Prevention of Packet Dropping in MANET Using HLA

[1] Rekha , [2] Bhagavadgeeta , [3] Bharati S. Pochal

[1]PG Student, Department of Studies in Computer Applications, Visvesvaraya Technological University Centre for PG Studies, Kalaburagi, Karnataka, India

[2]PG Student, Department of Studies in Computer Applications, Visvesvaraya Technological University Centre for PG Studies, Kalaburagi, Karnataka, India

[3]Assistant Professor, Department of Studies in Computer Applications, Visvesvaraya Technological University Centre for PG Studies, Kalaburagi, Karnataka, India

Abstract: Wireless networks are gaining popularity to its peak today, as the user wants wireless connectivity irrespective of their geographic position. Adhoc wireless networks operate as peer to peer network model where all the functions are carried out by the nodes in the network. The scalability and mobility brought by these networks finds it useful in many applications. There are several issues in wireless communication, one such issue is Security. A malicious attack is an attempt made by a compromised node in the network or an external node to attack and modify the packets reduce the functionality of the target and degrade the network performance. The malicious attack often results in selectively dropping packets intended for destination critical to the network performance.

In this paper a Homomorphic Linear Authenticator (HLA) based public auditing architecture detection scheme to authenticate the reporting of the packet loss information by nodes is implemented. The advantage of this algorithm is secure communication, minimum packet drop and less control overheads. The simulation of the project is done in NS2 and various parameters like Delay, Throughput, Node Packet Delivery, packet drop are compared with malicious node and the after detection and removal of malicious node.

Index terms- Denial of Service , Jellyfish reorder , ACF , privacy Preserving Cryptography (SHI) .

I. INTRODUCTION

In MANET link error and malicious packet dropping are two sources for packet losses. Link errors are low connectivity between the nodes and the malicious packet dropping is caused due to intentional packet drops by the nodes. So we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. Satisfactory detection accuracy is not achieved by subsisting algorithms. To improve the detection accuracy, we propose by utilizing the reciprocity between the positions of lost packets, as calculated from the Auto-correlation Function (ACF). Auditing is done to verify the truthfulness of calculations of reciprocity between lost packets. To verify the truthfulness of the packet loss information reported by nodes Homomorphic Linear Authenticator (HLA) based detector is used. This construction leads to privacy preserving, incurs low communication and storage overheads. By using Advanced Encryption Standard (AES) algorithm end to end encryption is provided for secure routing. n a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes.

While observing a sequence of packet losses, we are interested in determining whether losses are due to link errors only, or due to the combined effect of link errors and malicious drop. We are especially interested in insider's attacks, whereby a malicious node that is part of the route exploits its knowledge of the communication context to selectively drop a small number of packets that are critical to network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads.

II. LITERATURE SURVEY

In [1]] investigated the recently developed security provisions for VANET. Investigation covers various threats (Repudiation, Wormhole, Spamming, Replay, Jamming, DoS, DDoS and Black Hole etc.), issues and remedies. Study shows that threats can be categorized on the basis of V2V and V2I. It also compares the various simulation tools i.e. NCTUns, NS-2, Qualnet, GrooveNet and TraNs etc.

In [2] developed an algorithm to identify the DoS attack over VANET, called EAPDA. It uses time slots and Threshold values. Communication gap is used to identify the intruder nodes. Finally, entire network is isolated from detected threat. Simulation results show that it enhances the Throughput of the network and does not produce False alarms.

In [3] conducted a survey of the DDoS and Wormhole attack and compared various existing prevention schemes. Study shows that FireCol method can reduce the intensity of the attack over network where as Traffic Matrices can be used to monitor the traffic for P2P based applications. Use of Bloom filters can protect the routing information. Survey also includes the comparison of these methods.

In[4] explored the impact of DoS over VANET and proposed a solution based on game theory. Proposed scheme monitors the packet losses for each vehicle present in the current network and tries to enhance their performance. If any vehicle does not perform well, it can be considered as a malicious node. It can adopt the mobile environment and uses different game stages to filter out the attack.

