International Journal of Multidisciplinary Research and Development 2014; 1(6): 145-147

International Journal of Multidisciplinary Research and Development

IJMRD 2014; 1(6): 145-147
www.allsubjectjournal.com
Received: 11-10-2014
Accepted: 19-11-2014
e-ISSN: 2349-4182
p-ISSN: 2349-5979

Alka Swami
M. Tech (CSE)
Mody University of Science and Technology (FET), Rajasthan.

Sarvesh Tanwar
Asst. Professor (CSE)
Mody University of Science and Technology (FET), Rajasthan.

Correspondence:
Alka Swami
M. Tech (CSE)
Mody University of Science and Technology (FET), Rajasthan.

Key Management Technique for group communication in Vehicular Ad Hoc Networks

Alka Swami, Sarvesh Tanwar

Abstract
VANET provides the communication among the Vehicles running on the road. To provide group communication in VANET, broadcasting is not an efficient method. Security in the communication is also requirement of some VANET application. Security in network stands for user anonymity, authentication, integrity and privacy of data. In this paper a key management technique is proposed that can provide the group communication in the VANET. The objective of this paper is to provide communication among selective nodes, which are willing to communicate with each other. The Security in communication is also enhanced through this approach.

Keywords: VANET, security, communication.

1. Introduction
Communication in VANET is the most popular application of wireless these days. In VANET the communication can either be among vehicle (vehicle to vehicle) or between vehicle and infrastructure (vehicle to infrastructure) [3]. Important issues in VANET are Privacy and Security. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private [2]. Security in network stands for user anonymity, authentication, integrity and privacy of data. Without security, a Vehicular Ad Hoc Network (VANET) system is wide open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents. Another form of attack in VANET is tracking [2]. Safety applications of VANET are traffic management, collision avoidance and safety warning. VANET is mostly configured for sharing safety messages from vehicle to vehicle. There are some scenarios in which group communication is also required by the vehicles. In case of police patrolling, car racing, and tour travelling, the group of vehicles will require sharing information without disclosing it to vehicles outside the group [1].
Use of Blind broadcasting to provide group communication in VANET results in exchange of useless and irrelevant message creates an overhead [1]. Unicasting is not preferred due to dynamic topology of the network.
Group formulation, group management, and key exchange are the issues which required special attention before starting group communication. Here in this paper, we are providing a method that is able to make the group communication in VANET among selective vehicles only and privacy is also concerned.

2. Proposed Work
VANET compromises three main network entities. Road Side Unit (RSU), it's a static component that serves as a gateway to a VANET and also allows connection to the Internet. The vehicle / User, are the nodes in the network who communicates with each other. Trusted Authority (TA), provide an identity for vehicles and monitor the network. The objective of this paper is to provide communication in selective nodes only which are willing to communicate with each other. Privacy is also considered as a major aspect of the communication.
For this algorithm we are assuming that nodes in a group have knowledge about each other. Every node has the information about all other nodes in the network. This information includes the existence of nodes, the public key of nodes. In this algorithm we are considering three scenarios.
Scenario 1: Network initialization.
Scenario 2: New node joins the network.

Scenario 3: Node leaves the network.

Scenario 1: Network Initialization

During network initialization, each node shares some information with RSU. This information contains the id of the node, a hash of its identity with a random number to include while sending back the session keys in order to prevent uncovering its identity in next phases, preference in send/receive list.

The other information it shares with RSU is how it is going to treat a new node, whether it is allowing a new node to communicate or restricting. This whole message is encrypted with the public key of the RSU. On the basis of the preference list of all the nodes in the network the RSU prepares a final list that includes who want to communicate with whom. One node can belong to more than one group. As per this final list RSU identifies the group, assign the group Ids and creates session keys. Every node has as many session keys as many groups it belongs to. RSU sends these session keys to the nodes in the form of session key, group id, hash. This message is encrypted two times to provide authentication and integrity. Now each node will have one sent session key and as many receiving keys as many nodes are in it's receive list.

