ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 6, June 2013

Secured Intersection based Geographical Routing Protocol for VANET

Suvya P, Prabhu C

***Abstract*—To achieve efficient routing protocol for vehicular ad hoc networks (VANETs) existing system employs intersection-based Geographical Routing Protocol (IGRP) in city environments. IGRP is based on an effective selection of road intersections through which a packet must pass to reach the gateway to the Internet. The selection is made in a way that guarantees with high probability, network connectivity among the road intersections while satisfying quality-of-service (QoS) constraints on tolerable delay, bandwidth usage and error rate. Geographical forwarding is used to transfer packets between any two intersections on the path reducing the path's sensitivity to individual node movements. To achieve QoS routing problem as a constrained optimization problem, the existing system uses genetic algorithm to solve the optimization problem. To deal with security and privacy issues in VANET the proposed scheme build a secure environment for value-added services in VANETs using An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks(ABAKA). ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead. The security of ABAKA is based on the elliptic curve discrete logarithm problem, which is an unsolved NP complete problem. To deal with the invalid request problem, which may cause the batch verification fail, a detection algorithm has been proposed.**

***Index Terms*— Message routing, Authentication, batch verification, elliptic curve cryptographic.**

I. INTRODUCTION

VEHICULAR ad hoc networks (VANETs) represent a rapidly emerging and challenging class of mobile ad hoc networks (MANETs). In such networks, each node operates not only as a host but also as a router, forwarding packets for other mobile nodes. Vehicles form a decentralized communication network by means of wireless multihop routing and forwarding protocols. Most existing research considers vehicular ad hoc networks(VANETs) as a vehicle-to-vehicle or a vehicle-to road-side-unit network architecture that can be easily deployed without relying on expensive network infrastructure. VANET-based applications can be classified into two categories:1) Applications that are delay sensitive ,e.g., downloading a multimedia application and connecting to a virtual personal network (VPN) for video or voice conferencing, and video streaming from the closest Internet gateway; and 2) Applications that are delay tolerant, e.g., sending simple text messages or an advertisement.

VANET is a special type of MANET, in which vehicles act as nodes. Unlike MANET, vehicles move on predefined roads, vehicles velocity depends on the speed signs and in addition these vehicles also have to follow traffic signs and traffic signals. There are many challenges in VANET that are needed to be solved in order to provide reliable services. Stable & reliable routing in VANET is one of the major issues. Hence more research is needed to be conducted in order to make VANET more applicable. As vehicles have dynamic behavior, high speed and mobility that make routing even more challenging.

VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment.

According to the DSRC standard, avehicle sends a safety-related message to its neighboring RSU every 100–300 ms, which means that an RSU has to verify some 600 safety-related message/s if there are roughly 180 vehicles kept within the communication range of the RSU. In other words, the security scheme for value-added applications should not pose a heavy burden on RSUs. Therefore, the burden may gather at a single authentication server, which incurs a bottleneck problem. Obviously, it is critical to develop an efficient and secure authentication scheme before value-added applications

Manuscript received June, 2013.

***Suvya P**, PG Scholar, Computer Science and Engineering, Coimbatore Institute of Engineering and Technology., . Narasipuram, Coimbatore, Tamil Nadu, ,India,08547162187*

***Prabhu c**, Asst Professor, Computer Science and Engineering, Coimbatore Institute of Engineering and Technology, Narasipuram, Coimbatore, Tamil Nadu,,India,*

can take effect.

To tackle the aforementioned problems, including security, efficiency, and scalability problems, we proposed an anonymous batch authentication and key agreement (ABAKA) scheme with intersection based geographical routing protocol to build a secure environment for value-added services in VANETs.

II. RELATED WORK

Message routing protocols are classified into two categories, i.e., topology and position based. Topology based routing protocol use links information that exists in the network to perform packet forwarding. Each node has information about the entire network topology before the node begins forwarding messages. In position-based routing protocols, messages are routed based on knowledge of the geographical location of the source, intermediate nodes, and final destination. One advantage of geographical routing protocols is that they can find a suboptimal route from source to destination without the use of routing tables; therefore, there is no need to flood the network and store routing information at each node.

Recently, several related studies have been proposed, addressing the security and privacy preservation issues for safety related applications in VANETs [1].