In[5] developed a authentication method to secure the group communication over VANET. Keys are produced w.r.t. current Time slots and messages are signed and verified to ensure the secure data exchange. Intrusion can be detected on the basis of location and time updates. Simulation results show that it can perform under compromised situation and can enhance the network performance by maintaining the PDR.

III. PROPOSED SYSTEM

To expand a precise algorithm for detecting discriminating packet drops. HLA algorithm is used and it also offers a straight and openly demonstrable conclusion data as evidence to sustain exposure pronouncement.

HLA Detector interacts with each node in the network and make sure that all the nodes are properly connected or not in the network. If one of the nodes is malicious in the path then the packet transfer is stopped and then another optimal path is selected eliminating the malicious node. This decision is taken by the detector.

Denial-of-Service attack As a result of this drastic Denial-of-Service attack network becomes debilitated by fencing off the network topology.

Jellyfish reordering attack The reorganization attack. Jellyfish attack" is an occurrence that activity the close to close crowding control tool of TCP.

Blow fish algorithm While each node must rely on supplementary nodes deliberate for sustain into routing as well as forwarding packets to the target. The transitional nodes might be in concurrence to forward the packets although really collapse or vary them as they are mischievous. This work provides a way out to recognize cruel nodes in wireless "Ad hoc networks"in the course recognition of malicious communication transmissions in a network. Furthermore to prevents the network from the malicious nodes by using the blow fish algorithm, in order to provide the safety measures to the network by message encryption mechanism. In the proposed method, the detection of malicious node is performed by link error rate and malicious pack drop and then security is provided through blow fish algorithm. Finally, by evaluating the recognition rate and the effectiveness of proposed method with the parameters like throughput, packet delivery ratio and delay.

The main goal is to determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. Satisfactory detection accuracy is not achieved by subsisting algorithms. To improve the detection accuracy, we propose by utilizing the reciprocity between the positions of lost packets, as calculated from the Auto-correlation Function (ACF). Auditing is done to verify the truthfulness of calculations of reciprocity between lost packets. To verify the truthfulness of the packet loss information reported by nodes Homomorphic Linear Authenticator (HLA) based detector is used. This construction leads to privacy preserving, incurs low communication and storage overheads.

To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This architecture is privacy preserving, collusion proof, and incurs low communication and storage overheads. Through extensive simulations, we verify that the proposed mechanism achieves significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.

To enhance the detection accuracy using correlations between the positions of lost packets, as calculated from the auto-correlation function(ACF) and homomorphic linear authenticator (HLA) that allows the detector to verify the truthfulness of the packet loss information reported by nodes. In addition detection mechanism should provide is privacy preserving, incurs low communication and storage overheads.

The work includes some of the objectives and those are:

- ❑ To improve the detection accuracy, we propose by utilizing the reciprocity between the positions of lost packets, as calculated from the Autocorrelation Function (ACF).
- ❑ To guarantee the packet loss information reported by individual node is truthful or not nodes Homomorphic Linear Authenticator (HLA) based detector is used. Verifying the truthfulness is necessary because sometimes invader reports fallacious information to evade being diagnosed.

- As intrusion prevention mechanisms, such as encryption and authentication, are not sufficient regarding security, we need a second line of defense, Intrusion Detection.
- In the proposed method, the detection of malicious node is performed by link error rate and malicious pack drop and then security is provided through blow fish algorithm.
- time-space cryptography and modified SHA-1 (mSHA-1) hash function for verifying whether packets are Reorder or not. .
- 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.

To improve the detection accuracy, we propose by utilizing the reciprocity between the positions of lost packets, as calculated from the Auto-correlation Function (ACF). Auditing is done to verify the truthfulness of calculations of reciprocity between lost packets. To verify the truthfulness of the packet loss information reported by nodes Homomorphic Linear Authenticator (HLA) based detector is used. This construction leads to privacy preserving, incurs low communication and storage overheads. By using Advanced Encryption Standard (AES) algorithm end to end encryption is provided for secure routing.

