loss over the jth hop is caused by link error or both link error and malicious drops. In particular, if $E_j \geq e_{th}$,where e_{th} is an threshold value, then Ad decides that there is malicious packet drop over the hop or not. In Fig 2 whole working model of the project is described briefly.

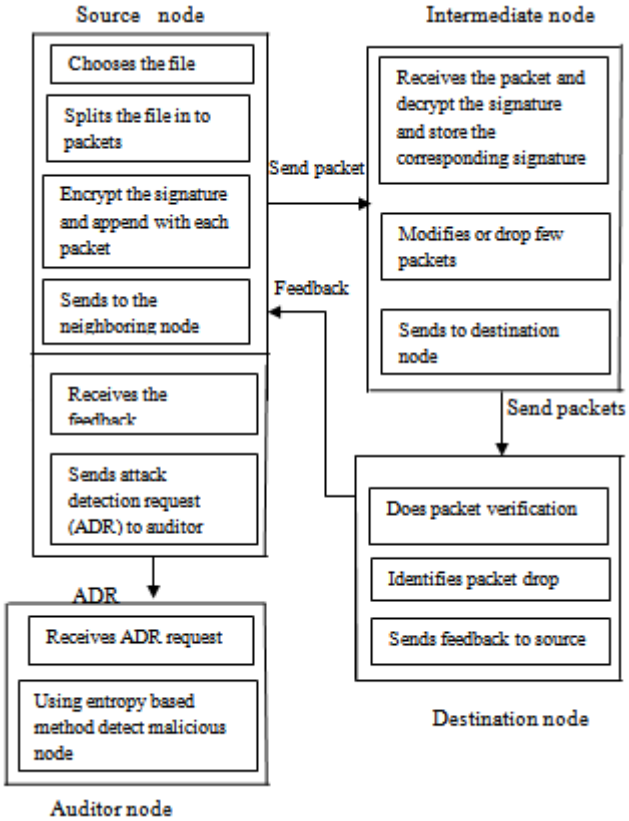

Fig 2: working of system model

IV. Simulation Setup

The proposed form is simulated using Network Simulator (NS) with its version 2.35. The required system parameters are configured using the TCL Wireless network is generated and aodv routing protocol is used for transferring the packets from source to destination. Total 55 packets are sent from source to destination from that 12 packets are dropped in intermediate nodes due to link error and 22 packets are dropped by malicious node in the path. All the given parameters in Table I have to be set first. The nodes are placed at a position initially.

Table I. Parameter Used In Simulation

Parameters	Value
Simulator	Network Simulator 2
Topology	Random
Interface Type	Phy/WirelessPhy
channel type	Channel/WirelessChannel
MAC type	Mac/802_11
radio-propagation model	Propagation/TwoRayGround
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/OmniAntenna
max packet in ifq	55
number of mobile nodes	50
time of simulation end	240sec

V. Simulation Results

In this an attempt has been made to find impact of malicious node in AODV routing protocol. In order to find the performances metrics such as throughput, packet delivery ratio, packet drop ratio and end to end delay with and without malicious attack and channel error. We designates few nodes as malicious node in the network. Where blue line in the graph indicates output without malicious attack and link error and red line indicates output with malicious attack and link error.

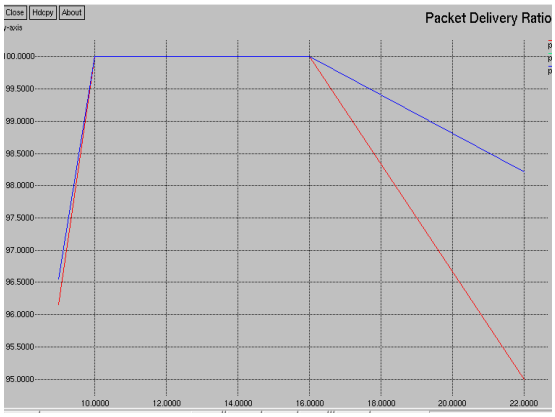

Fig 3: xgraph of packet delivery ratio with and without malicious malicious attack and link error in wireless network