To deal with the scalability issues, Lin *et al.* proposed a time-efficient and secure vehicular communications (TSVC) based on TESLA to address the scalability issue. In TSVC, a vehicle first broadcasts a commitment of hash chain to its neighbors. By the use of the elements of the hash chain, the neighbors can authenticate this vehicle's following messages.Owing to the rapid verification of MAC, TSVC can greatly alleviate the message LR. However, the weakness of TSVC is not robust enough. The larger the dynamics of traffic becomes, the more Loss Ratio TSVC has [4].

Analysis of traditional routing protocols for mobile ad hoc networks (MANETs) demonstrated that their performance is poor in VANETs. The main problem with these topology based routing protocols (e.g., optimized link-state routing (OLSR) , dynamic source routing, and ad-hoc on demand distance vector routing (AODV) in VANET environments is their route instability. Indeed, the traditional node-centric view of the routes (i.e., an established route is a fixed succession of nodes between the source and destination) leads to frequent broken routes in the presence of VANETs' high mobility. Consequently, many packets are dropped, and the overhead due to route repairs or failure notifications significantly increases, leading to low delivery ratios and high transmission delays.

Despite better path stability, geographical forwarding does not perform well in a city environment. Its problem is that, many times, it cannot find a next hop (i.e., a node closer to the destination than the current node).

The recovery strategies proposed in the literature are often based on planar graph traversals, which were shown not to be as effective in VANETs due to radio obstacles and high node mobility[3].

A number of road-based routing protocols [6] [7] have been designed to address this issue. However, they fail to factor in vehicular traffic flow by using the shortest road path between source and destination.It is possible indeed that the road segments on the shortest path are empty.

III. METHODOLOGY

GENETIC ALGORITHM

As in the selection of backbone route is formulated as an optimization
problem with the objective function given as

$$\max P_c(y) \quad (1)$$

$$p_c(y)=\prod_{j=1}^{n} p_{cj}(y) \quad (2)$$

$$D(y)=\sum_{j=1}^{n} D_j(y) \le D_{th} \quad (3)$$

$$H_c(y)=\sum_{j=1}^{n} H_{cj}(y) \le H_{th} \quad (4)$$

$$BER(y)=\prod_{j=1}^{n} BER(y) \le BER_{th} \quad (5)$$

where $Pc(y)$ is the connectivity probability of route y, and Dth, Hth, and BERth are thresholds on the tolerable end-to-end delay, hop count, and BER, respectively.

Fig 1 shows the flowchart of the proposed GA, which includes the following components: solution representation, initialization, evaluation, selection, crossover, mutation, and termination.

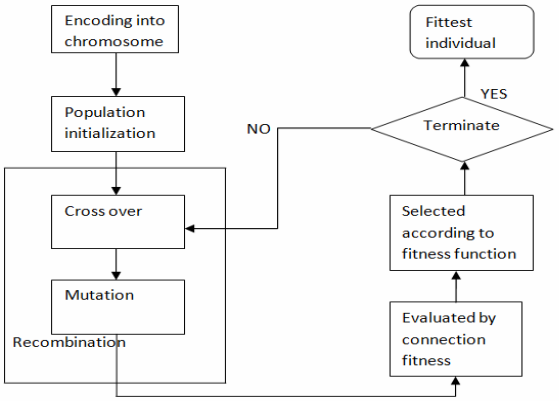

Fig 1. GA Flowchart.

Solution Representation and Initialization

In our approach, a natural encoding scheme would be to define each intersection in the backbone route as a gene. The backbone route consists of the identification number of each selected intersection. Then, the ordered intersections in one route can be represented as a chromosome. Therefore, each feasible solution y consists of one chromosome, which is denoted as $v1, v2. . . vm$. For example, routes 1-2-7-8-25, 1-28-27-26-25, and 3-6-9-8-25 in Fig 2 are chromosomes. Thus, an individual (or chromosome) is a vector containing the

ordered intersections. The initial population is generated by randomly selecting feasible solutions. Each solution or chromosome begins with the intersection adjacent to the MN. The next gene is constructed from a randomly selected intermediate intersection. Then, the process randomly chooses the next intermediate intersection in the backbone route, and the process stops when the next intersection corresponds to that adjacent to the Internet gateway. It is important to ensure that the solution is feasible, i.e., it satisfies the following two conditions: 1) Each of the two consecutive intersections in the route are connected by a backbone link. 2) The route satisfies the QoS constraints.

