Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.118 – 129

RESEARCH ARTICLE

THE NEW RSU BASED ON SECURE DATA TRANSMISSION AND SYBIL ATTACK DETECTION SYSTEM IN VANET

K. Malathi[1], Dr. R.Manavalan[2]
Research Scholar in Department of Computer Science, Periyar University, Tamil Nadu[1],
Head of the Department of Computer Applications, Periyar University, Tamil Nadu[2]
K.S.Rangasamy College of Arts and Science, Tiruchengode-637-215
Email: *malathi2301@gmail.com*

Abstract-- In Vehicular Communication, the security system against the attacker is an essential one. Sybil attack is an identity based attack through which the vehicle can successfully masquerades the ID of vehicles to create the wrong destination. The identification of Sybil attacks, determining the number of attackers and eliminating them is a challenging task in vehicular ad hoc Network. The message verification is an approach that is used to detect the Sybil attack in vehicles. This approach did not predict the attackers accurately. To overcome this problem, the paper proposes Diffe-Hellman key algorithm to detect the Sybil attack. The Diffe-Hellman key algorithm monitors and gives the secret key to the vehicles to reach the correct destination in Vehicular Ad Hoc Network. Analytical and simulation experiments result shows that the proposed scheme detects the Sybil attacks in VANET efficiently and robustly with the cost of reasonable overheads.

Key words: Vehicular networks, communication security, message authentication, certificate revocation

I.INTRODUCTION

Vehicular ad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic

© 2015, IJCSMC All Rights Reserved

communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs.

It is a new type of network which is expected to support a large spectrum of mobile distributed applications applied on vehicles [1]. VANET is a subset of MANET. In VANET each node is a vehicle or RSU (Road Side Unit) which can move freely within the network range and stay connected. Every node communicates with other nodes in single hop or multi hop. VANET provides safe and non safe services to the drivers. VANET constitutes short range radios installed in vehicles, Road Side Units (RSUs) and central authorities which are responsible for identity registration and management. Communication in VANET is Vehicle to Vehicle (V-V) and Vehicle to Infrastructure (V2I).

In VANET, it is always assumed that the malicious attacker can collect messages sent by other vehicles and monitor the vehicle's movement as well [7]. It is enabled to speculate the information and trace the vehicle's real identity, travelling routes and position. To become a real technology with public safety on the roads, Vehicular Ad Hoc Network (VANET) needs appropriate security architecture. Secure architecture should protect it from different types of security attacks and preserve privacy of the drivers. One of these attacks against Vehicular Ad Hoc Network is Sybil attack, in which the attacker is creating multiple identities that are identities belonging to other vehicles or dummy identities made by the attacker. The overview of the proposed model is discussed in section 1.1.

A. Overview of proposed model

Fig. 1 shows the overview of the proposed model. The information is clustered by the nodes. RSU gives key to the vehicles. By using the Diffe-Hellman key algorithm the RSU gives secret key to the vehicle in the source. After getting the key from source (RSU) the vehicle starts to move .Before reaching the destination the vehicle again get the key from RSU (destination)[12]. If the key gets matched the vehicle reaches the destination. The Message verification and Diffe-Hellman algorithm are implemented to detect the Sybil attack and localize them in VANET.

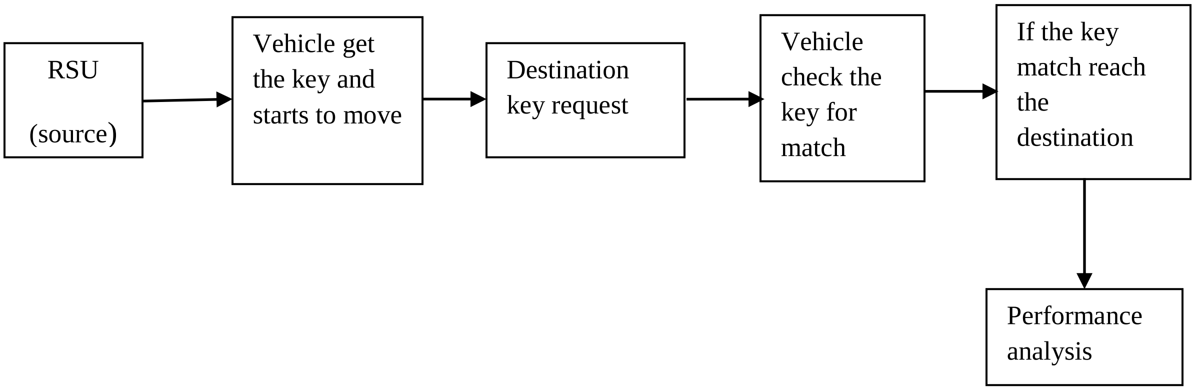
RSU
(source)
Vehicle get the key and starts to move
Destination key request
Vehicle check the key for match
If the key match reach the destination
Performance analysis

Fig 1. Block diagram of proposed system

The rest of this paper is organized as follows: In Section II, some related works are discussed. Section III discuss about the Expedite Message Authentication Protocol (EMAP). Message Verification Algorithm is discussed

© 2015, IJCSMC All Rights Reserved

in Section IV. The Diffe-Hellman key algorithm for detecting and localizing the Sybil attack is provided in section V. In Section VI, the performance analysis of the proposed framework is discussed. Section VII provides the final conclusion with future scope.

