USING HYBRID ROUTING PROTOCOL FOR IMPROVING PRIVACY IN VANETS' ROUTING: IMPROVING PRIVACY FOR CRITICAL VEHICLES

[1]HAMED SAYYADI, [2]ALI SHARIFARA

[1] Dep. of Computer Systems and Communications Faculty of Computer Science and Information System
University Technology Malaysia (UTM).81310 Skudai Johor, Malaysia.
[2] Department of Computer Graphics and Multimedia Faculty of Computer Science and Information System
University Technology Malaysia (UTM).81310 Skudai Johor, Malaysia.
Email: [1] hamed.sayyadi@gmail.com , [2] a.sharifara@gmail.com

ABSTRACT

Nowadays, one of the most interesting areas in Ad Hoc networks is VANET. Although, security in VANETs' routing increased a lot during these years, it is not happened for privacy. Usually, improving privacy in routing protocols is in conflict with security. In this research, we improve the privacy compliant secure routing in VANETs by using hybrid protocol called as PIDP.

Keywords: VANET, Security, Routing, Privacy

1. INTRODUCTION

Vehicular Ad hoc Network, VANET, is a form of Mobile Ad hoc Network, MANET, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment. Usually, privacy is not important in VANET routing, but sometimes we need it like when we talk about military or Law-Enforcement.

As mentioned above, military and law-enforcement are compelling examples of settings where privacy, in addition to security, is very important. Zooming in on the military example, one can imagine a battlefield MANET composed of different types of nodes, e.g., infantry soldiers, vehicles, aircrafts as well as other types of personnel and equipment. If the adversary can track nodes' movements, it can easily deduce node types. For example, one that moves 50 miles within 10 minutes is most likely, an aircraft. Also, one moving only 5 miles within the same interval is probably a vehicle. Another example in the same setting is an adversary aiming to track specific nodes. If the adversary knows that a certain node corresponds to a commander, it could wait until this node moves within reach of sniper fire, with obvious consequences.

When we talk about routing in VANET, we have to kinds of routing protocols: Position-Based or Geography-Based and Identity-Based. Identity-Based methods are for sending data to an individual node. And Geography methods are for sending data to group of nodes. Each one has its own advantages and disadvantages. ID based protocols could cover the security but they cannot have privacy alone. And position based protocols improved privacy by hiding the exact location of nodes but they cannot hide it completely.

This research has three contributions: first of all, we discuss about VANET routing protocols and introduce AODV and PRISM. After that, we argue why each one of these routing protocols cannot cover privacy alone. Finally, we suggest a hybrid routing protocol to approach a complete privacy during VANETs routing.

2. POSITION-IDENTITY-BASED ROUTING PROTOCOL (PIDP)

This project proposes a Position-Identity-Based routing protocol and considers the using position and identity together is the best way to improve privacy compliant secure routing in VANETs. PIDP is the first routing protocol which using both position and identity to route between two nodes in VANETs. PIDP uses a series of unreal identities beside the position of nodes to improve privacy.

There are a lot of prior protocols which using the identity or position separately. The major problem with them is that they cannot provide secure routing beside privacy or vice versa. Identity-based protocols can provide a secure routing by sending messages in peer to peer and also by using cipher algorithms; but, there is no more privacy for identity of nodes and also position. Although, position-based protocols such as PRISM could improve privacy, there is no way to hide the position of nodes when the connection takes a long time or when the nodes do not move.

Position-based routing is used for initial routing messages in PIDP. PIDP uses three initial messages to make a route, exchange unreal identities, and design the route table. Other connections are based on these unreal identities to hide the source and destination nodes from intermediate and also adversary nodes.

PIDP uses route request, the route reply from the destination, and route reply from source messages by the position of the source and destination to make a route. After that, PIDP sends other messages, data and acknowledgement messages, by using unreal identities; it is based on identity routing.

3. PACKETS

PIDP is designed by five different types of packets: RREQ, RREP, RREP2, DATA, and ACK-REP. RREQ is a request message which the source sends it by position of the destination node to find a route and make a connection with the destination node. Route reply message will send by destination node as RREP. When a route RREP received by source node, it will send a source route reply as RREP2 to inform the destination node about its unreal identities. Now, the route and unreal identities are ready for sending data messages. For each data message, there is an ACK-REP to inform the source or destination for receiving of data parts.