ARCHITECTURE OF THE SYSTEM

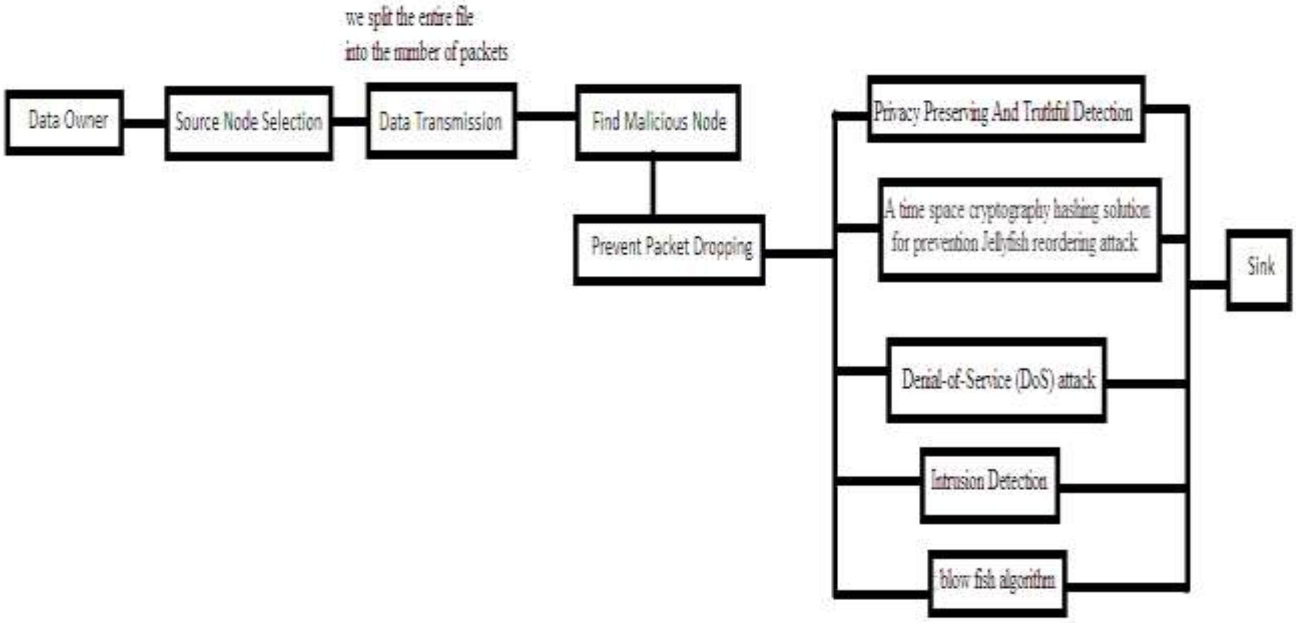

we split the entire file
into the number of packets
Data Owner
Source Node Selection
Data Transmission
Find Malicious Node
Prevent Packet Dropping
Privacy Preserving And Truthful Detection
A time space cryptography hashing solution
for prevention Jellyfish reordering attack
Denial-of-Service (DoS) attack
Intrusion Detection
blow fish algorithm
Sink