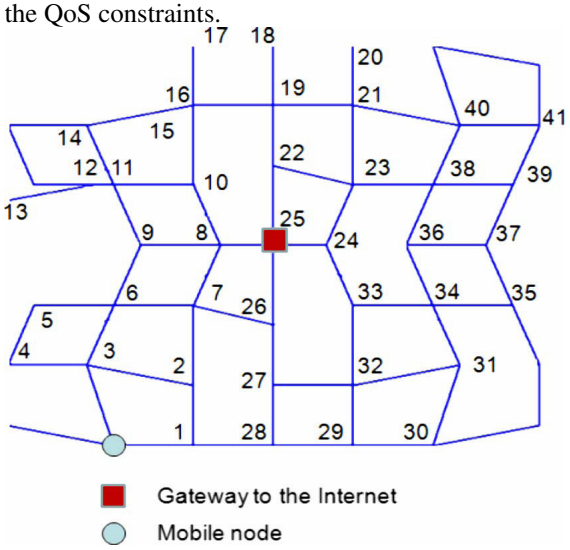

Fig 2. Road map used in the simulation.

Fitness calculation

A value for fitness function f(y) is used to select the best individuals. This is to maximize the connectivity probability which is defined as follows:

$$f(y)=Pc(y) \quad (6)$$

Selection

During the selection operation, the quality of the population is improved by giving the high-quality solutions a better chance to produce offspring's which will be part of the next generation.

$$P_{selection} = \frac{f(x)}{\sum_{y=1}^{P_z} f(y)/p_z} \quad (7)$$

Crossover

One possible crossover operator is the one point crossover where two chromosomes are selected from the current population and common intermediate gene is randomly selected. That is the one point crossover operator finds an intermediate intersection called point of crossover which is common to two selected routes as shown in Fig 3 . Then it swaps the second part of each selected route beyond the point of crossover to form two new offspring's.

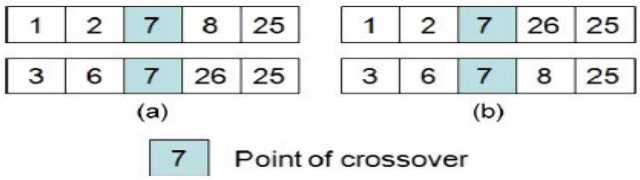

Fig 3. One point crossover operator. (a) Two chromosomes with 7 as crossover point. (b) Two new offspring's.

Mutation

Mutation is an operator that causes random changes in the genes inside one chromosome. Therefore mutation causes diversion in the genes of the current population which prevents the solution from being trapped in a local optimum. Mutation is performed on the current population with rate μ. In our implementation, we use a uniform mutation operator. Thus, after choosing any individual from the population with equal probabilities, we randomly pick an intermediate gene (intersection) and then randomly choose the adjacent intersection as in Fig 4. It is important to verify that the new individual is a feasible solution.

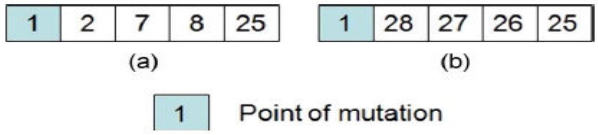

Fig 4. Uniform mutation operator. (a) Chromosome with 1 as a point of mutation. (b) New offspring

Termination

The termination criteria can be based on the total number of generations between feasible solutions in one population.

ABAKA

To deal with security and privacy issues in VANET the proposed scheme build a secure environment for value-added services in VANETs using An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks(ABAKA). ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead. The security of ABAKA is based on the elliptic curve discrete logarithm problem, which is an unsolved NP complete problem. To deal with the invalid request problem, which may cause the batch verification fail, a detection algorithm has been proposed.