A. RREQ

The route request message contains five parts. The first part is message type. The message type part is similar in all messages. Each kind of messages has its own number to determine the message. Message type takes one byte of each message.

The second part is destination area as called DST-AREA. DST-AREA is an 8 bytes part of the route request message which contains the position of the destination node. It could help the nodes to find the destination node at first. Also, there are 8 bytes as a source area which calls SRC-AREA. SRC-AREA is the source node position to inform the destination node about the sender.

There are 128 bytes public key which sends to destination node for encrypting unreal identities of the destination node. This key is temporary and will not use after reply message. Final part of route request message is time stamp. Time stamp takes 4 bytes of the route request message to decrease the traffic and prevent from infinity in routing.
Following table shows the details of RREQ message:

Table 1: Rreq Message

MESSAGE TYPE	RREQ	1 BYTE
1	DST-AREA	8 BYTES
2	SRC-AREA	8 BYTES
3	PUBLIC KEY TMP	128 BYTES
4	TIME STAMP	4 BYTES

B. RREP

Table 2: Rrep Message

MESSAGE TYPE	RREP	1 BYTE
1	SRC-AREA	8 BYTES
2	DST-AREA	8 BYTES
3	SESSION KEY ENCRYPTED BY PUBLIC KEY TMP	128 BYTES
4	8 IDs ENCRYPTED BY SESSION KEY	32 BYTES
5	TIME STAMP	4 BYTES

When RREQ received to destination node, that node will create 8 series of unreal identities and also one 128 bytes session key. Destination node creates a route reply message as follow and sends it to source node. The first part of RREP message is message type. Like other messages, message type in the RREP takes one byte. After that, RREP contains 8 bytes as SRC-AREA and 8 bytes for DST-AREA.

Now, destination node encrypts the session key by temporary public key which sent by source node and puts it as the next part of RREP message. Also, it encrypts unreal identities by this session key. Encrypted identities will take 32 bytes of RREP messages. Final part of RREP is time stamp. Time stamp like other messages will take 4 bytes of RREP and it will be equal by RREQ's time stamp.

C. RREP2

The source route reply will send when the RREP is received. After receiving the RREP, the source creates a series of unreal identities and encrypts them by session key which sent by the destination node. The source creates a RREP2 message by following details. Like other messages RREP2 has one byte for message type. The next parts of RREP2 are 8 bytes for DST-AREA and 8 bytes for SRC-AREA. After that, source node will put encrypted identities on RREP2 messages, it takes 32 bytes. The final part of RREP2 is time stamp, like other PIDP messages. Time stamp takes 4 bytes and it will be equal by RREP's time stamp.

Table 3: Source Route Reply (Rrep2)

MESSAGE TYPE	RREP2	1 BYTE
1	DST-AREA	8 BYTES
2	SRC-AREA	8 BYTES
3	8 IDs ENCRYPTED BY SESSION KEY	32 BYTES
4	TIME STAMP	4 BYTES

D. DATA

After making a route and exchanging the unreal identities, source and destination nodes can send data. Data message has seven parts. The first part, like other messages, is message type which takes one byte of data message. The next part will be message size. Because data messages size are variable, message size can help nodes to know about the completeness of message receiving. Message size takes one byte of data message.

Table 4: Data Messages

MESSAGE TYPE	DATA	1 BYTE
1	PACKET SIZE	1 BYTES
2	ONE OF DST IDs	4 BYTES
3	ONE OF SRC IDs	4 BYTES
4	DATA ENCRYPTED BY SESSION KEY	VARIABLE
5	TIME STAMP	4 BYTES
6	SEQUENCE NUMBER	1 BYTES

Now, the sender chooses one of the destination's unreal identities and it takes next 4 bytes of the data message. Also, the sender will choose one of its unreal identities and puts it as next 4 bytes of the data message. After that, sender will encrypt data and puts it in the data message. This part of data message is variable and does not have static size. Time stamp, like other messages, is next 4 bytes of the data message. The time stamp will be equal by RREQ's time stamp. Finally, the sender node will propose a sequence number for data messages. Sequence number could be useful for data which take more than one data message and the receiver can prioritize received data.

