Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LOCATION VERIFICATION TECHNIQUE FOR SECURE GEOGRAPHICAL ROUTING IN VANET

[1]A.PUNITHA, [2]J. MARTIN LEO MANICKAM
[1]Research Scholar, Anna University, M.N.M Jain Engineering College
[2]Professor, St.Joseph's College of Engineering
Department of Electronics and Communication Engineering, Chennai
E-mail: [1]punitha0581@gmail.com

ABSTRACT

The geographical path routing has more benefits in Vehicular Adhoc Network (VANET). However, the lack of location verification scheme results in cruel security attacks. In this paper, location verification technique for secure geographical routing in VANET that encodes the geographical locations of nodes using geographic hashes is proposed. Data packets are transmitted securely over the communication channel through private and public keys of a node. The next hop is carefully chosen by geographic routing. This technique uses two step location verification schemes. First, when data is transmitted from the source to its next hop, the packet is verified through reliability checks. Then, validation of its location is done by distance bounding scheme.The proposed solution effectively secures the geographical routing with valuable location verification schemes. By simulation, we show that the proposed technique defends various attacks by reducing the packet drop and increasing the packet delivery ratio.

Keywords: *Location Verification, Geographical Routing, VANET, Security*

1. INTRODUCTION

A network that offers communication among the vehicle and roadside units is defined as a "Vehicular Adhoc Network" (VANET). It is a promising new-fangled technology that provides vehicle-to-vehicle (v2v) communication and Inter-vehicle communication (IVC). This network enhances safe driving and traffic condition by contributing distributed ad hoc approach. In real time VANET has more benefits such as sending out warning messages of oncoming accidents and warning possible traffic congestion on a preferred path through traffic update messages.

Intelligent Transportation System (ITS) is a developed intelligent technique to enhance the performance of the transportation system. VANET is rooted by ITS. It facilitates vehicles to keenly communicate with other vehicles in the network and thereby it identifies circumstances such as accidents and traffic jams. VANET safeguards the vehicles by taking any desired action or by sending warning messages to the driver during critical situations.

High dynamics and mobility, frequently changing network topology, constrained temporal and functional network redundancy and frequent fragmentation are the characteristics of VANET [1][2][3][4].

In Adhoc network, routing is accomplished by multihop forwarding. To transmit data from the source to the destination, this approach uses intermediate nodes as forwarding nodes [3]. Be deficient in pre-existing routing and security infrastructure is a substantial dispute to provide security in Adhoc routing. Nodes of VANET are required to construct the routing infrastructure without necessitating global knowledge. Since, the node lacks secure node identification; it adds much complexity during the process of secure routing. Spoofed, altered or replayed routing information, selective forwarding, sinkhole attacks, wormhole attacks and acknowledgement spoofing are the different types of attacks in VANET [3] [5] [6].

Owing to lack of infrastructure, highly dynamic network topology, large number of network entities and directness of wireless medium complicates making available secure and reliable routing in VANET. Defying mischievous activities of attacker and security attacks are the key design goals of security architecture in VANET [7].

The identified objectives of security requirement in VANET are as follows: Message Authentication and integrity, Message Non-Repudiation, Entity

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Authentication, Access Control, Message Confidentiality, Accountability and Privacy protection.

Dynamic Trust-Token (DTT), trusted routing framework, geographical secure path routing protocol (GSPR), Detecting and Correcting Malicious Data (DCMD) protocol and so on are some of the examples for secure routing mechanisms in VANET [2][3][5][6][9].

The geographical secure path routing protocol (GSPR) is proposed in [5]. They have introduced authentication scheme for data transmission. However, they have not addressed any location verification scheme. In [11], the authors have put forwarded a Secure Location Verification (SLV) that exploits distance bounding, plausibility checks, and ellipse based location estimation to validate the claimed location of a vehicle. On the other hand, message security is not been provided for the replay attacks at the destination node. Further, their scheme cannot verify the location of a vehicle globally for larger area.