IV. PROPOSED WORK

In this project we provide a secured intersected based geographical routing using An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks(ABAKA). Here each

mobile node request for the backbone route which information can be retrieved from the neighbor MN or from the Gateway as in Figure 5 Proposed work. Here the Gateway acts as a location server where it is responsible for saving current location information about all vehicles in its vicinity. This can be addressed using proposed location service management protocol called Region based Location-Service-Management Protocol (RLSMP).Each vehicle reports its location information to the gateway each time it moves one transmission range farther from its previous location. This information contains the node ID, transmission range Tr, **X** and Y coordinates of the node location, time of the last update, and the velocity and direction of the node's movement. Based on these location information, the Internet gateway constructs a set of routes between itself and the MNs. To increase their stability, IGRP builds routes based on intermediate and adjacent road intersections toward the gateway. These routes, which are called backbone routes, are represented as sequences of intersections.IGRP runs an intersection based routing protocol using GA to find the optimal route. For securing the network the system uses ABAKA scheme. With ABAKA, an SP can simultaneously authenticate multiple requests and establish different session keys with vehicles using Gateway. ABAKA considers not only scalability and security issues but privacy preservation as well. To deal with the invalid request problem, a detection algorithm has been used.

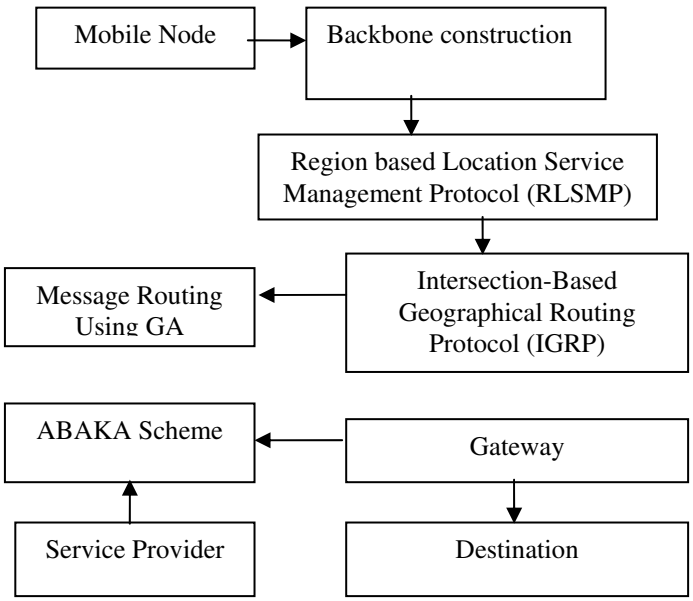

Figure 5. Proposed work

V. ALGORITHM

IGRP Algorithm

In the network
if (a gateway) then
if there is a significant change in the node density then
Recalculate the transmission range.
Recalculate the routes between the different intersections and the gateway.
Send this data to the nodes in the network;
end if
end if
if (an MN) then
if has data to transmit then
Queries its neighbors about the optimal backbone route before forwarding its messages.
if the required information is available then
A positive response will be sent back to the source node including the optimal route.
else
The query will be relayed to the local gateway using normal geographical routing.
Receive the required information from the gateway;
end if
end if
Save the updated route information;
Adjust the transmission range;
Use this route to forward the data packets to the required destination;
end if

ECDSA - Elliptic Curve Digital Signature Algorithm

Signature Generation

For signing a message m by sender A, using A's private key dA
Step 1: Calculate e = HASH (m), where HASH is a cryptographic hash function, such as
SHA-1
Step 2: Select a random integer k from [1,n − 1]
Step 3: Calculate r = x1 (mod n), where (x1, y1) = k * G. If r = 0, go to step 2
Step 4: Calculate s = k − 1(e + dAr)(mod n). If s = 0, go to step 2
Step 5: The signature is the pair (r, s)

Signature Verification

For B to authenticate A's signature, B must have A's public key QA
Step 1: Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid
Step 2: Calculate e = HASH (m), where HASH is the same function used in the signature generation
Step 3: Calculate w = s −1 (mod n)
Step 4: Calculate u1 = ew (mod n) and u2 = rw (mod n)
Step 5: Calculate (x1, y1) = u1G + u2QA
Step 6: The signature is valid if x1 = r(mod n), invalid otherwise

ECDH – Elliptic Curve Diffie Hellman

Let (dA, QA) be the private key - public key pair of A and (dB, QB) be the private key public key pair of B.
Step 1: The end A computes K = (xK, yK) = dA * QB

Step 2: The end B computes L = (xL, yL) = dB * QA
Step 3: Since dAQB = dAdBG = dBdAG = dBQA. Therefore K = L and hence xK = xL
Step 4: Hence the shared secret is xK