E. ACK-REP

There is one acknowledgement message for each data message. When a data packet received to destination, the destination node should send an ACK-REP to sender to inform the sender that data is received. ACK-REP contains one byte message type and one byte for informing that the data received completely or not. There should be 4 bytes for source identity and 4 bytes for destination identity. Next part will be sequence number to inform the sender to know which data packet is received or not received to the destination node. Also, this message contains 4 bytes time stamp equal by RREQ's time stamp.
ACK-RREP details come in table 5:

Table 5: ACK-REP Message Details

MESSAGE TYPE	ACK-RREP	1 BYTE
1	ONE OF SRC IDs	4 BYTES
2	ONE OF DST IDs	4 BYTES
3	ACK	1 BYTES
4	SEQUENCE NUMBER	1 BYTES
5	TIME STAMP	4 BYTES

4. ROUTE TABLE

PIDP does not use route table for saving a route which has made. When a packet received to a node, that node, it can be intermediate node or destination node, calls a hash function and makes 8 bytes hash from the received packet. It could be useful to decrease falsehood rings. The node will search in its route table and looks for same stored hash; if there was any same stored hash, the node drops the packet. Otherwise, the node will save packet's hash in the route table and does the operations on packet if needed.

PIDP uses 4 different functions to support route table: hash function, route table update, hash save, and hash find.

5. ROUTE QUEUE

Although, each node can operate its packets separately, there is no way to process all packets which received to node simultaneously. So, PIDP uses route queue to prioritize packets and does process on them. Route queue has some function to store, find, update, and process on packets.

First of all, when a packet received to a node, that node calls the saving function and stores the packet in queue. Each stored packet contains packet details and its time out. Packets will store until processing or finishing their time out. When a packet is in first priority, route queue calls a function and does processes for it.

6. PIDP ROUTING

As mentioned above, PIDP uses the position and identity of nodes together. Packets in PIDP contain route request (RREQ), route reply (RREP), source route reply (RREP2), data (DATA), and acknowledgment (ACK-REP). First connections follow position-based routing and other connections are based on identity. This part explains how PIDP routing works.

When a node decides to make a route and sends some data to one other node, it prepares a RREQ message. Source node will create a temporary public key and puts it in RREQ packet. RREQ should contain destination position area, source position area, temporary public key, message type, and time stamp. The source node guesses how long a RREQ takes to receive to destination and puts it as time stamp. If this RREQ did not reply by destination node during time stamp's time, the source knows that RREQ did not receive to destination; so, it increases time stamp and sends RRQ again. This circle continues until receiving route reply packet or after 100 times increasing.

After making a RREQ packet, the source will broadcast RREQ to its neighbors. When a RREQ message received to a node; first of all, that node takes a hash from RREQ and looks for any similar hash message in its route table. If there was not any similarity, the node will put the hash of RREQ packet in its route table and broadcast it again. Otherwise, the intermediate node will drop the RREQ message; because it has a similar hash and the message is repeated.

The route request packet will broadcast by intermediate nodes until its time stamp is finished or it goes in a falsehood circle and all intermediate nodes have been broadcasting it once. Otherwise, the route request message will receive to the destination node.