In order to alleviate the problems described above, in this paper, we propose to develop location verification for secure geographical routing in VANET. The paper is organized as follows. Section 2 contains literature review, section-3 includes proposed solution, section-4 describes simulation results and section-5 ends up the paper with conclusion.

2. LITERATURE REVIEW

Dynamic Trust-Token (DTT) based cooperation enhancement mechanism is put forwarded by Zhou Wang et al. in [2]. To safeguard packet integrity, their DTT has used both symmetric and asymmetric cryptography mechanisms. In order to verify correctness of packet, DTT has produced Trust Token based on instant performance through Neighborhood Watchdog. Reputation value of each node is obtained depending on runtime performance and therefore it does not require any additional information. Their technique has accomplished the secure network at the cost of high packet drop.

Vivek Pathak et al. [5] have proposed a geographical secure path routing protocol (GSPR) to secure location aware services over vehicular ad-hoc networks (VANET). Their GSPR is an infrastructure less geographic routing protocol, which is resilient to disruptions caused by malicious or faulty nodes. In their technique, geographic locations are authenticated to offer location authentication and location privacy at hand. Besides, their protocol authenticates the routing paths used by individual messages.

Papadimitratos et al. [6] have developed security architecture for vehicular communication (VC) systems. Initially, they have analyzed various threats, adversarial models, and security and privacy requirements according to the VC context. In regard with their analysis, they have introduced a set of mechanisms, to control identity and credential management, and to secure communication while enhancing privacy. The drawback of the proposed architecture is that on changing the pseudonyms for privacy reasons leads to increased instability in node's neighbor tables which in turn results in transmission faults to the next hop.

Charles Harsch et al. [8] have proposed a scheme that secures geographic position based routing (PBR) in VANETs. They have proposed their security scheme considering emerging Car2Car Communication Consortium (C2C-CC). They have incorporated security mechanisms to save from harm the position based routing functionality and services to achieve network robustness. Their defense mechanisms depend on cryptographic primitives and plausibility checks to alleviate inclusion of false position. However, their security scheme is limited to specific attacks like false injection attacks.

Terence Chen et al in paper [9] have introduced a trusted routing framework. Their trust establishment framework contains three modules namely digital signatures, node-to-node authentication module and cumulative Routability verification module. Their approach averts false link availability indication and some of routing protocol specific misbehaviors. Their framework has provided message authentication, node-to-node trust and rout ability verification, with limited requirement from online assistance of Certificate Authorities (CA). The drawback of this paper is that the proposed scheme cannot reduce the overhead and computation time to combine a number of neighbor signatures or batch signatures for faster verification.

A secure and application-oriented network design framework for VANET is proposed in [10]. They have taken into account security requirements of the communications and the requirements of potential VANET applications and services. Their technique encompasses of two components namely an application-aware control framework and a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

unified routing scheme. Further, they have analyzed some important technologies of VANET, which could improve the performance of the network.

Joo-Han Song et al. [11] have proposed the Secure Location Verification (SLV) scheme. Their scheme has the potential of recognizing position spoofing attacks. Their SLV is a cooperative infrastructure-less scheme. At first, a Radio-Frequency (RF) based scheme is used to put-off malicious vehicles from modifying measured distance between two nodes. The claimed location is verified through a series of plausibility checks. The plausibility check is achieved considering received location, speed, and direction information as key metrics. Finally, the position of claimant is controlled by the ellipse with foci at both verifier and cooperative neighbor vehicle. Though this cooperative scheme has more advantages, it incurs high delay.