When a node wants to communicate in a group it sends a message which is encrypted with send session key, and some additional information message id, group id and hash of both. Node signs the message with its private key. When the receiver receives the message, first it verifies the signature, if it matches then accept the message, discard otherwise. Then the receiver checks the hash, in order to ensure group id and message id are not corrupted. Then it checks group id, in order to ensure that this message belongs to this node or not. The receiver checks for message id, to get ensure that previously it has not received the same message.

Following are a few abbreviations used in the algorithm:

IDn: Identity of the node.
H (a||b): hash of a with b.
PbR: Public key of RSU
PvR: Private Key of RSU
PbN: Public Key of a node
PvN: Private Key of a node
SSK: Send Session Key

Step 1: Node sends preference list along with the information it wants to behave with a new node, its ID, hash of its identity with the random number. This whole message is encrypted with public key of Road Side Unit.

[Preference list, criteria for new node, IDn, H (IDn||a)] PbR

Step 2: RSU applies the algorithm

Step 2.1: Grouped the nodes as per their preference list.

Step 2.2: Allocate group IDs (group IDs ≤ number of total nodes in the network).

Step 2.3: Generate session keys.

Step 3: RSU sends relevant session keys, with hash, previously received from node, and the group IDs to the nodes by encrypting them with its private key then each node's public key.

((session key +H (IDn||a) + group IDs) PvR)PbN

Step 4: To communicate with other in a group, node exchanges following messages:-

Step 4.1: message is encrypted with send session key, [message] SSK

Step 4.2: group ID, Message ID, and Hash of both are attached with the message

[{[Message] SSK}, Group ID, Message ID, and H (GroupID||MessageID)]

Step 4.3: sender signs the message with its private ID

[{[Message] SSK}, Group ID, Message ID, and H (GroupID||MessageID)] PvN.

Step 5: When receiver receives a message:

Step 5.1: Verify signature; if verified, go to next step; else discard the message.

Step 5.2: Verify hash; if verified, go to next step; else discard the message.

Step 5.3: Check Group Id;

Step 5.3.1: If group id belongs to the node, go to next step.

Step 5.3.1: If group id does not belong to the node, forward the packet as it is.

Step 5.4: Check the message Id;

Step 5.4.1: If already exists, discard the message.

Step 5.4.2: else decrypt the message using receive session key and also forward the received message as it is.

Table 1: Node's preference list

Node	Send to	Receive from	Criteria for new node
P	Q,S,T,V	Q,R,T,U	N,N
Q	P,R,S,T	P,R,S,T,U	N,Y
R	P,Q,T,U	T,U,V	Y,N
S	P,Q,R,T,U,V	P,Q,R,T	Y,N
T	S,U	S,U,V	N,Y
U	P,Q,R,S,V	P,R,T,V	Y,N
V	Q,S,U	P,U,R	N,Y

Table 2: Application of algorithm on node's preference list

Node	Send to	Receive from	Criteria for new node
P	Q,S,V	Q,R,U	N,N
Q	P,S	P,R,S,U	N,Y
R	P,Q,U	U	Y,N
S	Q,T	P,Q,T	Y,N
T	S,U	S	N,Y
U	Q,R,V	R,T,V	Y,N
V	U	P,U	N,Y

Table 3: Group Id and session keys for each node

Node	Group Id	Send to	Receive from	Session keys
P	1	Q,S,V	Q,R,U	1+3
Q	2	P,S	P,RS,U	1+4
R	3	P,Q,U	U	1+1
S	4	Q,T	P,Q,T	1+3
T	5	S,U	S	1+1
U	6	Q,R,V	R,T,V	1+3
V	7	U	P,U	1+2

Scenario 2: New node joins the network

When new node joins the network, it also sends its send to/receive from preference list to the RSU. RSU scans for the "Criteria for new node" of the existing node in the network to check whether the node in Send to list of new node is willing to receive from new node or not. Similarly it check's for, receive from list of new node.

Table 4: Send to/receive from Preferences of new node A.