Detection algorithm

Step 1: DetAlg(BR):
Step 2: begin
Step 3: if BatchV erify(BR) then
Step 4: return True;
Step 5: elseifNum(BR) == 1 then
Step 6: return IDi □ BR as an invalid request;
Step 7: else
Step 8: setBRFront = {Req1,Req2, . . . , Req_n/2_};
Step 9: setBRRear = {Req_n/2_+1,Req_n/2_+2, . . . , Reqn};
Step 10: DetAlg(BRFront);
Step 11: DetAlg(BRRear);
Step 12: end if
Step 13: end

VI. IMPLEMENTATION

The proposed method implemented using ns2. The simulation results are fairly impressive.To implement SIGRP For VANETS, we implemented first the location service management protocol RLSMP [5]. In our experiments, we consider different scenarios such as Number of request vs. Rebatch Verification delay, No of compromised vehicle vs. Expected verification delay, No of request vs. Transmission overhead, Number of request vs. Verification delay.

Number of request vs. Rebatch Verification delay

In Figure 6 we verify the rebatch delay of the system between based on the number of request for intersection-based Geographical Routing Protocol (IGRP) in city environments and Elliptic curve digital signature algorithm (ECDSA).Compared to ECDSA ,proposed IGRP system have less rebatch delay verification .When the number of request is high , verification delay also high in existing system .

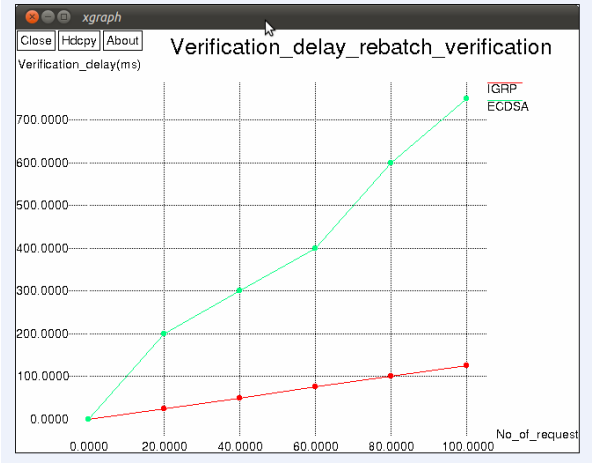

Fig 6. Number of request vs. Rebatch Verification delay

No of compromised vehicle vs. Expected verification delay

In Figure 7 we verify expected verification delay of the system between based on the number of compromised vehicle used for intersection-based Geographical Routing Protocol (IGRP) in city environments and Elliptic curve digital signature algorithm (ECDSA).Compared to ECDSA, proposed IGRP system have less expected verification delay (ms) .When the number of request is high, expected verification delay also high in existing system.

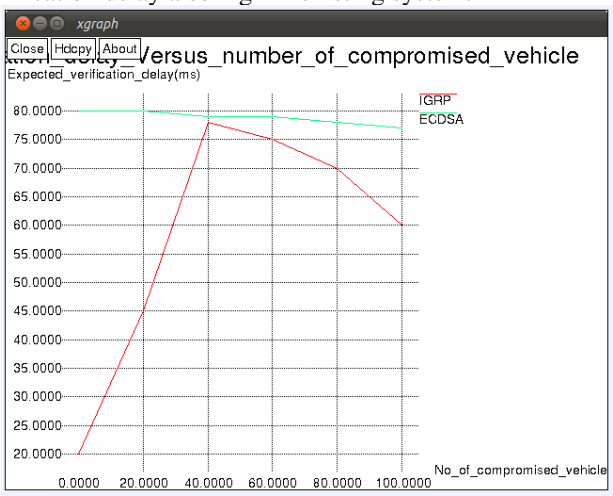

Fig 7. No of compromised vehicle vs. Expected verification delay

Number of request vs. Transmission overhead

In Figure 8 we measure the transmission overhead of the system between based on the number of request used for intersection-based Geographical Routing Protocol (IGRP) in city environments and Elliptic curve digital signature algorithm (ECDSA).Compared to ECDSA, proposed IGRP system have less transmission overhead .When the number of request is high, transmission overhead is also high in existing system.