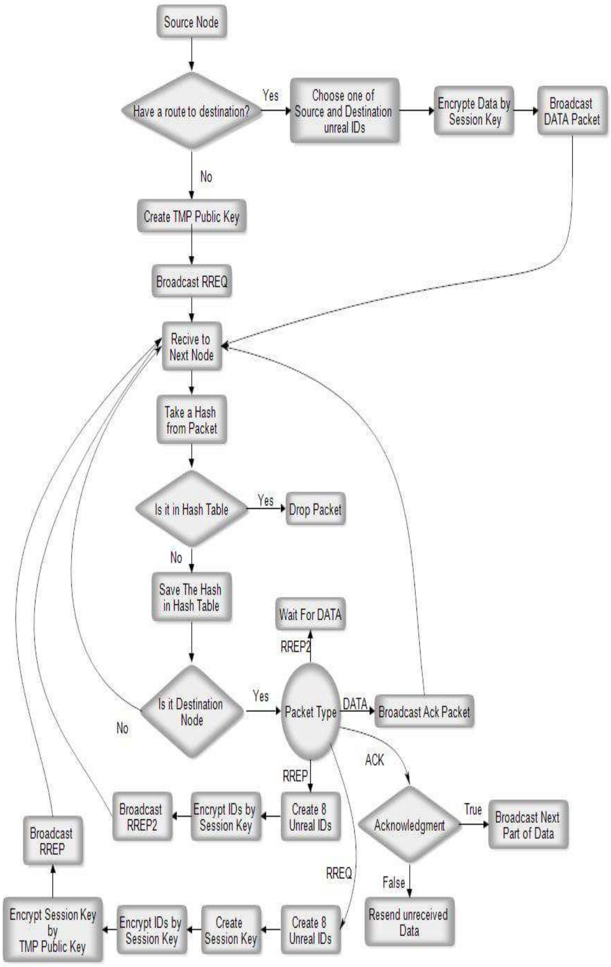

Figure 1: PIDP Flowchart

When a packet received to destination node, it also will store a hash message from that. Next, the destination node creates a session key. Also, it creates a series of 8 unreal identities and encrypts them by session key. After that, it encrypts the session key by temporary public key which has sent by the source node. Now, destination node will send a route reply message contains these encrypted identities, encrypted session key, and also time stamp, destination position, and source position.

Route reply packet will send to source node similar by the route request message. All intermediate nodes make a hash of the route reply packet and broadcast it. The similar route reply messages will drop by intermediate nodes. It continues till RREP received to source node or time stamp finishing, also if the route reply goes to a falsehood circle.

If there was no source reply message during time stamp from source node, the destination node will increase the time stamp and sends it again. It continues until receiving source reply packet or over 100 route reply sending.

When route reply message received to source node; it makes a series of 8 unreal identities and encrypts them by session key which sent by the destination node. The source node will send a source route reply contains these encrypted identities, destination position, source position, and time stamp. All routing operations to transfer source route reply are similar to destination route reply.

Now, if source route reply received to destination node, it will send an acknowledgment packet to source node. The ACK - REP packet will contain one of the destination unreal identities, one of the source unreal identities, time stamp, true value for ACK part, and zero value for the sequence number. This packet will send to source node by identity based routing. All transferring operations on ACK-REP packets are similar to other PIDP packets.

Finally, when ACK-REP received to the source node, it starts to send data by unreal identities. Each data packet contains one of destination identities, one of source identities, time stamp, sequence number for each related data packet, and encrypted data by session key. Operations of transferring the data packet are like other PIDP messages. For each data packet, destination node will send an acknowledgment message by equal sequence number.

7. COMPARISON ON ROUTE TABLE AND HASH TABLE

According to Precise Vehicle Topology and Road Surface Modeling Derived from Airborne LiDAR Data the average speed of vehicles in Ohio roads is 49 mile/hour. Also, the vehicles which flow from three proposed points in order are 3234, 2646, and 2793 vehicle/hour. Thus, the average vehicles which cross a proposed point in the road is 2891 vehicle/hour (Toth, 2010). This study can estimate the topology changes in VANET according to obtained vehicle changes.

Table 6: Traffic Flow Data (Toth, 2010)

Lane Number	Speed (mile/hour)	Flow (vehicle/hour)
L1	50	3234
L2	47	2646
L3	48	2793
Total	49 ± 10	8673 ± 1100

Toth et al (2012) estimate that the destiny of vehicle changes 177 ± 0.2 (vehicle/mile). Indeed, because the average speed of vehicles is 49 (mile/hour), the estimated topology changes can be obtained by equation 5.1. According to this equation, the topology changes estimated at 2.4 Vehicle/Second. Thus, when the topology changes 2.4 times per second, usual route tables are not useful.

*Topology Change = [Average speed * Average Destiny] /3600 (vehicle/Sec)* (equation 1)

PIDP uses a hash table instead of route table. In this case, PIDP takes a hash from each packet and store it. When a new packet received, PIDP node takes a hash value of new packet and compares it with its hash table. If the hash value matched, the PIDP node will drop the packet. Otherwise, the node will operate the packet. Hash tables can reduce 50% of waste operations on packet and packet transaction. Although, hash tables can reduce the waste packet transaction, there is infinite packet sending in VANET without time stamp. Time stamp proposes a limited time to send each packet.