3. LOCATION VERIFICATION TECHNIQUE FOR SECURE GEOGRAPHICAL ROUTING

3.1 Overview

In this paper, a Location Verification technique for Secure Geographical Routing in VANET is proposed. The technique periodically broadcasts a node's location to its neighboring nodes through beacon messages. The geographical locations of nodes are encoded using geographic hashes. Data packets are transmitted securely over the communication channel through private and public keys of a node. The next hop is carefully chosen by geographic routing. The proposed technique uses two step location verification schemes. Initially when data is transmitted from the source to its next hop, the packet is verified through reliability checks. Finally, its location is validated by distance bounding scheme. Reliability check is performed considering timestamp, appropriate transmission range and velocity as three key metrics. A packet can be forwarded to its next hop, only when it successfully completes all reliability checks. Otherwise, the corresponding packet is discarded.

3.2 Reliability Checking

When a forwarding node receives a data packet from its previous hop, immediately it performs the reliability check. Time stamp of a packet, transmission range and velocity of a node are taken as inputs to reliability checks. The forwarded packet can be transmitted to the next hop node only upon the successful verification of all reliability checks. Otherwise, the forwarded packet is simply discarded.

In this technique, reliability check consists of three phases. Here, the number of phases is determined based on number of inputs we have considered. As soon as the packet is received by an intermediate node, a series of checks are performed. Initially, the intermediate node verifies the data packet using source public key.

Phase-1

First, the timestamp of data packet is checked to ensure that the packet is not stale nor it does not tell untruths in the future. Successful verification of this check guarantees that the invader cannot modify the position of destination node.

Phase-2

Second, appropriate transmission range is verified. Assume $max\,\Re$ as the maximum acceptable transmission range of a node. Data transmissions from nodes that have higher transmission range than $max\,\Re$ are discarded.

Phase-3

Third, taking into account of physical laws of a vehicle, maximum velocity of a node is defined as *Vmax.* Thus, the obtained position of a node should exist inside a predicted space window. The value of space window is computed considering node's previous position and a radius of time between two successive position updates and *Vmax*.

Algorithm for determining reliability Checks

Assume $max\,\Re$ *as the maximum acceptable transmission range of a node*
Presume the maximum velocity of a node as Vmax
Let vn_i *be the VANET node and* d_{vni} *be the data packet forwarded by node* vn_i, *where* $i = 1,2 \ldots n$
Assume S and D denote source and destination nodes respectively
vn_i *transmits* d_{vni} *to* vn_{i+1} *towards D*
When vn_{i+1} *receives* d_{vni}, *it enters into phase-1*
If (Timestamp $(d_{vni}) \leq$ *existing time window) then*
If (Transmission range $(d_{vni}) \leq max\,\Re$ *) then*
If (Velocity $(d_{vni}) \leq$ *Vmax) then*
The packet is digitally signed by node vn_{i+1}
The packet is forwarded to next hop selected by geographic routing
Positive Reply is transmitted back to the forwarded node
Else
The Packet is discarded
Negati ve reply is transmitted back to the forwarded node
End if
Else
The Packet is discarded

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Negative reply is transmitted back to the forwarded node
End if
Else
The Packet is discarded
Negative reply is transmitted back to the forwarded node
End if

3.3 Secure Geographical Routing

3.3.1 Network Model

Consider a set of nodes {VN are distributed in VANET. The geographic location of each node vn_i (i = 1, 2…, n∈ {*VN*}) is represented by the integer coordinates (G_x, G_y). Here, G denotes the geographical location of a node. This integer coordinate is measured by means of scaling the geographic location with the global scaling factor.

We assume that nodes produce their individual public-private key pairs using RSA algorithm. Every node (vn_i) encompasses a pair of public puK_i and private keys prK_i to secretly transmitting a message M. The message M is encrypted and decrypted using puK_i and prK_i respectively. The messages are digitally signed with private key prK_i.

In geographic routing, we assume every node is aware of its geographic location. This information is periodically known to its one-hop neighbors through beacons. When the message is routed in the network, its target location is included in it.

When the message is transmitted between two nodes, their geographical positions are encoded using geographic hashes. A set of integer tokens are maintained by every node, termed as geographic hashes. Each token relates a secret of a geographical location. This secret is disclosed to nodes within a transmission range of the particular location. Nodes other than neighbors cannot obtain secret about geographic location. This criterion can be authenticated remotely by reason of one-wayness property.