Fig.1. System Architectural Design

1. **Node Deployment: -** In remote system is exemplary of both jump along PSD as incidental process that recognize great quality and awful state. Parcels transmit through the great quality state are prospering, and bundles transmitted in the awful state are vanished. The topology of portable system is changes energetically on account of that involvedness happens in finding of bundle drops in organize. For this situation, keeping up steady network in the midst of hubs is a superior nervousness than distinguishing noxious hubs. , or is an aggregate impact of connection blunder and noxious drop.
2. **Send Message: -** while conveyance parcel or message on organize, there is a self-administering reviewer Ad hoc arrange. Specially appointed is self-deciding in the shrewdness that it isn't connected amidst any hub in PSD. The inspector is reliable for recognizing noxious hubs on assert. Specially appointed requires gathering guaranteed in succession from the hubs on course PSD.
3. **Attack: -** Here the framework relies upon neighbor hubs to distinguish the malignant hub. A hub which drops the greater part of the parcels will get a terrible notoriety by its neighbor hub. This data is passed to every one of the hubs in the system and is utilized to choose courses for the following parcel transmission. A high parcel dropping hub is wiped out from the courses.
4. **Packet Dropping Detection and Prevention: -** This detects the reciprocity amongst the misplaced packages over both hop of the track. The sequence of number of packets that are spread back to back over a wireless channel but below dissimilar packet falling environments, packet damage is recognized. And if packet loss is present then indicate it by 0

otherwise set 1.using different algorithms like, HLA, jellyfish reordering, Blowfish algorithm, Privacy Preserving algorithm we can prevent packet dropping.

IV. RESULTS AND DISCUSSIONS

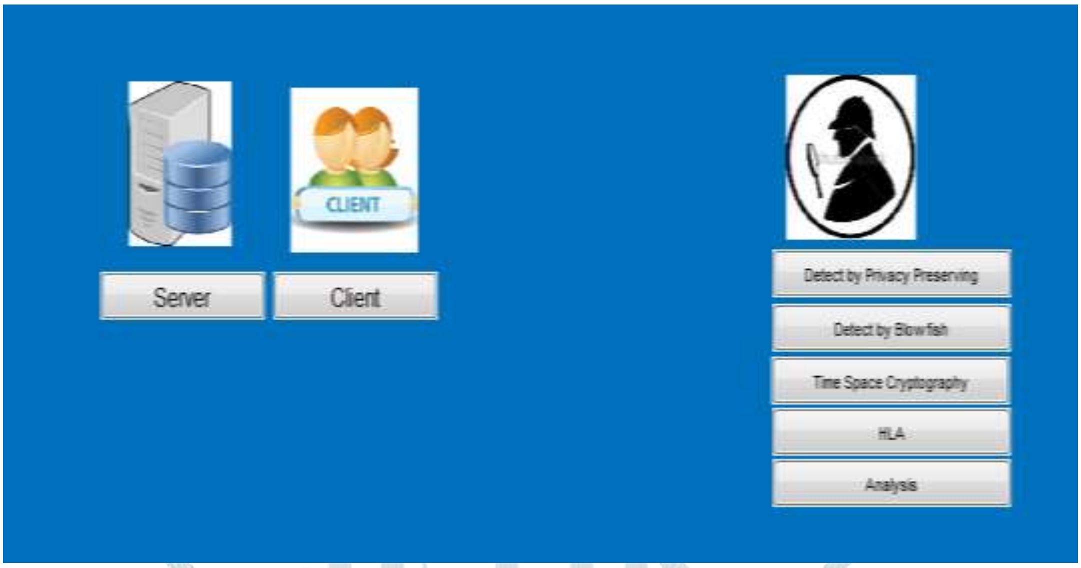
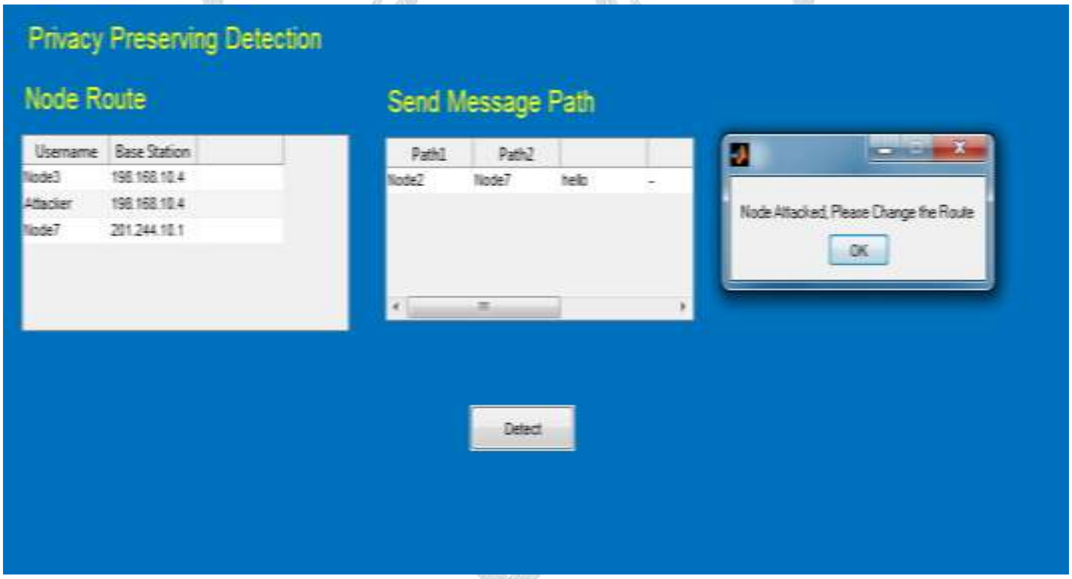