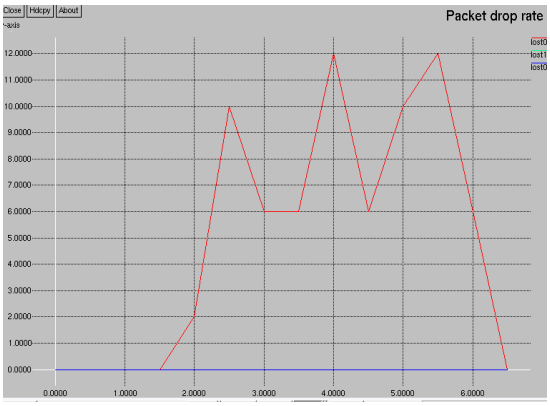

Fig 4: xgraph of packet drop with and without attack and link error in wireless network

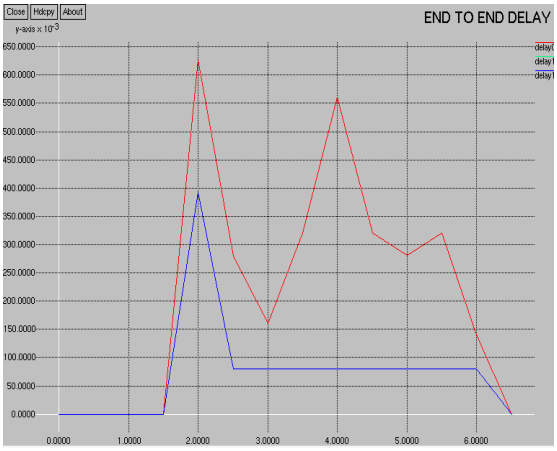

Fig 5: xgraph of average end to end delay with and malicious without malicious attack and link error in wireless network

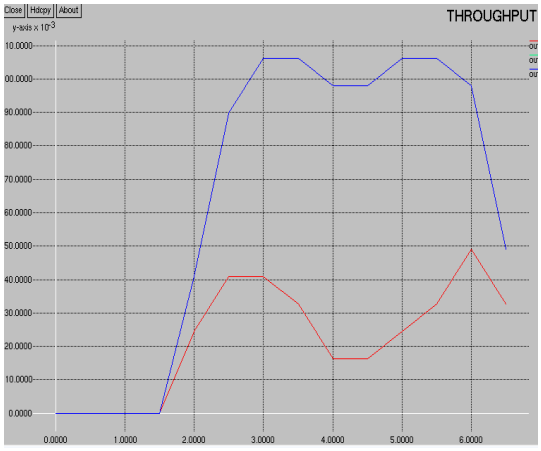

Fig 6: xgraph of throughput with and without attack and link error in wireless network

VI. Conclusion

We have showed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes. By doing so, a mutual communication process exist between sender and destination node. Through the simulation, this method exhibits large effectiveness in detecting packet dropping attacks. 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.

Some open issues remains to be explored as a upcoming work such as to decrease the computation overhead at the source, a packet-block-based method has to be proposed, which allows one to deal detection accuracy for lower computation complexity.

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, vol. 14, no. 4, april 2015*

[2]. J. N. Arauz, 802.11 Markov channel modeling, *Ph.D. dissertation,School Inform. Sci., Univ. Pittsburgh,Pittsburgh, PA, USA,2004.*

[3]. [3] G. Ateniese, S. Kamara, and J. Katz, Proofs of storage from homomorphic identification protocols, in Proc.Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319333

[4]. L. Buttyan and J. P. Hubaux, Stimulating cooperation in selforganizing mobile ad hoc networks, *ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.*

[5]. 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*

[6]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, *in Proc. ACM MobiCom Conf., 2000, pp. 255–265.*

[7]. D.B.Johnson, D.A.Maltz, and J.Broch, DSR: the dynamic source routing protocol for multi-hop wireless adhoc networks , *Addison –Wesley, Pages 139-172, 2001.*

[8]. Z.Alexander, Performance Evaluation of AODV Routing Protocol: *Real-Life Measurements, SCC,June 2003.*

[9]. Kejun Liu, Jing Deng,Pramod K. Varshney, and Kashyap Balakrishnan, An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in Manets *IEEE Transactions On Mobile Computing, Vol. 6, No. 5, May 2007*

[10]. Hongjun Dai, Yu Liu, Fenghua Guo and Zhiping Jia A Malicious Node Detection Algorithm Based on Principle Of Maximum Entropy In Wsns *Journal Of Networks, Vol. 7, No. 9, September 2012*

[11]. Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, and Taehoon Kim, Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks *IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings.*