Using modular arithmetic, the geographic hashes are constructed. Assume P denotes a large prime number and *b* symbolizes a generating number. Thus, the modular arithmetic is expressed as,

$$f(y) \equiv b^y \bmod P \quad (1)$$

Here mod P maps $Z_P^* = \{1,..., P-1\}$ be close to itself. Every integer $x \in Z_P^*$ represents a one-way function as,

$$H(y) \equiv \left(b^x\right)^y \bmod P \quad (2)$$

At regular intervals, node vn_i broadcasts a large prime P, b, $\vartheta_{vn_i}, \lambda_{vn_i}, \delta_{vn_i} \in Z_P^*$ and time interval T_{vn_i}. In this context, time interval (T_{vn_i}) is included to represent the expiry time for a specific geographic hash version.

At first, the geographic hash of node vn_i is set to $\left(R_{vn_i}, R_{vn_i}\right)$. R_{vni} represents a random nonce chosen by vn_i. The sequential hash versions of node vn_i is as follows,

$$R_{vn_i}[i+1]\, b^{\delta vni} \bmod P = R_{vn_i}[i] \quad (3)$$

The neighbor node of vn_i, say vn_{i+1} calculates the geographic hash of vn_i at vn_{i+1} as follows

$$H_G(vn_i, vn_{i+1}) = \left(R_{vn_i} b^{\ vn_i \Delta y} \bmod P, R_{vn_i} b^{\lambda vn_i \Delta x} \bmod P\right) \quad (4)$$

Here, Δy and Δx denote the discrepancy between the integer coordinates of geographic locations vn_i and vn_{i+1}. The validity of geographic hash of node vn_{i+1} runs out after the time interval Δ_{vn_i}.

In this technique, the nodes get aware of their neighboring nodes' locations through periodic beacon messages. In general, a beacon message includes node ID and its location. In this paper, we enhance the conventional beacon message format.

Beacon message in our technique takes in public key of a node, random nonce generated by that node, geographic hashes of neighboring nodes along with node ID and location. The format of a beacon message is given in table-1.

Table-1: Format of Beacon Message

Node ID	Location	geographic hashes of neighboring nodes	Public Key	Random Nonce

Every node periodically broadcasts beacon messages, so that, it's neighboring nodes are informed about location, public key and geometric hashes. The beacon message is digitally signed with the private key of the node. While receiving beacon messages, every neighboring node keeps them in their memory to accomplish geographic routing.

Consider the illustration given in figure-1, in that node vn_1 broadcasts the beacon message to all its one-hop neighbors namely vn_2, vn_3, vn_4, vn_5, vn_6, vn_7, vn_8, vn_9 and vn_{10}.

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

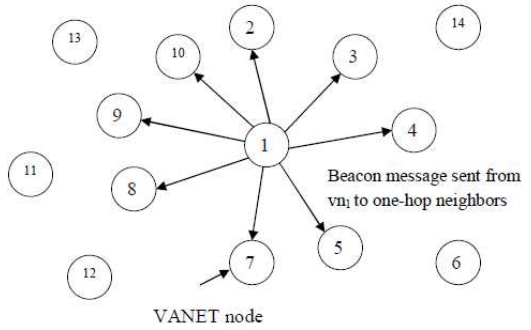

Figure. 1: A Node Broadcast Beacon Messages

Broadcasting of periodic beacon messages is helpful for authenticating routing process and also we can straightforwardly find out the false location attacks. Consider $\Re$ as the maximum one-hop radius. Each node keeps track of geographic hashes of nodes that are positioned within the two times of $\Re$. When the geographic hashes are shared among neighboring nodes, we can become aware of malicious routing behavior further than one-hop neighbors.

