An Efficient Vehicular Ad-Hoc Network to Reduce The Loss of Packets

[1]Abinaya. M ,[2]Archana. M ,[3]Arul Arasi. M, [4] Bragadeeswari. K
[1,2,3,4]Students, Department of Computer Science and Engineering
Panimalar Engineering College
Chennai,India

Abstract— A Vehicular ad hoc network (VANET) is a technology which follows the concept of establishing a network of cars, a special class of MANET. VANET provides communication between vehicles intelligently via vehicle to vehicle communication or vehicle to road side unit communication. Thus the technology enables smart vehicles to communicate with each other thus forming a mobile network. VANET facilitates users with improved traffic efficiency and safety, early warning signals for vehicles and provision of better in-transit communication. Authenticated communication with successful data transmission becomes the prime requirements of VANET. However, packet loss increases when the number of vehicles increases in a network. In this we proposed an efficient and practical approach to prevent the loss of packets during the packet transmission by using an algorithm called Advanced Ad hoc Algorithm (AAA). Our proposed protocol has two modes, cupidus mode and the circuitus mode. Our proposed algorithm provides a successful packet delivery by finding the shortest path from the sender to the receiver by using the cupidus mode. The circuitus mode is used only when the cupidus mode fails. Furthermore, we simulated our protocol in order to analyze the network performance and the results show the feasibility of our proposed method in terms of successful packet delivery.

Keywords- Vehicular ad hoc network, beacons, uthentication, Pseudonyms, Road Side Unit(RSU),Advanced Ad-hoc Network,cupidus, circuitus.

I. INTRODUCTION

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network since VANET is a subset of Mobile Ad-Hoc Network (MANET). VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a wide range of network. Position of the nodes in VANET will be frequently changing due to high mobility and random speed of the vehicles. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Traditionally, VANET simulators consist of two components. One is the wireless network simulator and the other is the road traffic simulator. The protocol is simulated with the help of veins, that is an open source framework, which can offer unrestricted extensibility. Veins simulator requires OMNeT++ and SUMO framework for simulation. Veins are used because it can be used to solve challenges in VANET.

A vehicle periodically broadcasts traffic and safety related messages known as beacons. The vehicles communicate each other with the help of vehicle-to-vehicle (V-2-V) communication and with Road-Side Unit (RSU) with the help of vehicle-to-infrastructure (V-2-I) communication. Network performance can be made efficient only by minimizing the loss of packets. But increasing packet loss occurs when number of vehicles receives more packets due to minimized gap between them and therefore, experience more packet loss due to collision. In order to overcome this problem we use the algorithm called AAA.

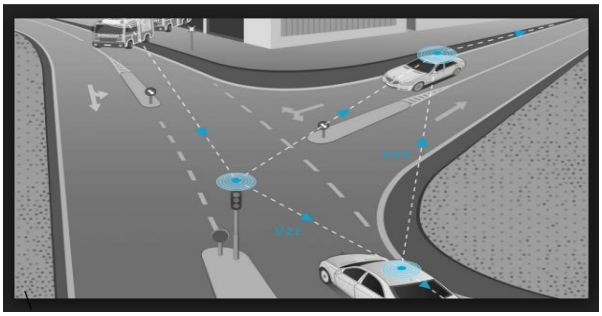


Figure 1. Typical VANET scenario.

II. LITERATURE REVIEW

A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET published on October 25,2016 by UBAIDULLAH RAJPUT, (Student Member, IEEE), FIZZA ABBAS, (Student Member, IEEE), AND HEEKUCK OH, (Member, IEEE) Department of Computer Science and Engineering, Hanyang University, South Korea stated a protocol with conditional privacy preservation. The protocol proposed a hierarchy of pseudonyms based on the time period of their usage. They proposed the idea of primary pseudonyms with relatively longer time periods that are used to communicate with semi-trusted authorities and secondary pseudonyms with a smaller life time that are used to communicate with other vehicles.

Most of the current pseudonym-based approaches are based on certificate revocation list (CRL) that are not very efficient and also suffer from trust issues related to certification authority. Their protocol only expects an honest-but-curious behavior from otherwise fully trusted authorities and protects a user's privacy until the user honestly follows the protocol. In case of a malicious activity, the true identity of the user is revealed to the appropriate authorities. Their protocol does not require maintaining a CRL and the inherent mechanism assures the receiver that the message and corresponding pseudonym are safe and authentic.

The performance of their proposed protocol is evaluated by comparing conventional beacons with the encrypted beacons of their proposed protocol with respect to mean end-to-end delay,

successful beacon delivery ratio (or successful packet delivery ratio), and total packet loss.

Their proposed protocol exhibits several advantages over current approaches such as less trust on Certification Authority (CA), revocation authority (RA) and road side unit (RSU) but no disclosure of valuable information in case of attacks on these entities. Usually, RSU are placed at road intersections with maximum number of passing by vehicles requesting RSU for pseudonyms.