Also, the hash table is useful to recognize any modifying by an adversary. If two different messages with same accessible detail received to a node, the node can inform the modifying by comparing hash of those messages. It could be more useful when the node is a terminal node.

8. SECURITY ANALYSIS

One of the major problems in secure routing is that intermediate nodes should not be able to read the data through packets which sent by terminal nodes. To gain this feature cryptographic algorithms are useful. PIDP uses Asymmetric algorithms for RREP. In this case, the source node sends its public key through RREQ message to destination. Destination node can encrypt unreal identities and session key by this public key. Thus, only the source node can decrypt the RREP details and know about identities and session key. Other messages will encrypt and decrypt by symmetric algorithms. Although, Asymmetric algorithms are slow, they are useful when the routing protocol wants to send initial packets without any information about network.

9. PRIVACY ANALYSIS

Privacy is a central requirement for VANET systems. Generally, privacy for VANETs can be divided into two, not entirely separable, categories: preventing identity information leakage and preventing location leakage from intermediate nodes. These two categories are not entirely separable because if an intermediate node knows the identity, it can find the location too.

Some prior works such as PRISM use Trusted Third Party (TTP) to hide identity and location. But, it increases the traffic and also it is threatening to network because if an unrelated third-party can associate a single vehicle with multiple identities or pseudonyms, then it is easier for the third-party to track its target vehicle or user. PIDP allows the terminal nodes to interchange identities in secure transmission without using TTP.

Hiding the location of nodes is the next major goal of PIDP. As mentioned above, VANET topology changes almost 2.4 times per second. PIDP uses only three initial messages based on position routing. Due to VANET nature, these three messages can be negligible. There is no doubt that due to VANET topology nature, recognizing a node location by only first three messages is impossible.

The final main goal of PIDP is to hide identity of terminal nodes from unrelated third party or intermediate nodes. Through the first three messages based on position, PIDP exchanges 8 unreal identities of each terminal node for next packet transmissions. By these unreal identities, PIDP can use 82 different pair of terminal node's identity. In comparing on AODV, recognizing the terminal nodes in PIDP is 97.4% safer (equation 2). To do the comparison between AODV and PIDP, this study changed the existing AODV protocol and added temporary identities in it. In this case, the proposed routing protocol uses 8 temporary identities for each terminal node for AODV. Thus, there is 64 pair of identities to make a connection between two nodes. Figure 5.1 shows the simulation results of the pair of nodes connections in AODV and PIDP by NS2. In this figure, Node_0 and Node_1 are two nodes which connected by AODV and Node_0_change and Node_1_change which connected by changed AODV. This figure can show that what intermediate node see from the packet transmissions of two terminal nodes in AODV and PIDP. It is clear that finding the nodes from one pair of identities in all packets is easier than finding them from 64 pair of identities.

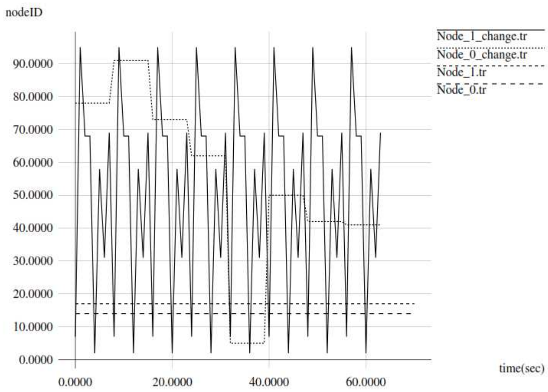

Figure 2: Different pair of node's identities in AODV and PIDP

*Possibility of identity hiding= (Possible couples of identities in previous protocol in each transmission)/(Possible couples of identities in new protocol in each transmission)*100*
(equation 2)

Delivered packet rate and total RREQ sends are two main traffic measurements. Figure 8 shows the delivered packets based on population of nodes in the network. Also, Figure 9 shows the total number of RREQ based on population of nodes. These figures show that the differences in delivering packet rate and total RREQ sends between AODV and changed AODV are negligible.