Fig.2. Home Page


Privacy Preserving Detection

Node Route

Username	Base Station
Node3	198.168.10.4
Attacker	198.168.10.4
Node7	201.244.10.1

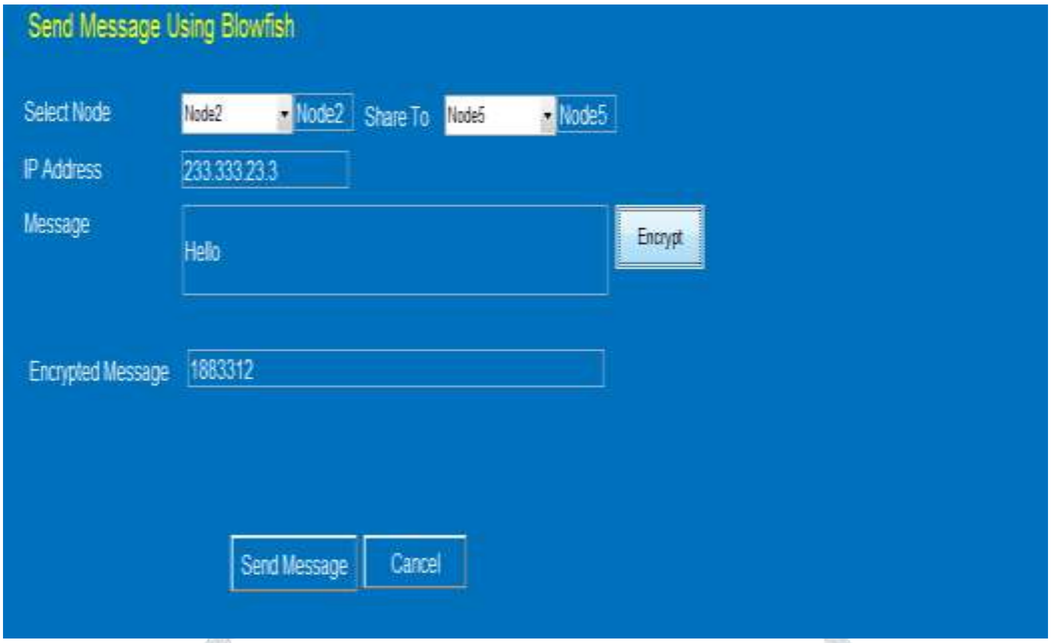
Send Message Path

Path1	Path2		
Node2	Node7	hello	-

Node Attacked, Please Change the Route

Fig.3. Implementation of Privacy preserving algorithm

Jellyfish attack is a new denial of service attack that exploits the end to end congestion control mechanism of TCP (Transmission Control Protocol).



