Truthful Detection of Packet losses using Homomorphic Linear Authenticator in Dynamic Environment

J. Jeno Mactaline Pears*, D.C. Joy Winnie Wise
Department of CSE with specialization in networks, Francis Xavier Engineering College, Vannarpettai, Tirunelveli-627003, Tamil Nadu, India
***Corresponding author: E-Mail: jenopears25@gmail.com**

ABSTRACT

A wireless ad-hoc network is a redistributed type of network. In which the communication links are wireless and nodes in the ad-hoc network are ready to transfer a data to neighboring nodes and here determination of nodes which can forward data is dynamically depended on the network topology. It refers to the infrastructure and makeup of the network as a whole. A packet loss is a major problem in packet transmission. There are two reasons that providing packet losses are link failure and malicious attack in wireless ad hoc network. While observing a continuous packet losses in the network for determining whether the packet drops are occurred by link errors or by the joined effect of link errors and malicious drop. Homomorphic Linear Authenticator (HLA) mechanism can find the misbehavior node and also the link error by the auditor node. But these mechanisms are limited to static or quasistatic networks. The changes on topology and link characteristics have not been considered. A new proposed mechanism is a combination of HLA with Volcano Routing Algorithm (VRA) which can successfully transfer a data packet in dynamic topology.

KEY WORDS: packet loss, Attacker Detection, Homomorphic Linear Authenticator (HLA), Volcano Routing Algorithm (VRA).

1. INTRODUCTION

In networks the data packets transfer from source node to destination node throughout the intermediate nodes. The malicious node can act as a normal intermediate node until it discover the actual path from source to destination when the malicious node added into the routing path, the misbehaving node starts to discard the packets This is called as persistent dropping. These packets dropping completely increase the packet dropping ratio of the network. But it is very simple to identify persistent dropping.

Selective dropping is a second type of packet dropping. It is quite different from persistent dropping. Here malicious node analyze the needs of various packets and drops those packets that are very essential. The selective dropping also increases the packet loss ratio of the network. But here the possibility of detecting dropped packet is very small than the persistent dropping. Analyzing selective dropping is more complex in a highly dynamic environment because it is needs to finds the packet drop is intentional or unintentional. Intentional packet dropping is occurred by attacker's node and unintentional packet dropping is occurred by harsh channel conditions. The link error mainly caused in the open environment. Therefore the attacker may use the harsh condition to drop the minimum amount of packets. The packet dropping rate should be higher than the link error packet dropping for the accurate detection.

The algorithm helps to detect the malicious packet drop. The packets those are lost during transmission help to find whether packet dropping is caused only because of link error or by the joined effect of both link error and malicious packet drop. Evaluation of cooperation in between the transmitting nodes is very important. To ensure the information provided by each node HLA cryptographic primitive is used proposed by Tao Shu and Marwan Krunz (2015). This mechanism provides some extra new features which include privacy preservation and reduce overheads between the intermediate nodes. But here frequent changes on topology and link characteristics have not been considered. Traditionally, routing in a network is considered to be a two-phase process. In the route-discovery phase, a route is established between all source-destination pairs. Figure.1, show that the type of routing process in a Mobile Ad hoc Network.

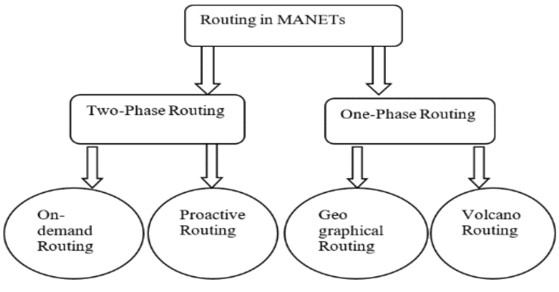

Figure.1. Routing in Mobile Ad hoc Network

The proposed an alternative one-phase routing algorithm is the Volcano Routing Algorithm (VRA), which does not need geographic information. VRA is a simple and fast method for routing packets in a dynamic network. The combination of HLA with VRA helps to reduce the link failure and malicious attack and improves packet delivery ratio. It does not consider the topology of changes, and movement model of the nodes but VRA guarantees to deliver packets to their destinations.

Related Works: Packet dropping and malicious packet attack are the major problems in Wireless Ad-Hoc network. Various packet dropping detection scheme have been discussed here.

Serrat-Olmos (2012), has proposed a watchdog detection scheme. The watchdog detection scheme is a best technique for finding misbehavior node during data transmission. Here, each node in a network has a watchdog agent to store a packet replica before the transmission of that packet. This technique is helpful to finds the packet loss in the transmission. Due to False misbehavior and insufficient transmission power, this technique fails. And it also causes receiver collision problem.