Inorder to provide a valuable information successful delivery of packets must be done and can be achieved by making the sender to easily identify their receiver by means of an alternative protocol.

III. PROBLEM IDENTIFICATION

A. *Performance Matrix:*

The performance of their proposed protocol is evaluated by comparing conventional beacons with the encrypted beacons of their proposed protocol with respect to mean end-to-end delay, successful beacon delivery ratio (or successful packet delivery ratio), and total packet loss. It can be noted that the packet loss and end-to-end delay incurred by the beacons increases with the increase in traffic density and vehicles' speed. This is due to the packet collisions due to high traffic density, increasing speed of vehicles and packet loss while transmitting due to high packet reception rate.

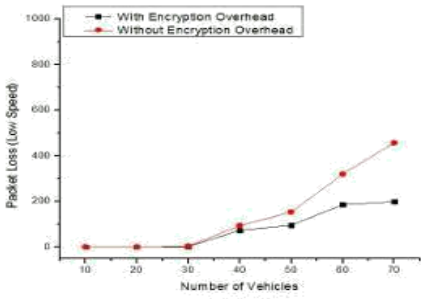


Figure 2. Problem identification graph

IV. RESULT ANALYSIS

The preservation and proposed the idea of two levels of hierarchy for the pseudonyms with different life time. The protocol also exhibits several advantages over current approaches such as less trust on CA, RA and RSU but no disclosure of valuable information in case of attacks on these entities. The analysis of the existing protocol is done with two perspectives. First is the security analysis and next is by providing communicational overhead in form of excess bytes due to the encryption. Base paper have proposed a hierarchical pseudonymous authentication protocol with conditional privacy.

A. *Security analysis*

In terms of Privacy Preserving Authentication, in case of the protocol, only RA has the secret key of the encrypted real identity (vehicle identity,VID). However, RA does not have access to the encrypted values in the database of CA. Moreover, the protocol requires that a user vehicle to acquire a new primary pseudonym after a certain time period that is set by CA, and therefore, the RSU will find it very hard to correlate a user because of his changing primary pseudonyms. At the RSU side, after every few message broadcast, a new secondary pseudonym is used. Therefore, it is very hard for an attacker to correlate the secondary pseudonyms of the vehicle. Even the message integrity is preserved by the protocol, non repudiation is provided by also providing prevention against replay attacks. However, the system provides guarantee for the anonymity of the honest vehicles.

B. *Attack scenarios*

Communication between all the participants is semantically secured since all the communication in the protocol is encrypted using the Elliptic Curve Cryptography (ECC). If an attacker tries to replay the message in any step , the replay attack will not be succeed sine nonce have been used. If an attacker tries to compromise a RSU it is not possible but if he tries to compromise a CA database the system become unsecured.

C. *Network simulation results*

The performance of the existing protocol is analysed in two major aspects. First is the performance of inter-vehicle beacon communication with respect to unsecure beacons and the next is the performance evaluation of RSU. The RSU performance is measured by evaluating any loss of packets while receiving requests from vehicles and issuing secondary pseudonym. This evaluation shows the ability of RSU to consistently provide secondary pseudonym to the vehicles in time without dropping any significant number of requests. But it should be noted that the packet loss and end-to-end delay incurred by the beacon increase with the increase in traffic density and vehicles' speed due to more collision.

From the result analysis of the existing paper the network performance gets affected due to loss of packets. In order to overcome the packet loss we have created our protocol by analyzing the results of the paper Analysis of Position Based Routing Protocols in VANET using NS2 Simulator published by Deepak Bindlish, Alka Jindal, Sanjay Batish and Amardeep Singh Dept. of Comp. Science, PEC University of Technology, Chandigarh, India. Their results stated that a good protocol must have an increased packet delivery ratio(PDR) and throughput and a decreased end to end delay.Thus from the result analysis a new algorithm have been designed to overcome the drawbacks in the existing paper.

V. EXISTING SYSTEM

In our existing protocol, two separate cryptosystems have been used, Paillier homomorphic cryptosystem and Elliptic Curve Cryptography. Paillier encryption, an asymmetric algorithm for public key cryptography which provides semantic security. Elliptic Curve Cryptography, a public key encryption technique based on elliptic curve theory, establishes equivalent security.

A user needs to register with the Certification Authority (CA) in order to get the primary pseudonym. The primary pseudonym has a life time and expires after that period of time. This period of time is denoted as TCA in the existing protocol and set by CA at the time of primary pseudonym generation. The sender vehicle (or initiator of the beacon message), denoted by Vi signs the beacon message with the private key whose corresponding public key is mentioned in the secondary pseudonym. The initiator then broadcasts the signed beacon message along with the secondary pseudonym.

CA initializes the system by establishing the domain parameters p, a, b, G, n and h.

The field is defined by p.