3.3.2 Routing Procedure

Our secure geographical routing technique uses two step *request-reply* messaging model. While transmitting control and data packets, the next hop is selected by the geographic routing protocol. When the message M is transmitted between two nodes, say vn_i and vn_{i+1}, it is encrypted by public key (puK_i) of vn_i and decrypted using its private key. The protocol messages are digitally signed with private key of the sender. Data transmission between source and destination nodes is secured through two step location verification schemes. Initially when data is transmitted from the source to its next hop, the packet is verified through reliability checks and its location is validated by distance bounding scheme as discussed in the section-3.5.

Every intermediate node (forwarding node) checks digital signatures to discover mischievous behavior of nodes. Data forwarding phase of geographic routing forwards data packet to the next node and then forwards back a reply message to the source. The reply message includes geographic hash of the next hop. The local reply message helps the source to select an alternate path in case of attack, since, geographic hashes are unforgeable. By receiving the reverse replies, the source authenticates the public key of the destination node.

Assume S and D as source and destination nodes respectively. Let R_S be the random nonce generated by the source and consider vn_i, vn_{i+1}, $vn_{i+2...}$ vn_{i+n} as a set of forwarding or intermediate nodes between source and destination. Let that L_{vni} denotes the location list of node vn_i.

The process of transmitting data between the source and destination is as follows,

(i) The source constructs the data packet by including destination ID (D), location list (L_S), random nonce generated by S and the message. The entire data packet is encrypted using public key Kpu_s of source. Finally, the message is digitally signed with private key Kpr_s of source.

$$S \xrightarrow{DataPacket} vn_i \quad \text{Data packet: } \left(\left\{D, R_S, L_S, Message\right\}_{puK_S}\right)_{prK_S} \quad (5)$$

(ii) When the data packet is received by an intermediate node, it performs reliability checks, which is explained in section-3.4

On successful completion of reliability checks, the message is forwarded to another next hop (vn_{i+1}) determined by geographical routing and a positive reply is transmitted back to the previous hop. On the other hand, upon the failure of reliability checks, the data packet is simply discarded and a failure message is forwarded back to the source.

If (Reliability checks are successful) then

$$vn_i \xrightarrow{DataPacket} vn_{i+1} \quad \text{Data packet: } \left(\left\{D, R_S, L_{vni-1} + location(vn_i), Message\right\}_{puK_S}\right)_{prK_{vni}} \quad (6)$$

$$vn_{i-1} \xleftarrow{PositiveREPLY} vn_i \quad (7)$$

Positive Reply:

$$\left(\begin{Bmatrix} R_S, prK_{vni}(R_S), \\ \langle puK_{vni+1}, P_{vni+1}, Location(P_{vni+1}), H_G(P_{vni+1}, P)\rangle \end{Bmatrix}\right)_{prK_{vni}} \quad (8)$$

Else
Negative reply is transmitted to the previous node
End if

(iii) Finally, the data packet reaches the destination node. On receiving the data, node D verifies the integrity of message by checking digital signatures. Then, it forwards a recursive reply towards the source (S).

$$vn_{k-1} \xleftarrow{\text{Re}\,cursiveREPLY} D \quad \text{Recursive Reply: } \left(\left\{L_D, R_S, neighborID, positionInformation\right\}\right)_{prK_D} \quad (9)$$

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Here, the location information is authenticated through the authenticated distance bounding technique given in section (3.5) [11].

(iv) As soon as receiving recursive reply message, the source (S) authenticates public keys by the side of routing path. This is accomplished by verifying the obtained key value in the recursive reply message as,

$$R_S = puK_{vn_i} \circ puK_{vn_{i+1}} \circ \cdots \circ puK_D \quad (10)$$

The strategy of reliability checks and the authenticated distance bounding scheme is described in section (3.4) and (3.5) respectively.

3.4 Distance Bounding Scheme to Authenticate Locations

In our proposed solution, the location information is authenticated through the authenticated distance bounding technique given in [11]. Consider vn_i and vn_{i+1} as two intermediate nodes (forwarding nodes). Assume D (vn_i, vn_{i+1}) symbolizes the distance between vn_i and vn_{i+1}. We assume nodes share a secret key (K_S) before data transmissions through Diffie-Hellman key exchange protocol.