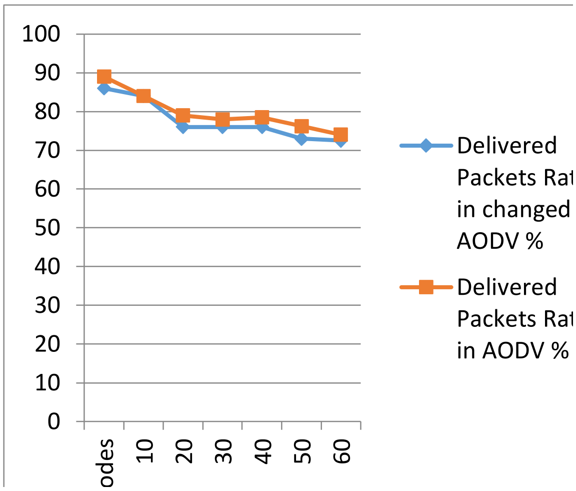

Figure 3: Delivered Packet Rate

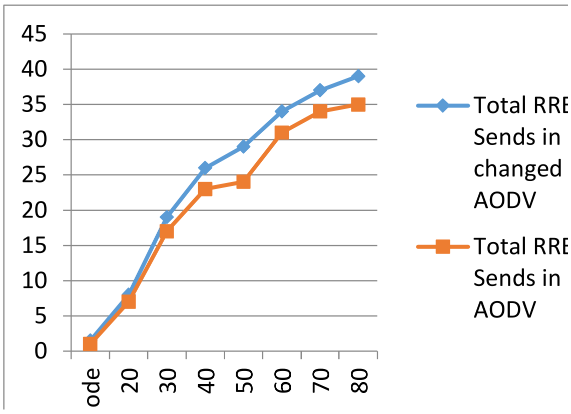

Figure 4: Total RREQ Based on Population of nodes

10. CONCLUSION

PIDP is a new routing protocol for VANETs to improve privacy compliant secure routing. It is the first routing protocol base on identity and position together. PIDP can hide the exact position and the real identity of terminal nodes from intermediate nodes. It is useful to prevent from Sybil attack and Sinkhole attack. Also, because of hash table, PIDP can inform the terminal nodes about any modifying in packets by suspected nodes.

REFERENCES:

[1] Abdoos, M. Faez, K. and Sabaei, M. (2009). Position Based Routing Protocol with More Reliability in Mobile Ad Hoc Network. World Academy of Science, Engineering and Technology 49. 248-252.

[2] AntolinoRivas, D. J. Barcelo´, M. M. Zapata, G. Morillo, J. D. (2011). Security on VANETs: Privacy, Misbehaving Nodes, False Information and Secure Data aggregation. Journal of Network and Computer Applications 34. PP 1942–1955.

[3] Blazevic, L. Boudec, J. L. and Giordano, S. (2005). A Location-Based Routing Method for Mobile Ad Hoc Networks. IEEE Transaction on Mobile Computing, VOL. 4, NO. 2. PP 97-110.

[4] Brestford, A. R, Stajano, F. (2005). Location Privacy Computing. IEEE Pervasive Computing 2, PP 46-55.

[5] Camp, T. Boleng, J. Williams, B. Wilcox, L. Navidi, W. (2001). Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks. International Conference on Mobile Computing and Networking (Mobicom), PP 243–254.

[6] Chen, S. Wu, M. (2010). Anonymous Multipath Routing Protocol Based on Secret Sharing in Mobile Ad Hoc Networks. International Conference on Measuring Technology and Mechatronics Automation. IEEE. PP 582- 585.

[7] Chim, T. W. Yiu, S. M. L. Hui, C. K. V. Li, O. K. (2011). SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs. Ad Hoc Networks. PP 189–203.

[8] Defrawy, K. E. and Tsudik, G. (2011). Privacy-Preserving Location-Based On-Demand Routing in MANETs. IEEE Journal on Selected Areas in Communication, VOL. 29, NO. 10. PP 65-74.