The cyclic group is defined by its base point G.

n is the order of G.

a, b are curve constant.

cofactor h = 1/n|E(Ep)|.

CA randomly chooses x ∈ Zp ∗ as its private key. RA generates a number of public/private ECC key pairs and provides CA the public keys, that are later used by CA for VID encryption.

A. *Vehicle egistration and primary Pseudonym generation*

During the registration, sender/initiator vehicle (Vi) generates a random number n (This value is encrypted in CA's Paillier public key) and a public/private ECC key pair PKi/SKi . Vi sends this information along with the VIDi to CA.

Step 1: The Vi sends this information to the CA via some secure channel. Step 1 is required only once.

Step 2:CA validates the VIDi . Upon verification it encrypts VIDi with one of the public keys generated by RA, encrypts n with its paillier public key PKCAP, generates an expiration time TCA for the primary pseudonym and creates DB.

Step 3: Once the TCA expires, Vi needs to acquire the primary pseudonym again. In this regard, Vi randomly select some n' , generates a public/private ECC key pair PK'' i /SK'' i , encrypts this data in public key of CA along with n and sends it to CA using 3G/4G communication.

Step 4: CA verifies this message with correct n, generates new expiration time TCA' , update its DB with new values of n' , PK'' i and the TCA' . CA repeats step 2, but encrypts the newly generated primary pseudonym in PK'' i and sends back to Vi .

B. *Secondary pseudonym generation*

Step 5: RSU periodically broadcasts a message announcing its presence which contains the public key of the RSU. Once a vehicle receives,it requests for the secondary pseudonym. The vehicle generates another ECC key pair (PK' i , SK' i). It encrypts this newly generated public key, its primary pseudonym, −n and a n once in RSU's public key and sends it to the RSU.

Step 6: RSU verifies CA's signature, encrypts −n with paillier public key of CA. RSU takes homomorphic sum of both(n)PKCAP and (−n)PKCAP , gets (R)PKCAP . Where (R)PKCAP =(n)PKCAP + (−n)PKCAP RSU sends (R)PKCAP to CA for verification.

Step 7: CA decrypts R, finds 0 (n + (−n) = 0) and sends verified message to RA otherwise sends not verified.

Step 8:Upon getting verification,the message from the sender Vi , RSU prepares a secondary pseudonym. It creates the expiration time TRSU , embed it with newly generated PK' i , signs it, encrypts in PK' i and sends it to Vi . Note that, PK' i has to be generated by Vi every time a secondary pseudonym is requested. However, a vehicle can pre-compute a pool of ECC key pairs

C. *Beacon broadcast*

Step 9: Vi signs the beacon message with the private key whose public key is contained by the secondary pseudonym, attaches with the beacon and broadcasts the message. The receiver of the message verifies it, by checking the RSU's signature and then verifies the beacon by Vi's signature with the help of PK' i contain in the secondary pseudonym.

D. *Vehicle revocation*

If a user is found to be involved in broadcasting a bogus message then the culprit is traced and revoked by the following ways:

The receiver presents the recordings of the malicious message (step 9) to the Law Enforcement Authority(LEA).

LEA contacts the RSU that signed the secondary pseudonym attached with the bogus message.

RSU provides LEA with the corresponding primary pseudonym.

LEA instructs the RA to provide the decryption key of the encrypted VID whose associated primary pseudonym is found to be malicious.

RA provides the corresponding decryption key to CA Along with are vocatio request.

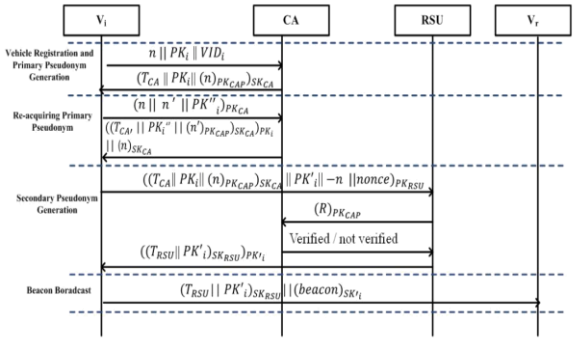


Figure 3. Working of the existing protocol

TABLE I. NOTATIONS USED IN THE EXISTING SYSTEM

Notations	Explanation
V_i	Initiator/Sender vehicle
V_r	Receiver vehicle
VID_i	Initiator's/Sender's vehicle ID
$PK_i, SK_i, PK'_i, SK'_i, PK''_i, SK''_i$	ECC public/ private key pairs of V_i
PK_{CA}/SK_{CA}	ECC public/private key pairs of CA
PK_{CAP}	Paillier public key pair of CA
PK_{RSU}/SK_{RSU}	ECC public/ private key pair of RSU
$T_{CA}, T_{CA'}$	Expiration time of primary pseudonym set by CA
T_{RSU}	Expiration time of secondary pseudonym set by RSU
Beacon	Typical VANET message

CA decrypt the VID of the malicious party and revokes it.