Send Message Using Blowfish

Select Node: Node2 Node2 Share To: Node5 Node5

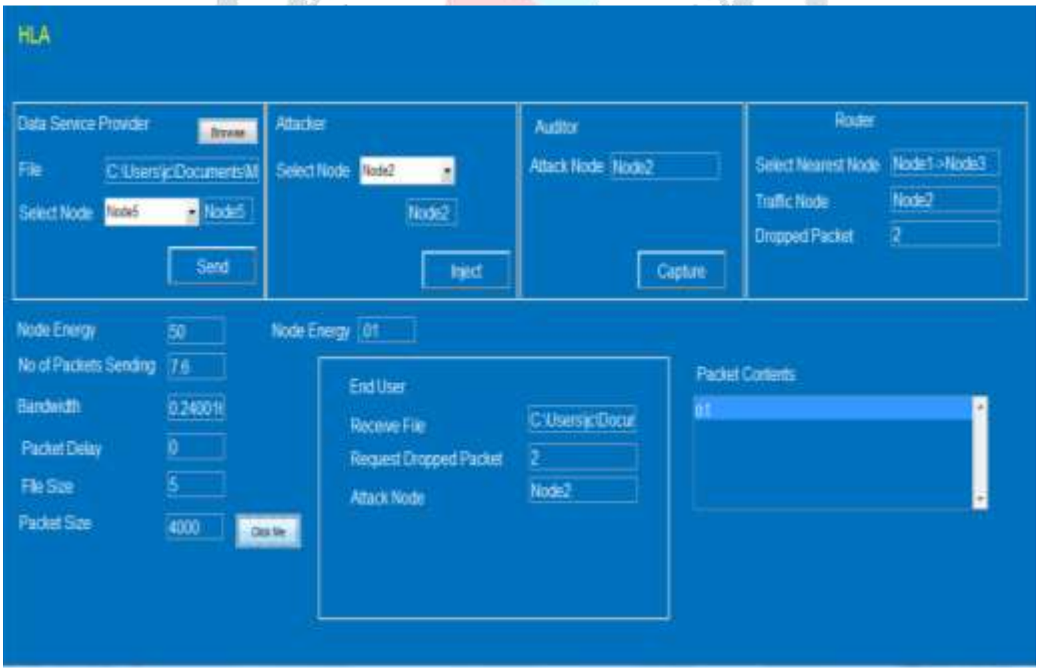
IP Address: 233.333.23.3

Message: Hello

Encrypted Message: 1883312

Fig.4. Implementation of Blowfish algorithm

By using the blow fish algorithm, in order to provide the security to the network by data encryption mechanism. In the proposed method, the detection of malicious node is performed by link error rate and malicious pack drop and then security is provided through blow fish algorithm. Finally, by evaluating the detection rate and the efficiency of proposed method along with the parameters like throughput, packet delivery ratio and delay.



HLA

Data Service Provider
File: C:\Users\jc\Documents\M
Select Node: Node5 Node5

Attacker
Select Node: Node2
Node2

Auditor
Attack Node: Node2

Router
Select Nearest Node: Node1->Node3
Trafic Node: Node2
Dropped Packet: 2

Node Energy: 50
No of Packets Sending: 7.6
Bandwidth: 0.24001
Packet Delay: 0
File Size: 5
Packet Size: 4000

Node Energy: 01

End User
Receive File: C:\Users\jc\Docu
Request Dropped Packet: 2
Attack Node: Node2

Packet Contents
01

Fig.5. Implementation of HLA algorithm

Homomorphic Linear Authenticator (HLA) based detector is used. Detector interacts with each node in the network and make sure that all the nodes are properly connected or not in the network.