Yaohui Wang and Xiaobo Huang (2010), proposed Analysis of Intrusion Management System Technology. Here, the authors introduce an invasion supervision system, which can constitute for these deficiencies. Intrusion Detection System (IDS) is a fast growth kind of security object which follows the firewall. By examination of the network traffic, it discovers the network system if it has a breach of security strategy and attack symbols. It categorizes intrusion, Prohibits network traffic if required and notifies in real-time. When it discovers the attack, it not only files the record and the alarm, but also alerts the administrator of dynamic protection approach to attain appropriate counter measure, and enable the emergency repair to restore the system in a sensible way.

Badach and Belmehdi (2012), proposed an mechanism to cope with packet droppers. The core of the aim is that all intermediate nodes need to acknowledge the entry of the packet. Using this acknowledgement, the source node desingn a Merkle tree and compared with the values of the tree rout with a pre calculated value. If both values are equal then the end-to-end path is packet droppers free.

Rohit Pal (2013), gave a description of various ideas on security of Ad hoc networks as well as counter work for Black Hole Attack. A Combat Approach for Black Hole Attack is actually based on Cooperation of all the nodes in MANET. In this Approach each individual node act as intrusion detection system and monitors each request that it receives to avoid the attack

In Tao Shu and Marwan Krunz (2015), Homomorphic linear authenticator (HLA) based on the auditing scheme is developed that allows the Auditor or detector to verify the packet loss information during transmission informed by nodes. The Dynamic Source Routing algorithm is use to find the optimal path for transmission. And there is no algorithm for transfer a data packet in dynamic environment. This mechanism only give a status of lost data packets.

2. PROPOSED DETECTION SCHEME

Overview: The frequent changes of topology carried out in a network. The new detection scheme is based on simple and fast method for routing packets in a dynamic network and finds the packet loses. Alternative one-phase routing algorithm called as Volcano Routing Algorithm (VRA) is proposed. VRA routes packets by locally balancing the load.

HLA with Volcano Routing Algorithm: Consider P_{sd} be an arbitrary path in a network. The path should be as $n_1, \ldots, n_k$, where n_1 is the upstream node of n_k, Routing in ad-hoc network is very complex because topology can change very rapidly. The proposed scheme of HLA with volcano Routing Algorithm helps to detect the packet losses effectively.

Figure.2, illustrates the system design of the proposed scheme. Initially Source node ready to transfer a packet during transmission packet losses will occur. At that situation, the sender node can get a feedback from the receiver node. Then the sender can invoke the HLA mechanism to find the unwanted link and the loosed packets and also ensure the packet loss caused by the malicious attack or link error. Then it eliminate the misbehaving nodes and resent the packet for reducing packet losses. But these mechanisms will not works in dynamic environment and frequent changes on topologies does not be considered. Topological changes can cause high data packet losses and link errors. The proposed scheme of HLA with Volcanic Routing Algorithm can route packets successfully in dynamic topology.

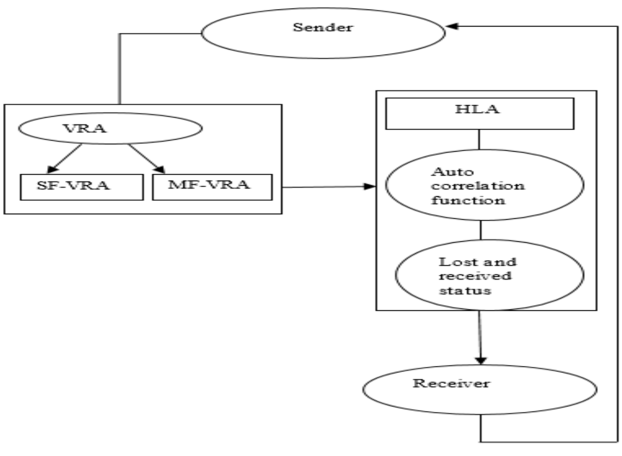

Figure.2. System Architecture

Single-Flow Networks: Single-flow networks are the network with only one flow (S, D, F), where S is the source node, D is the destination node, and F is the flow of maximum packets. It describes how VRA works in single-flow networks and prove its stability.

Single-Flow VRA (SF-VRA): Here the potential function associated with node v at time t, denoted by Pv (t), as the number of buffered packets at node v at the beginning of time slot t. During any time slot (t), the following steps are performed in order.

At the beginning of the time slot, N packets are generated by the source node.

Each link (s, d) for which Ps (t) − Pd

(t) ≥ Δ, is marked active. Here, Δ ≥ 0 is a pre-specified parameter which is called the transfer threshold. All other links are marked inactive.

If the amount of packets residing at node s, which is Pd (t), is greater than or equal to the number of active outgoing links adjacent to v then each such link transfers one packet from v to its neighbors. Otherwise, node s chooses Pd (t) of its active outgoing links, and each of these links transfer one packet from v to a nearby nodes.