The contents of a beacon message are used to construct the traffic view. The typical transmission range of a vehicle is around 300 meters. Therefore, the contents of a bogus traffic report will be verifiable within minutes. The victim will immediately complain the LEA with the recordings of the bogus message. Therefore, the beacon messages needed to be recorded for a short time period with an upper bound of 30-60 minutes.

VI. PROPOSED SYSTEM

Our existing system provides security for the information that are transmitted from the source to destination but no guarantee towards the successful delivery of packets. To provide a successful packet delivery, we proposed an algorithm called Advanced Ad-hoc Algorithm.

Networks comprised entirely of wireless stations, communication between source and destination nodes will require traversal of multiple hops, as radio ranges are finite. In order to improve the efficiency of the network performance by overcoming the drawbacks of the existing system we proposed an algorithm named as Advanced Ad-hoc Algorithm (AAA).This algorithm follows a forwarding strategy, in which the data packets know the physical position of their destination. As the originator knows the position of its destination node so the hops are selected to forward the packets to the nodes that are closer to their destination. This process is repeated until the packets are successfully delivered to the desired destination. Nearest neighbor's physical position is gathered by utilizing beaconing algorithms or simple beacons.

Modes of AAA

- Cupidus mode.
- Circuitus mode.

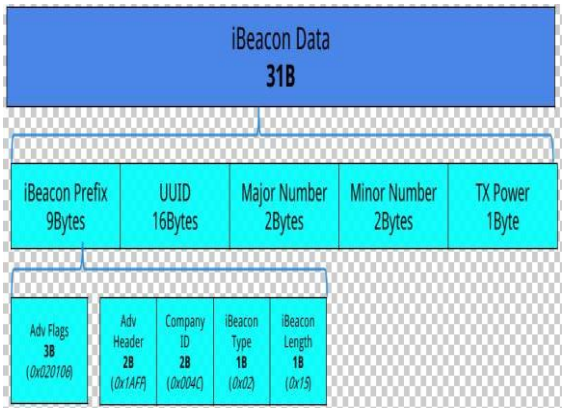


Figure 4. beacon data format

The AAA allows nodes to figure out the closest neighbors using beacons that are also close to the destination . Since AAA follows a forwarding strategy to calculate a path, that will send the information to the final destination using the most efficient path possible. It is possible only in the cupidus mode. If this mode fails then the Circuitus mode becomes active .The proposed algorithm depends on two dominant factors in the scaling of a routing algorithm,they are:

1)The rate of change of the topology

2)The number of routers in the routing domain.

The wireless routers called nodes should know their own locations and should try to find the closest router which is also the closest to the final destination.

A. The node finds its closest neighbor

A beaconing algorithm tells a node the locations of its neighbors. Periodically, each node will transmit a beacon to the broadcast MAC address containing only its own identifier (which is its IP address) and its location using two four-byte floating point values for the x and y coordinates, IP(x,y). Every node stores the position of it's one hop neighbors thus maintaining a location table. If a node doesn't receive a beacon from a neighboring node after a certain amount of time, the router will assume that the neighbor no longer exists and will remove it from its table of valid neighbors.

The source node S in fig5 transmits a beacon which contains it's IP address and location inorder to indicate it's position to it's neighboring nodes.

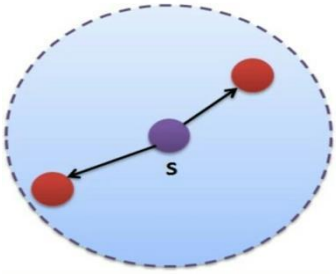


Figure 5. node S transmitting beacons.

B. About the cupidus algorithm

In cupidus algorithm, the network topology or prior route discovery are not taken into account since each node is aware of their own location

along with their neighbor node location and the destination node location.

Since the wireless routers know their own location, the cupidus algorithm will try to find the closest neighbor to the destination node. In the figure 6,an example for cupidus algorithm is shown, in which S denotes the source node and D denotes the destination node while W denotes the S's neighbor closest to D.

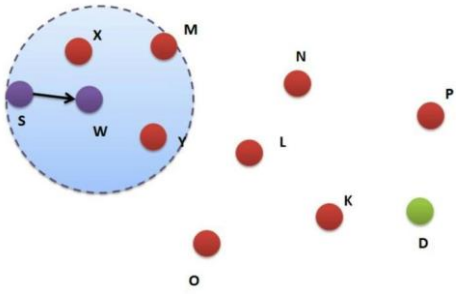


Figure 6. Cupidus algorithm example

The source S needs to send information to D so S uses cupidus algorithm to find the nearest neighbor. Using the cupidus algorithm S checks it's table and finds W as its nearest neighbor even though there are several nodes because W is the only node which is also nearer to the destination. Similarly node W will check it's table and finds Y to be it's nearest neighbor. Thus by following the algorithm, the information will be transmitted to D.