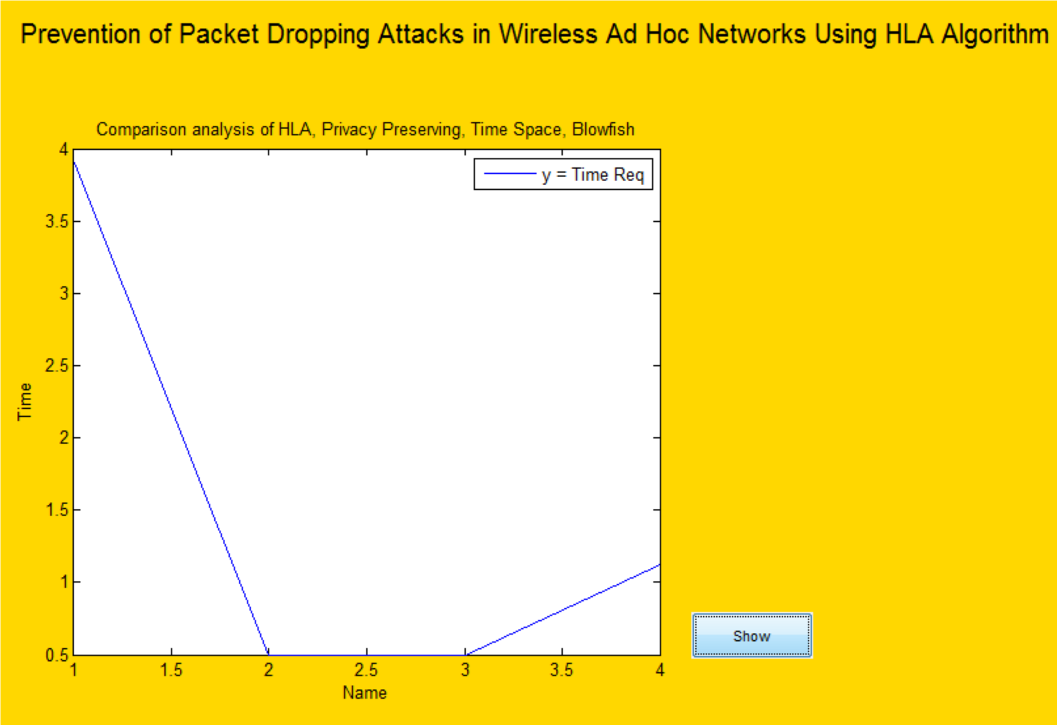

Prevention of Packet Dropping Attacks in Wireless Ad Hoc Networks Using HLA Algorithm
Comparison analysis of HLA, Privacy Preserving, Time Space, Blowfish
y = Time Req
Time
Name
4
3.5
3
2.5
2
1.5
1
0.5
1
1.5
2
2.5
3
3.5
4
Show

Fig.6. Comparison analysis of HLA , Privacy Preserving , Time Space Cryptography and Blowfish Algorithms

V. CONCLUSION

In MANET the packets are dynamically arranged. So, if any attack is happens over a network that can be recognized slowly because of the source node will not get the attack message soon. Using HLA algorithm numbers of auditors are placed in the network then the nearest auditor will send the attack message to the source node.

In proposed work the detection and prevention of packet loss can be made by using HLA algorithm in efficient manner. This work overcomes the problems like Link Error and malicious attacks. While sending a message, if any attacks is made then HLA algorithm cut the path and finds the shortest path to transmit the packets.

REFERENCES

[1] L. Bariah, Dina Shehada, Ehab Salahat and Chan Yeob Yeun, "Recent Advances in VANET Security: A Survey", Vehicular Technology Conference (IEEE-VTC Fall), pp.1-7, 2015.

[2] A. Singh, Priya Sharma, "A novel mechanism for detecting DoS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)", 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), pp.1-5, 2015.

[3] R.Saranya, Dr.S.Senthamarai Kannan,N.Prathap, "A survey for restricting the DDOS traffic flooding and worm attacks in internet", International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp.251-256, 2015.

[4] M. N. Mejri, Nadjib Achir, Mohamed Ham, "A New Security Games Based Reaction Algorithm against DOS Attacks in VANETs", 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp.837 – 840, 2016.

[5] G. Kumaresan, T. Adiline Macriga, "Group Key Authentication scheme for Vanet INtrusion detection (GKAVIN)", Wireless Networks, Springer, pp 1–11, 2016.