Node	Send to	Receive from	Criteria for new node
A	P,Q,S,U,V	Q,R,U,V	Y,Y

Table 4 shows the send to/receives from preferences of new node A with the criteria to deal with new nodes. After receiving it RSU applies the algorithm again. RSU scans the criteria for new node of all the existing nodes. New Node A wants to send message to node Q and Q is also willing to receive from the new node. RSU adds the node A to the receives from list of node Q and Add Q to the send to list of node A. Number of session keys of the nodes also change. Table 5 shows the group id and session keys of nodes after joining of new node.

Table 5: Group Id and session keys of nodes after joining of new node

Node	Group Id	Send to	Receive from	Session keys
P	1	Q,S,V	Q,R,U	1+3
Q	2	P,S	P,RS,U,A	1+5
R	3	P,Q,U,A	U	1+1
S	4	Q,T	P,Q,T	1+3
T	5	S,U	S	1+1
U	6	Q,R,V,A	R,T,V	1+3
V	7	U	P,U,A	1+3
A	8	Q,V	R,U	1+2

Scenario 3: Node leaves the network

When a node leaves the network, algorithm removes the entry of the leaving node from "Send to/receive from" list of all the other nodes and also refreshed all the keys which are shared with leaving node. In the example node S leaves the node.RSU removes the entry of node S from the list and all the session keys shared with S are also refreshed.

Table 6: Group ID and session keys of nodes after a node leave the network

Node	Group Id	Send to	Receive from	Session keys
P	1	Q,V	Q,R,U	1+3
Q	2	P	P,R,U,A	1+4
R	3	P,Q,U,A	U	1+1
S	**4**	**Q,T**	**P,Q,T**	**1+3**
T	5	U		1
U	6	Q,R,V,A	R,T,V	1+3
V	7	U	P,U,A	1+3
A	8	Q,V	R,U	1+2

3. Conclusion

In this paper, a group based key management technique is proposed to provide privacy and security in VANET. Here privacy is achieved by sharing the keys to selective vehicles which want to communicate between each other. Unlike flooding, in this technique redundancy is less as multiple technique is used, instead of broadcasting. This also reduces the key refreshment load. The performance may differ in sparse and dense network.

4. References

1. ZeeshanShafi Khan, Mohammed Morsi Moharram, Abdullah Alaraj, Farzana Azam. "*A Group Based Key Sharing and Management Algorithm for Vehicular Ad Hoc Networks*." The Scientific World Journal, Volume 2014, Article ID 740216, 8 pages, 2014.
2. Jessy Paul, Elizabeth Saju, Mercy Joseph Poweth. "*Privacy in VANET using Shared Key Management*. International Journal of Innovative Research in Science Engineering and Technology, 2014.
3. AM Arul Raj, Naganthan. *A study of signcription with group signature based authentication in vehicular ad-hoc network.* International Journal of Advanced Information and Communication Technology, 2014.
4. Rashmi R, Gandhi S. *Survey of Various Security Techniques in VANET.* International Journal of Advanced Research in Computer Science and Software Engineering 2014; 4(6):2014.
5. Yong Hao, Yu Cheng, Chi Zhou, Wei Song. *A Distributed Key Management Framework with Cooperative Message Authentication in VANETs"*. IEEE Journal on Selected Areas in Communications 2011; 29(3).
6. Sasikala G, Dhanalakshmi KS. *Key Management Techniques for VANETs.* International Conference on Electronics, Communication and Information Systems.
7. You Lu, Biao Zhou, Fei Jia, Mario Gerla. "*Group-based Secure Source Authentication Protocol for VANETs",* IEEE Globecom Workshop on Heterogeneous, Multi-hop Wireless and Mobile Networks, 2010.
8. Vishal Kumar, Shailendra Mishra, Narottam Chand. *Applications of VANETs: Present & Future*". Scientific Research, Communication and Network, 2013.
9. Palanisamy V, Annaduri P. Secure Group Communication using Multicast Key Distribution Scheme in Ad Hoc Network (SGCMKDS). Internation Journal of Computer Applications (0975-8887) 2010; 1(25).