[9] Defrawy, K. E. Tsudik, G. (2008). PRISM: Privacy-friendly Routing in Suspicious MANETs (and VANETs). Irvine. PP 248-258.

[10] Eichler, S. D¨otzer, F. Schwingenschl¨ogl, Ch. Caro, F. J. F. and Ebersp¨acher, J. (2004). Secure Routing in a Vehicular Ad Hoc Network.

[11] Emmelman, M. Bochow, B. Kellum, C. (2010).Vehicular Networking. Wiley, USA.

[12] F¨ußler, H. Mauve, M. (2002). A Comparison of Routing Strategies for Vehicular Ad-Hoc Networks. REIHE INFORMATIK. PP 100-114.

[13] Festag, A. Hessler, A. Baldessari, R. Le, L. Zhang, W. and Westhoff, D. (2009). Vehicle-to-Vehicle and Road-Side Sensor Communication for Enhanced Road Safety. Network Research Division.

[14] Festag, A. Noecker, G. Strassberger, M. Lübke, A. Bochow, B. Torrent-Moreno, M. Schnaufer S., Eigner, R. Catrinescu, C. and Kunisch, J. (2008). NOW – Network on Wheels: Project Objectives, Technology and Achievements. Proceedings of 5rd International Workshop on Intelligent Transportation (WIT). PP 211-216.

[15] Gerlach, M. Festag, A. Leinm¨uller, T. Goldacker, G. and Harsch, Ch. (2007). Security Architecture for Vehicular Communication. Open Communication Systems. PP 152-158.

[16] Harsch, Ch. Festag, A. and Papadimitratos, P. (2008). Secure Position-Based Routing for VANETs. Proceedings of IEEE 66th Vehicular Technology Conference (VTC Fall). PP 103-112.

[17] Hui, F. (2005). A survey on the characterization of Vehicular Ad Hoc Networks and routing solutions. ECS 257 Winter.

[18] Johnson, D. B. Maltz, D. A. (1996). Dynamic Source Routing in Ad Hoc wireless Networks, in: Mobile Computing. Kluwer Academic Publisher.

[19] Kaur, M. Kaur, S. and Singh, G. (2012). VEHICULAR AD HOC NETWORKS. Journal of Global Research in Computer Science. Volume 3, No. 3. PP 61-64.

[20] Kent, S. T., Millet, L. I. (2002). IDs-not That Easy: Questions about Nationwide Identity Systems. Natl. Academy Pr. PP 42-49.

[21] Li, F. Wang, Y. (2007). Routing in Vehicular Ad Hoc Networks: A Survey. IEEE VEHICULAR TECHNOLOGY MAGAZINE. PP 12-22.

[22] Maqsood , A. Khan, R. (2012). Vehicular Ad-hoc Networks. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3. PP 401-408.

[23] Namboodin, V. Agarwal, M. and Gao, L. (2004). A Study on the Feasibility of Mobile Gateway for Vehicular Ad Hoc Networks. Proceeding of the First ACM Workshop on Vehicular Ad Hoc Networks. PP 66-75.

[24] Perkins, C. E. Royer, E. (1999). Ad Hoc on Demand Distance Vector Routing. Proceeding of IEEE WMCSA. PP 344-352.

[25] Perkins, C. E. Royer, E. (2003). Ad Hoc on Demand Distance Vector (AODV) routing, Internet Draft, Draft-IETF-MANET-AODV.

[26] Qian, Y. Moayeri, N. (2008). Design Secure and Application-Oriented VANET. National Institute of Standards and Technology. PP 264-272.

[27] Raya, M. and Hubaux, J. P. (2007). Security Vehicular Ad Hoc Networks. Journal of Computer Security, 15 (1). PP 39-68.

[28] Sarma, A. H. K. D. Kar, B. A. and Mall, C. R. (2011). Secure Routing Protocol for Mobile Wireless Sensor Network. IEEE.

[29] Xiong, H. Chen, Zh. Li, F. (2011). Efficient and Multi-Level Privacy-Preserving Communication Protocol for VANET. Computers and Electrical Engineering.

[30] Zakhary, S. R. Radenkovic, M. (2009). Reputation-Based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments. Computer Science & IT. PP 214-221.