There also chances for the cupidus algorithm to chose more than one node as the nearest neighboring node to the destination but in such cases the available free node will be chosen. The drawback may occur when the network topology is like the one in the fig 7. When nose S is not having any neighbor more near to node D.

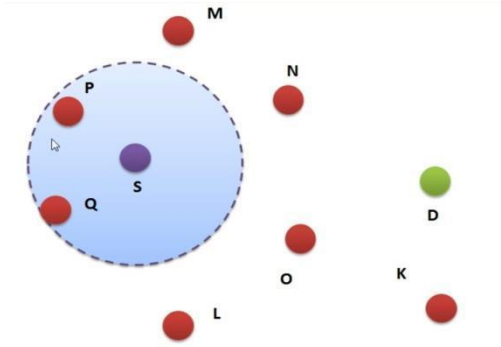


Figure 7. example of failure of cupidus algorithm

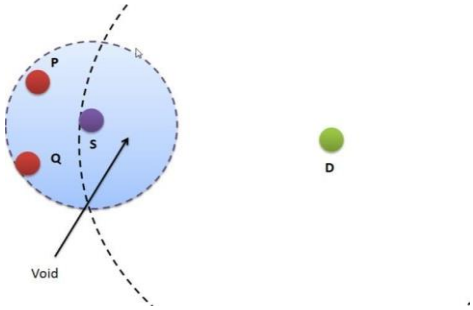


Figure 8. failure of cupidus algorithm

Lile in the fig 8,whenever a void region exist between the source and destination, the cupidus algorithm fails, so it activates the Circuitus mode.

C. About the circuitus algorithm

This algorithm uses the right hand rule. In right hand rule , the voids regions are exploited by traversing the path in counter clockwise direction in order to reach at specific destination. When a packet forward by source node, it is forwarded in counter clockwise direction including destination node until it again reached at the source node. According to this rule each node involved to forward packet around the void region and each edge that is traversed are called circuitus. Edges may cross when right hand rule finds a path that are enclosed in the void by utilizing heuristic approach. In fig 9, x the sender node follows the circuitus algorithm to transmit the data to D. it results in the tour x-v-u-D-x.

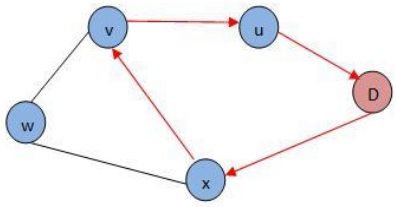


Figure 9. circuitus algorithm

Heuristic has some drawbacks besides it provides maximum reach ability to destination. When two edges get crossed the heuristic approach may fail. The drawback is that it removes without consideration of those edges which are repeated and this may cause the network partitions.

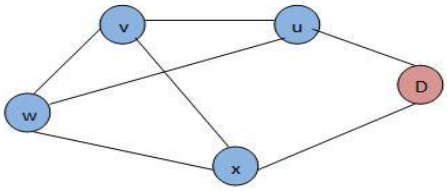


Figure 10. failure of heuristic approach.

It can also be avoided using another strategy called the Planarized Graph.

Fig 11 shows nodes x and D are connected by a planar graph. Then the graph divides the plane into faces. Line xD crosses one or more faces.

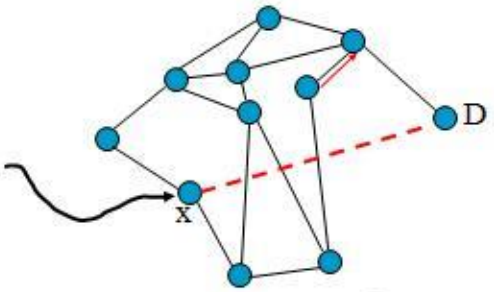


Figure 11. Circuitus algorithm example

The circuitus algorithm can again be switched to cupidus algorithm when the planner graph becomes a non planner graph.

D. Planarized Graph

When two or more edges cross each other in a single graph is called planar graph. Relative Neighborhood Graph (RNG) and Gabriel Graph (GG) are two types of planar graphs used to remove the crossing edges. Relative neighborhood graph (RNG) is defined as, when two edges intersect with radio range of each other and share the same area. For example, x and y are the two edges that share the area of two vertices x and y. The edge x, y are removed by using RNG because another edge from x towards v is already available Figure-12. Gabriel Graph (GG) is used to remove only those crossing edges which are in between the shared area of two nodes having the same diameter as the other nodes have. Figure-13 depicts GG which shows that the midpoint diameter is less than the diameter of node x or node y. Thus the edge from the x, y cannot be removed. So there is less network disconnection in the GG as compared to RNG.