The distance bounding scheme is utilized to bound the minimum distance between two nodes. When this technique is used between two nodes say, vn_i and vn_{i+1}, the node vn_{i+1} being at a distance D (vn_i, vn_{i+1}) from vn_i, it cannot pretend as it is at a distance D (vn_i, $vn_{i+1}^{'}$) < D (vn_i, vn_{i+1}).

To make clear distance bounding scheme, let us describe vn_i as forwarder node and vn_{i+1} as receiver node. At first, the forwarder generates a random nonce (R_F). It then transmits a *query* message to the receiver. The query message is a Message Authentication Code (MAC) of R_F generated by forwarder by means of K_S. While receiving query, the receiver constructs a *response* message, which comprises current location of node, velocity and direction. The content in *response* message is concatenated with R_F. It creates MAC for the response message and then forwards back to the forwarder. By receiving *response* message, the forwarder verifies the authenticity of the message and checks whether R_F and MAC are same. If so, it uses the elapsed time to validate the correctness of location information of receiver.

Merits of Proposed System

- A secure architecture which provide security against position based attack and replay attack.
- Efficient utilization of network resources and maintains the integrity of messages.
- Increase in packet delivery ratio in case of any black hole attacker.

4. SIMULATION RESULTS

The proposed Location Verification Technique for Secure Geographical Routing (LVTSGR) is simulated using NS2 [12]. In this simulation, the channel capacity of mobile hosts is set to the value of 2 Mbps.

In the simulation, the number of nodes is 72. The mobile nodes move in a 2500 meter x 700 meter region for 20 seconds simulation time. In our simulation, the data transmission rate is 250kb.

The simulation topology is summarized as below,

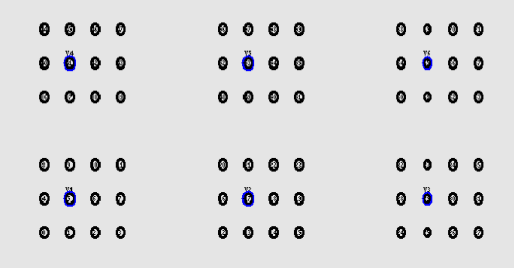

Figure 2: Simulation Topology

The simulation settings and parameters are summarized in table 2.

Table 2 Simulation Parameters

No. of Nodes	72
Area	2500 X 700
MAC	802.11
Simulation Time	20 sec
Traffic Source	CBR
Rate	250kb
Packet Size	512 bytes
Antenna Type	Omni Antenna
Number of Attackers	6
Speed	5,10,15,20 and 25m/s

4.2 Performance Parameters

We compare LVTSGR with the GSPR [5] technique. We evaluate performance of mainly according to the following parameters.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Throughput: It is the number of packets received by the receiver.

The simulation results are presented in the next section.

4.3 Simulation Results

A. Based on Attackers

The attackers are varied from 1 to 6 keeping the mobile speed as 5m/s.