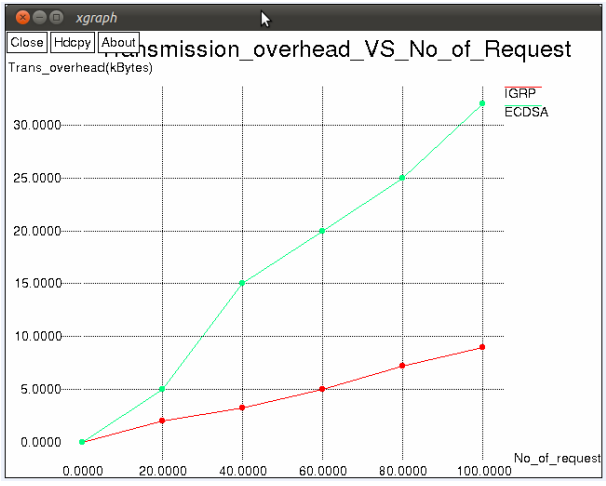

Fig 8. No of Request vs. Transmission Overhead

Number of request vs. Verification delay

In Figure 9 we verify the delay of the system between based on the number of request for intersection-based Geographical Routing Protocol (IGRP) in city environments and Elliptic curve digital signature algorithm (ECDSA).Compared to ECDSA ,proposed IGRP system have less verification delay (ms) .When the number of request is high , verification delay also high in existing system.

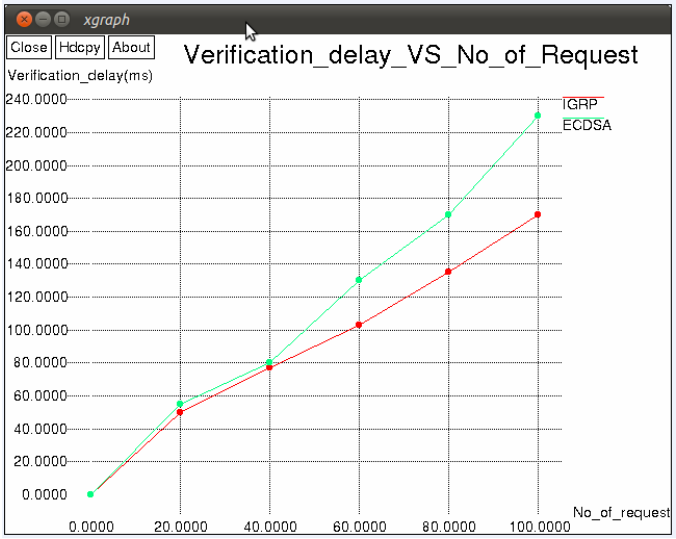

Fig 9. Number of Request vs. Verification Delay

VII. CONCLUSION

The approach for routing messages using IGRP improves the performance of routing in VANETs. It satisfies QoS constraints as a constrained optimization problem. IGRP achieves better performance in such a way it selects routes that are connected and at the same time, satisfies thresholds on the end-to-end delay, hop count and BER. The proposed trusted routing framework is developed using ABAKA scheme. With ABAKA, an SP can simultaneously authenticate multiple requests and establish different session keys with vehicles. ABAKA considers not only scalability and security issues but privacy preservation as well. To deal with the invalid request problem, a detection algorithm has been used.

REFERENCES

[1] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," RSA Crypto., vol. 5, no. 2, pp. 2–13, 2002.

[2] B. Ducourthial, Y. Khaled, and M. Shawky, "Conditional transmissions:Performance study of a new communication strategy in VANET," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3348–3357, Nov. 2007.

[3] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," IEEE Trans. Veh.Technol., vol. 58, no. 7, pp. 3609–3626, Sep. 2009.

[4] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[5] H. Saleet, O. Basir, R. Langar, and R. Boutaba, "Region-based locationservice-management protocol for VANETs," IEEE Trans. Veh. Technol.,vol. 59, no. 2, pp. 917–931, Feb. 2010.

[6] H. Su and X. Zhang, "Clustering-based multichannel MAC protocols for QoS provisioning over vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3309–3323, Nov. 2007.

[7] V. Naumov and T. Gross, "Connectivity-Aware Routing (CAR) in vehicular adhoc networks," in Proc. IEEE INFOCOM, 2007, pp. 1919–1927.

Suvya P is currently pursuing M.E Computer Science and Engineering at Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, (Anna University, Chennai). She has about 6 years experience in industry.Her research interests include wirelesss networking, Cryptography, Data Structures.

Prabhu C is currently Asst Professor in the Department of Computer Science, at Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, (Anna University, Chennai). His research interests include wired and wirelesss networking, Cryptography.