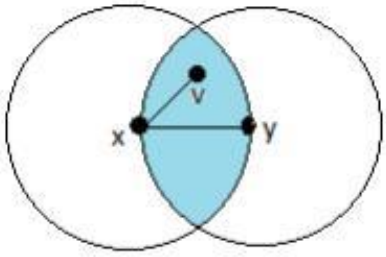


Figure 12. example of RNG

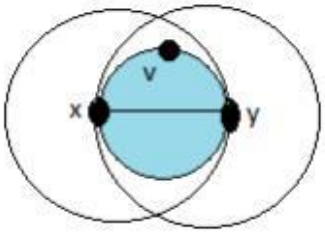


Figure 13. example of GG

E. Performance of AAA in ns2

In wireless networks comprised of numerous mobile stations, the routing problem of finding paths from a traffic source to a traffic destination through a series of intermediate forwarding nodes is particularly challenging. When nodes move, the topology of the network can change rapidly. Such networks require a responsive routing algorithm that finds valid routes quickly as the topology changes and old routes break. Yet the limited capacity of the network channel demands efficient routing algorithms and protocols, that do not drive the network into a congested state as they learn new routes. The tension between these two goals, responsiveness and bandwidth efficiency, is the essence of the mobile routing problem.

AAA, is a responsive and efficient routing protocol for mobile, wireless networks. Unlike established routing algorithms before it, which use graph-theoretic notions of shortest paths and transitive reach ability to find routes, AAA exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. AAA uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. In regions of the network where such a greedy path does not exist (i.e., the only path requires that one move temporarily farther away from the destination), AAA recovers by forwarding in circuitus mode, in which a packet traverses successively closer faces of a planar subgraph of the full radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes.

AAA will allow the building of networks that cannot scale using prior routing algorithms for wired and wireless networks. Such classes of networks include:

Rooftop networks: fixed, dense deployment of vast numbers of nodes

Ad-hoc networks: mobile, varying density, no fixed infrastructure

Sensor networks: mobile, potentially great density, vast numbers of nodes, impoverished per-node resources

Vehicular networks: mobile, non-power-constrained, widely varying density

We are Projecting AAA:

Geographic provisioning: We use geographic forwarding via a waypoint not on the path found by naive AAA to distribute load on the network. This approach is promising because on a wireless network, position and capacity are correlated; distributing load geographically leverages spatial reuse, and cuts the average load in regions where traffic is concentrated.

Obstacles: We are investigating AAA's behavior in the presence of obstacles to radio propagation, which introduce the risk that the planar subgraph used by AAA's circuitus mode may not be connected.

We are investigating both deterministic and randomized algorithms for recovering from such disconnections when they occur. We plan to build novel wireless network systems in the above categories that use AAA. More information on the systems we are building will appear on this page in the near future.

TABLE II. A ROUGH LIST OF WHAT'S AAA-SPECIFIC IN THIS NS-2 TARBALL

File(s)	Description
AAA/{AAA.cc, h}	C++ code for the AAA routing agent.
AAA/paper-cmu.tcl	TCL script for simulations used in 8-node cases
AAA/paper-cmu.pl	Perl script for iterating over several simulations, all 8-node cases from the.
tcl/mobility/AAA.tcl	TCL library code for AAA.
locdbase.{cc,h}	C++ code for the idealized (omniscient) location database.