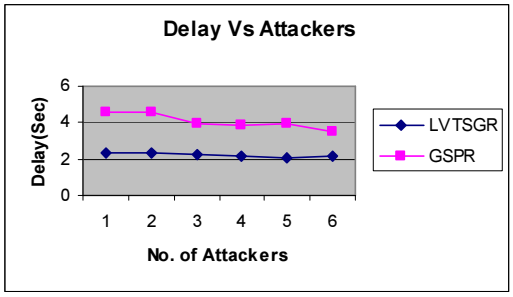

Figure 3: Delay Vs Attackers

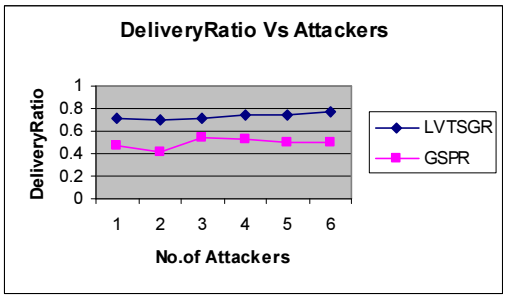

Figure 4: Delivery Ratio Vs Attackers

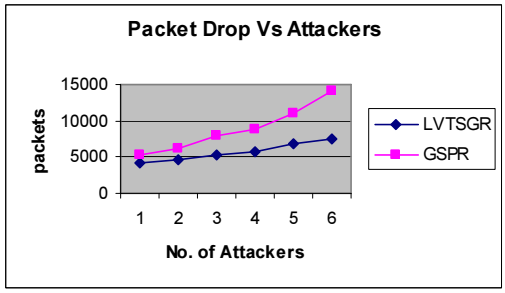

Figure 5: Packet Drop Vs Attackers

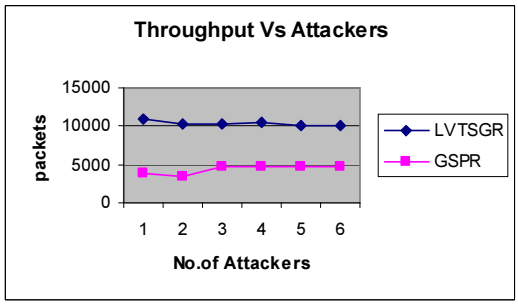

Figure 6: Throughput Vs Attackers

Since LVTSGR uses both location verification techniques as well as secure geographic routing, it eliminates more attacks involving false injection, false position advertisement, packet alteration and dropping thus decreasing the packet drop and increasing the throughput, packet delivery ratio. Also since the optimum routing is selected by avoiding the false routes, the route discovery delay is minimized.

From figures 3 to 6 we can see that the performance of LVTSGR outperforms GSPR in terms of delay, delivery ratio, packet drop and throughput by 45%, 33%, 32% and 57% respectively.

B. Based on Speed

The mobile speed is varied as 5,10,15,20 and 25m/s keeping the number of attackers as 2.