If the packet which has reached the node D is eliminated from the system. Step (ii) is run in parallel on all links of the network, and step (iii) is run in parallel on all nodes and active links of the network. Note that the potential function Ps (t) is updated instantaneously after a data packet leaves node v or if a packet arrives at v.

Theorem 1: Let us takes a network G = (V, E (t)) with a single flow (S, D, F). If the min capacity of any cut C separating the nodes S and D is at least F, then network remains strictly stable under SF-VRA. Instead of proving Theorem 1, we will prove the following stronger result.

Theorem 2: Let us consider a single-flow network G = (V, E (t)) with flow (S, D, F) running SF-VRA. Let as assume that the minimum capacity of any cut C separating the nodes S and D is at least F. Then, for any subset of nodes U such that |U | = k, and at any time slot (t), the total amount of packets residing in U, denoted by $P_U(t)$ is at most;

$$B(k) = \Delta \times [Nk - \frac{k(k+1)}{2}] + k$$

Where N is the total number of nodes in the network (i.e. N = |V |) and Δ is the transfer threshold of the SF-VRA.

Multi-Flow Networks: Consider a network there are two flows, one from node 1 to node 4, and one from node 4 to node 1, each generating one packet every other time slot. Since the amount packets in nodes 2 and 3 are always the same, if we use SF-VRA, no packets make it across the middle link (2, 3). Thus, the considered network is unstable.

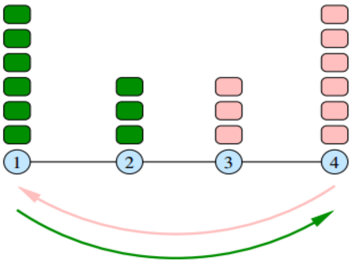

Figure.3. Multi flow Networks

Time Division VRA (TD-VRA): Here divide the time between the K flows, i.e. at time slot (t) the network will be completely dedicated to the (t mod K + 1)-th flow, and use SF-VRA to route packets belonging to this flow.

Theorem 3: consider a multi-flow network G = (V, E(t)) with K flows (Si , Di , Fi). Let $F = max_{i=1}^{k}$ {Fi}. If for any cut C that separates Si and Di. For some i (1 ≤ i ≤ K), Min Cap(C) ≥ KF then the network will be stable under TD-VRA.

Maximum Pressure VRA (MP-VRA): During the time slot t, need to denote the amount of packets corresponding to flow i at node v with $P_v^i(t)$. At time slot (t), each link (v, w) computes

$$i^* = \arg\max\{P_v^i(t)\text{-}P_w^i(t)\}$$

Routing Path Length: This method determines the distance of the path taken by a packet compared to shortest-routing path. Note that no matter what the routing scheme is, it is not always possible to route all packets on the shortest path. A simple shortest path routing scheme can route all packets on the shortest path. The following theorem, shows that the same is true with high probability in VRA.

Theorem 4: In a single-flow network with a fixed topology, if the amount of flow injected to the network is 1 − per time slot (for an arbitrarily small), then transfer threshold Δ for which SF-VRA almost surely (i.e. with probability one) routes packets on the shortest path from the source to the destination. In general, if the demand of the flow is D −, by choosing appropriate Δ we can show that packets take the first D disjoint shortest paths with probability one.

System modules:

Network Formation:

- 100 numbers of nodes are deployed with 1500 x 1500 in network animator area.
- The parameters such as, transmission range of each node, maximum speed of a mobile node, Communication range.

Packet Transmission Using VRA:

- Volcano Routing Algorithm (VRA), it does not require geographic information. VRA is a simple and fast method for routing packets in a dynamic network.
- VRA routes messages by locally balancing the load between nearby nodes.
- The length of the path taken by packets under VRA is near optimal (i.e. shortest path), when the network topology is fixed.

Audit Phase:

- Auditor Ad is presented in the network topology.
- Ad is independent in the sense that it is not associated with any node in P_{sd} and does not have any knowledge of the secrets (e.g., cryptographic keys) held by various nodes.
- The auditor node is responsible for finding misbehaving nodes on demand.
- Specifically, assume Sender S gets a feedback from Destination D when Destination suspects that the route is under attack.

Detection Phase:

- Detecting malicious nodes may not be a easy in highly mobile networks, because the fast-changing topology of such networks makes a routing path dynamically
- In such a situation, maintaining stable connectivity between nodes is a major problem.
- The function fc(i) can be calculated.
- Sequences of M packets are forwarded continuously over the path. By observing whether the transmissions are successful or not, the receiver obtains a realization of the channel state (a1. . . aM), where aj € {0, 1} for j = 1, . . . ,M.
- In this sequence, “1” denotes the packet was successfully received, and “0” denotes the packet was dropped.