TABLE III. A ROUGH LIST OF WHAT'S AAA-SPECIFIC IN THIS NS-2 TARBALL

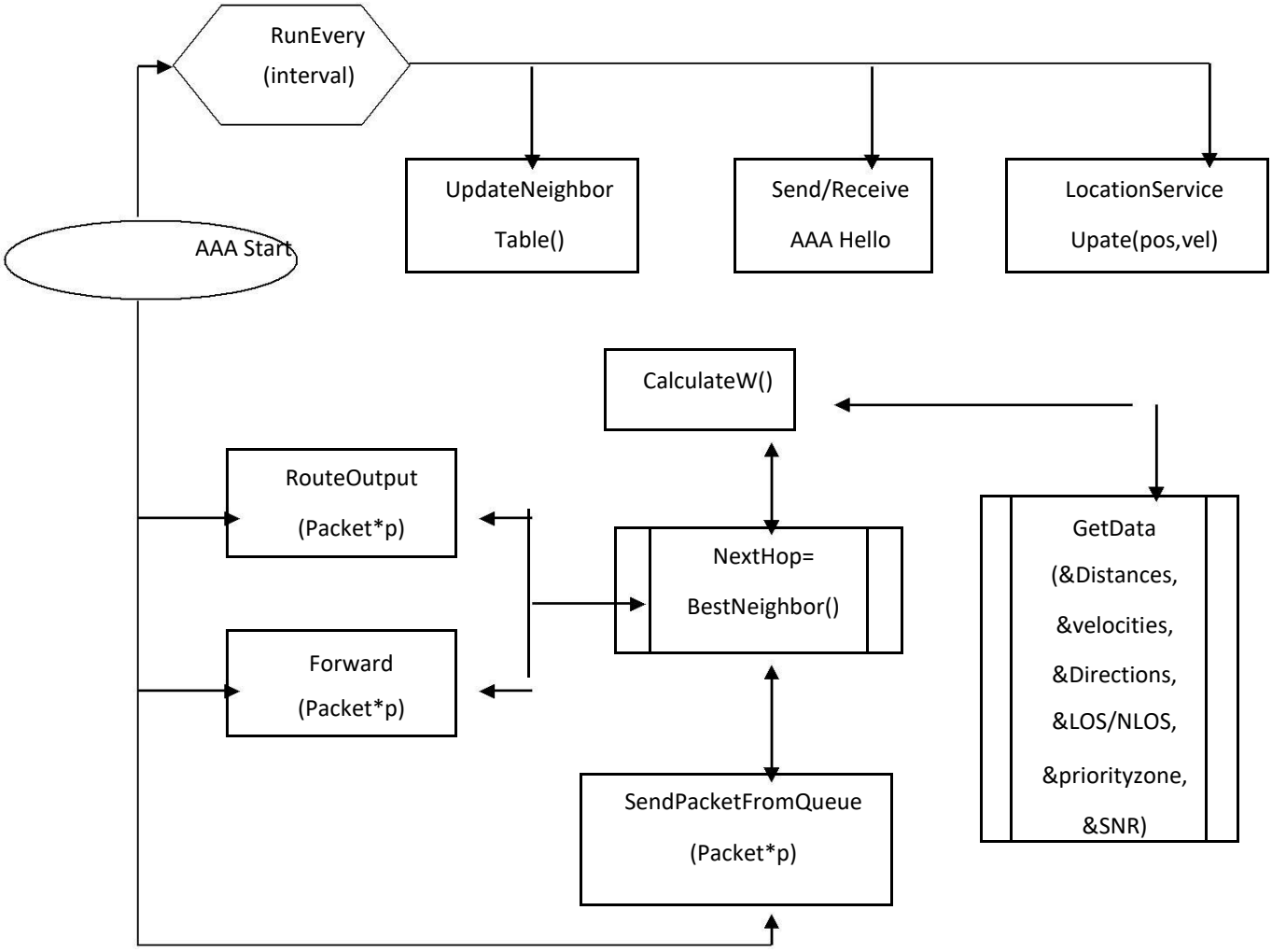
There are also minor modifications to ip.h,cmu-trace.h, and packet.h, for underlying support required by AAA.

N.B. that we should set all these parameters in our simulation script; the defaults may not be appropriate for the simulation .

TCL Configuration Variable	Value	Function
bint_	{1.0, 1.5, 3.0}	Beaconing interval (seconds)
bdesync_	0.5	Random component magnitude (percentage) in beaconing interval, to avoid synchronized beaconing by neighbors
bexp_	3 * (bint_ + bdesync_ * bint_)	Beacon expiration interval (seconds) before timing out neighbor from neighbor list
use_implicit_beacon_	1	When set to 1, treat data packets as beacons; receive promiscuously and reset neighbor expiration timer for every received unicast packet from a neighbor, and reset the beacon transmission timer whenever transmitting a unicast packet
use_mac_	1	When set to 1, use link breakage detection from failed MAC retransmit to remove neighbors from neighbor list
use_peri_	1	When set to 1, forward packets in circuitus mode when greedy forwarding impossible
use_planar_	1	When set to 1, enables planarization in circuitus mode
use_timed_plnrz_	0	When set to 1, enables periodic replanarization, on the basis of a timer

TABLE IV. A TABLE OF THE TCL VARIABLES USED TO CONFIGURE THE BEHAVIOR OF THE NS-2 AAA IMPLEMENTATION

F. Block diagram of aaa algorithm



VII. OBTAINED RESULT

Ultimately, the affiliation of circuitus and Cupidus algorithm furnishes a perfect AAA algorithm that encompasses the forwarding algorithm on the lavish network graph with circuitus forwarding only when Cupidus forwarding is absurd .