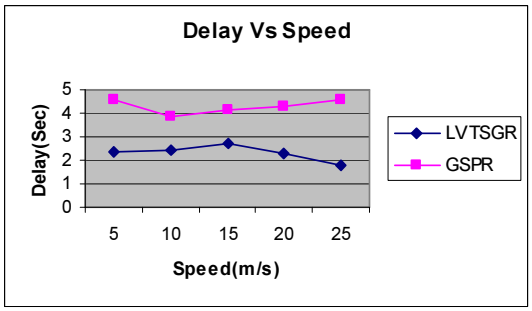

Figure 7: Delay Vs Speed

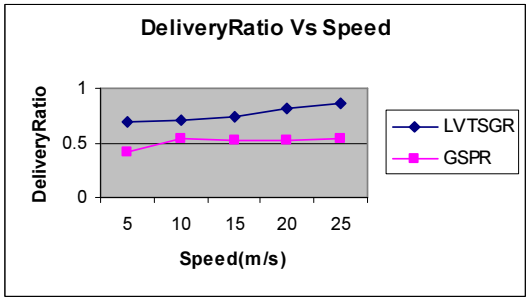

Figure 8: Delivery Ratio Vs Speed

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

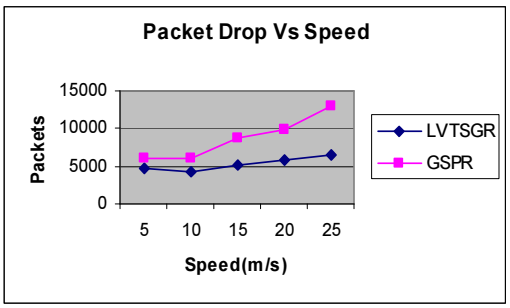

Figure 9: Packet Drop Vs Speed

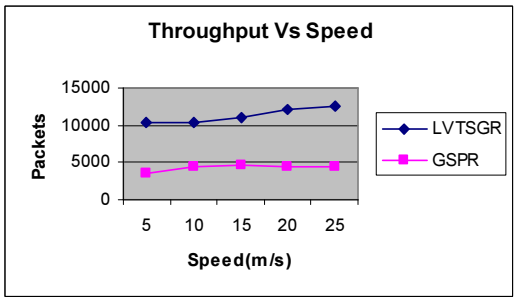

Figure 10: Throughput Vs Speed

Since LVTSGR uses both location verification techniques as well as secure geographic routing, it eliminates more attacks involving false injection, false position advertisement, packet alteration and dropping thus decreasing the packet drop and increasing the throughput, packet delivery ratio. Also since the optimum routing is selected by avoiding the false routes, the route discovery delay is minimized.

From figures 7 to 10 we can see that the performance of LVTSGR outperforms GSPR in terms of delay, delivery ratio, packet drop and throughput by 46%, 34%, 36% and 62% respectively.

5. CONCLUSION

In this paper, location verification technique for secure geographical routing in VANET is proposed. In this technique, the geographical locations of nodes are encoded using geographic hashes. Data packets are transmitted securely over the communication channel through private and public keys of a node. The next hop is carefully chosen by geographic routing. The proposed technique uses two step location verification schemes. Initially when data is transmitted from the source to its next hop, the packet is verified through reliability checks. Finally, its location is validated by distance bounding scheme. Reliability check is performed considering timestamp, appropriate transmission range and velocity as three key metrics. The proposed technique is validated by simulation results. It shows the proposed solution effectively secures the geographical routing with valuable location verification schemes. But the limitations of this technique are it does not provide confidentiality and integrity for the routing packets. Hence future work aims to select legitimate nodes for routing and provide confidentiality and integrity for routing packets.

REFERENCES

[1] Dok, Hang, et al. "Privacy Issues of Vehicular Ad-Hoc Networks" *International Journal of Future Generation Communication and Networking* 3.1 (2010)

[2] Wang, Zhou, and Chunxiao Chigan. "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs" *Communications, ICC'07 IEEE International Conference on IEEE*, 2007

[3] Fonseca, Emanuel, and Andreas Festag. "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS." *NEC network laboratories* 28 (2006): 1-28.

[4] Choudhary, Gyanesh Kumar. "Providing VANET Security through Position Verification" *Master's Project Final Report* (2007).

[5] Pathak, Vivek, Danfeng Yao, and Liviu Iftode. "Securing location aware services over VANET using geographical secure path routing" Vehicular Electronics and Safety, *ICVES 2008 IEEE International Conference on IEEE*, 2008

[6] Papadimitratos, Panagiotis, et al. "Secure vehicular communication systems: design and architecture." *Communications Magazine*, IEEE 46.11 (2008): 100-109.

[7] Lin, Xiaodong, et al. "Security in vehicular ad hoc networks." *Communications Magazine*, IEEE 46.4 (2008): 88-95.

[8] Harsch, Charles, Andreas Festag, and Panos Papadimitratos. "Secure position-based routing for VANETs." *Vehicular Technology Conference*, VTC-2007 Fall. 2007 IEEE 66th IEEE, 2007

[9] Chen, Terence, Olivier Mehani, and Roksana Boreli. "Trusted routing for VANET" *Intelligent Transport Systems Telecommunications,(ITST),* 2009 9th International Conference on. IEEE 2009

[10] Qian, Yi, and Nader Moayeri. "Design of secure and application-oriented VANETs."

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Vehicular Technology Conference, VTC Spring IEEE 2008

[11] Song, Joo-Han, Vincent WS Wong, and Victor CM Leung. "Secure location verification for vehicular ad-hoc networks." *Global Telecommunications Conference, IEEE GLOBECOM* 2008.

[12] Network Simulator: http:///www.isi.edu/nsnam/ns