3. SIMULATION RESULTS AND DISCUSSIONS

The simulation results performed using the network simulator ns2 version 2.31. Here, evaluate the performance of VRA using simulations. All nodes are distributed on a square surface of unit area. Examine the performance of VRA based on several metrics such as packet loss. The major objective of simulation is successfully detecting the attackers. Here rectangular shape area is selected for good node scattering and collaboration. Initially, 31 nodes are deployed. The Source node can transmit a data through a path as 28.12.23.26.26.23.0. The auditor node can find the misbehaving node (12) by detector node. Detector node is the previous node of the misbehavior node. Then the auditor eliminate that misbehaving node and quickly detect the optimal another routing path. And HLA scheme uses to detect the collaboration between the lost packets to find whether the dropping is occurred by link error or malicious attack. Table.1, shows the bitmap. It maintains the detector and attacker list. In each path detector node is the previous node of the attacker node.

Table.1. packet loss bitmap

Detector	Path	Attacker
28	28.12.23.26.26.23.0	12
16	19.16.9.12.0	9
13	13.21.4.0	21

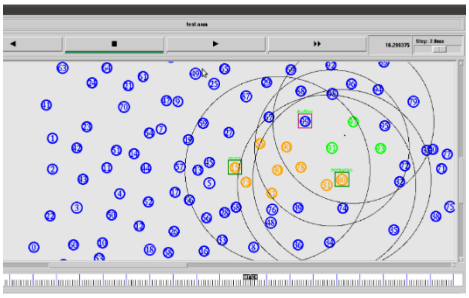

Figure.4. Packet Transmissions in Dynamic Environment

Figure.4, denotes how the proposed system of HLA with Volcano Routing Algorithm can helps to transfer a data packet in mobility network. Here simulation contains the 100 nodes and nodes 15 and 80 will be considered as a source to destination. The nodes colored with yellow are star topology and nodes colored with green are considered as a tree topology. While transmission the destination node will be disconnected from star topology and joined with tree. Proposed algorithm helps to detect the destination by the auditor node 99. Auditor node gather the packet from the source and by the load balancing method it can find the destination even dynamic environment. The new scheme can reduce the packet dropping and increase the throughput.

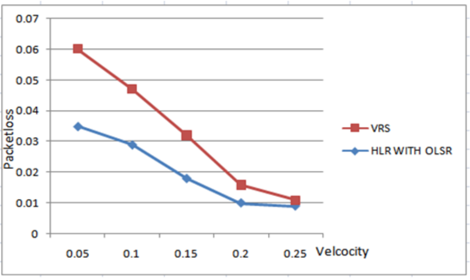

Figure.5. Packet loss Ratio in Volcano Routing Algorithm

Figure.5, illustrate the Time vs packet loss graph. It shows the packet loss ratio of the proposed system. The previous method of HLA with OLSR does not perform in the dynamic Environment. The packet loss detection also low. The proposed scheme can detect the high packet loss

4. CONCLUSION

The overhead of VRA is very low. The execution time of the algorithm at each node v is O (KLv), where, Lv is the no of links connected to v and K is the no of flows in the networks. The amount of control traffic exchange between nodes will be low. The drawback is some packets might remain in the network for a long time before reaching their destination. Therefore, the packets Reordering is important, which makes VRA inappropriate for applications. It does not allow packet re-ordering. It will be considered in the next future work.

REFERENCES

Badach A, Belmehdi A, Fighting against packet dropping misbehavior in multi-hop wireless Ad-hoc network, Network and Computer Application, 35, 2012, 1130-1139.

Jeno Mactaline Pears J, Joy Winnie Wise D.C, Black Hole Attack Detection Using HLA With Optimized Link State Routing Protocol in Wannet, International Journal of Engineering and Computer, 5, 2016.

Proano A and Lazos L, Packet-hiding methods for preventing selective jamming attacks, Dependable and Secure Computing, 9 (1), 2012, 101–114.

Rohit Pal, Mukesh Azad and Santosh Kumar. Article: An Approach to Combat the Black hole Attack in AODV Routing Protocol, International Journal of Computer Applications, 77 (11), 2013, 13-19.

Serrat-Olmos, Hernandez-Orallo M.D, Cano E, Calafate J, Manzoni C.T, Accurate detection of black holes in MANETs using collaborative bayesian watchdogs, Wireless Days (WD), IEEE Conference, 2012, 1-6.

Tao Shu, Marwan Krunz, Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks, IEEE Transactions on Mobile Computing, 2015.

Yaohui Wang, Xiaobo Huang, Analysis of Intrusion Management System Technology, Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on , 1 (3), 2010, 23-25.