A. Sample coding

```
# seeding
ns-random $val(seed)
# create simulator instance
set ns_          [new Simulator]
set loadTrace $val(lt)
set topo  [new Topography]
$topo load_flatgrid $val(x) $val(y)
set tracefd[open $val(out) w]

#$ns_ use-newtrace

set nf [open hls.nam w];

# trace and nam file

$ns_ trace-all $tracefd

$ns_ namtrace-all-wireless $nf 2000 2000 ;# mobily topo x&y set chanl [new $val(chan)]

# Create God

set god_ [create-god $val(nn)]

# Attach Trace to God

set T [new Trace/Generic] $T attach $tracefd

$T set src_ -5 $god_ tracetarget $T
##

# Define Nodes

##

puts "Configuring Nodes ($val(nn))"

$ns_ node-config -adhocRouting $val(adhocRouting) \ -llType $val(ll) \
```

```
-macType $val(mac) \ -ifqType $val(ifq) \ -ifqLen $val(ifqlen) \ -antType $val(ant) \ -propType $val(prop) \ -phyType $val(netif) \ -channel $chanl \ -topoInstance $topo \ -wiredRouting OFF \

-mobileIP OFF \ -agentTrace $val(agttrc) \

-routerTrace $val(rtrtrc) \ -macTrace $val(mactrc) \ -movementTrace $val(movtrc)

##
Create the specified number of nodes [$val(nn)] and "attach" them

to the channel.

##

for {set i 0} {$i < $val(nn) } {incr i} { set node_($i) [$ns_ node] $node_($i) random-motion 0;

# disable random motion

# Bring Nodes to God's Attention $god_ new_node $node_($i)}

#Setup UDP connection set udp_s [new Agent/UDP] set udp_r [new Agent/Null]

$ns_ attach-agent $node_(0) $udp_s $ns_ attach-agent $node_(5) $udp_r
#Setup a MM Application

set e [new Application/Traffic/CBR] $e set packetSize_ 500

$e set rate_ 20Kb $e set random_ 1

#$e attach-agent $udp_r $e attach-agent $udp_s

$ns_ connect $udp_s $udp_r

#$ns_ at 0.0 "$e start" $ns_ at 1.0 "$e start"

$ns_ at 2.0 "$e stop "

source $val(sc)

#source $val(cp)

##

# Tell nodes when the simulation ends

##

for {set i 0} {$i < $val(nn) } {incr i} { $ns_ at $val(stop).0 "$node_($i) reset";
}
$ns_ at $val(stop).0002 "puts \"NS EXITING... $val(out)\" ; $ns_ halt"
proc stop {} {
global ns_ tracefd global ns_ nf $ns_ flush-trace close $nf
close $tracefd exit 0
}
puts "Starting Simulation..." $ns_ run
```

B. OUTPUT

While executing our code in Ubuntu software with NS2 (network simulator) platform we will grab a depreciated packet loss of (0.0008%). Our algorithm bring out over 98% of message relinquished to a node to emancipate to its destination. Furthermore our AAA algorithm is susceptive and competent routing protocol for mobile and wireless networks.

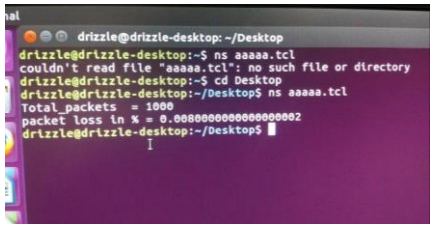


Figure 14. Output of the proposed system

The fig 14 is the screenshot of the output for the proposed system.

VIII. CONCLUSION

In our algorithm for packet forwarding a node is adopted that is absolutely one hop to the adjacent locus. In our algorithm, packet selection has been rendered dynamically which is the preeminent asset. On analogizing against distinctive routing protocols our algorithm afford great exactness towards prostate packet loss. Thus our aspiration to abate the packet loss was achieved and the packet loss seems to be 0.008% over 1000 packets .Our AAA algorithm can be administered to sensor network etc, our destined activity is to actualize our algorithm by forwarding more number of packets.

REFERENCES

[1] Deepak Bindlish, Alka Jindal, Sanjay Batish and Amardeep Singh Dept. of Comp. Science, PEC University of Technology, Chandigarh, India(2014):Analysis of Position Based Routing Protocols in VANET using NS2 Simulator.

[2] M. Raya, P. Papadimitratos, and J. Hubaux, ‘‘Securing vehicular communications,’’ IEEE Wireless Commun. Lett., vol. 13, no. 1, pp. 8–15, Oct. 2006.

[3] S. Tomar Machine Intelligence Research Labs, Gwalior 223, New Jiwaji Nagar, Gwalior 474011 India:Position Based Routing for Wireless Mobile Ad Hoc Networks Geetam.

[4] http://www.ist-drive.org http://www.webopedia.com/TERM/S/static_routing.h tml

[5] http://www.isi.edu/nsnam/ns :the official ns homepage

[6] http://www.isi.edu/nsnam/ns/ns-documentation.

[7] http://jan.netcomp.monash.edu.au/ProgrammingUnix /tcl/tcl_tut.html - Tcl tutorial

[8] http://bmrc.berkeley.edu/research/cmt/cmtdoc/otcl/ oTcl tutorial

[9] A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET byUBAIDULLAH RAJPUT, (Student Member, IEEE), FIZZA ABBAS, (Student Member, IEEE), AND HEEKUCK OH, (Member, IEEE) Department of Computer Science and Engineering, Hanyang University, South Korea.

[10] VANET connectivity analysis from Nokia Research Center, Germany.

[11] VANET, its characteristics, attacks and routing techniques: A survey , by Manjyot saini and Harjit Singh.