II. RELATED WORK

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [4, 12]. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long. In [12], Hubaux identifies the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In [4], Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANETs. In 2002, Samuel Madden et al., [3] proposed a Sybil attack detection technique for urban vehicular networks. In these schemes, a number of location information reports about a vehicle are required for identification. Road Side Units (RSUs) periodically broadcasts an authorized time stamp to vehicles in its vicinity. Vehicles collect these authorized time stamps and the same is used for future identity verification. Trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification process. However, the location privacy was not taken into consideration since RSUs use long term identities to generate signatures. The location information of a vehicle can be inferred from the RSU signatures. In Footprint, authorized messages issued from RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed. In 2005, Jinyuan Sun et al., [7] proposed ID-based cryptosystem framework to address the security problem in VANET. The method achieved desired privacy by vehicles and required non repudiation by authorities; in addition to that fundamental security requirements including authentication, message integrity and confidentiality are satisfied. In this framework, certificates are not needed for authentication. It increases the communication efficiency for various VANET applications where the real-time constraint on message delivery should be guaranteed. The result showed that the framework achieved good communication and authentication security in some extent. In 2013,ByungKawn Lee et al.,[16] Proposed a detection technique against a Sybil attack(DTSA) protocol using Session Key based Certificate(SKC) to validate inter-vehicle IDs in VANETs. In DTSA,SKC(Session Key based Certificate) is used to verify the IDs among vehicles, and also generates a vehicle's anonymous ID, a session Key, the expiration date and a local server's certificate for the detection of a Sybil Attack and the verification time for ID. However, none of these approaches are suitable for determining the number of attackers when there are multiple adversaries collectively use the same identity to launch malicious attacks. There is no ability to localize the positions of the adversaries after attack is detected. None of the existing work can determines the number of attackers when there are multiple adversaries uses the same identity. Additionally, the proposed approach can accurately restrict multiple adversaries even though the attackers vary their transmission power levels to Sybil the system of their true locations.

III. EXPEDITE MESSAGE AUTHENTICATION PROTOCOL (EMAP)

EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

System Model

As shown in Fig. 2, the system model under consideration consists of the following: A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. Roadside units (RSUs), which are fixed units, are distributed all over the network. The RSUs can communicate securely with the TA.OBUs, are embedded in vehicles [9]. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

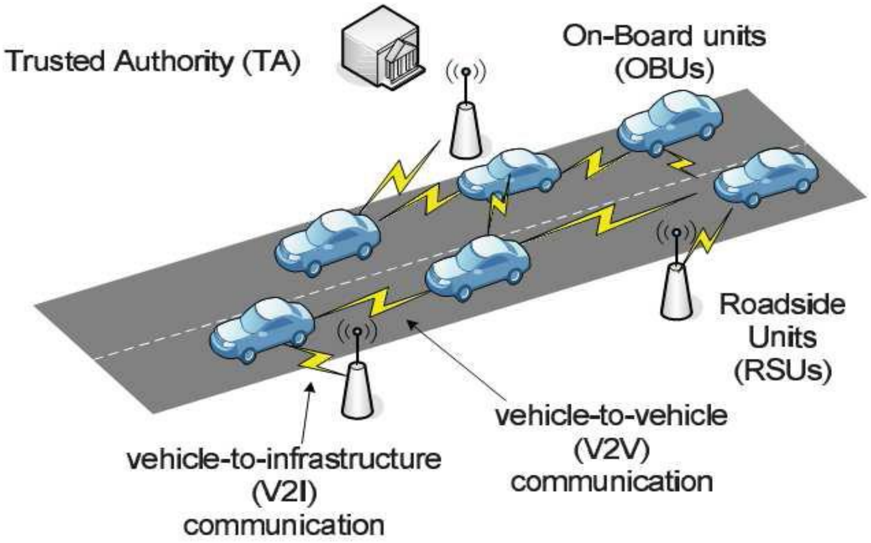
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Fig 2: System Model

EMAP Initialization

```
Step 1: Select two generators P and Q
Step 2: for i=1
Step 3: Select a random number ki
Step 4: Set the secret key Ki =kiQ2GG1
Step 5: Set the corresponding public key Kþi =1kiP2GG1
Step 6: end for
Step 7: Select an initial secret key Kg 2GG2.to be shared between all the non-revoked OBUs
Step 8: Select a master secret keys2ZZq
Step 9: Set the corresponding public key P=P
Step 10: Choose hash functions H
Step 11: Select a secret valuev2ZZq and set v=v
Step 12: for i=1 to obtain a set V of hash chain values
Step 13: end for
Step 14: for all OBU in the network, TA; do
Step 15: for i=1; do
Step 16: Select a random number
Step 17: Upload the secret key
Step 18: end for
Step 19: Upload CERT of OBU
Step 20: end for
Step 21: end for
```

Fig 3: Working of EMAP

IV. MESSAGE VERIFICATION ALGORITHM

The purpose of a Message Verification algorithm is to verify the message between the vehicles and CRL (Certificate Revocation List).If the vehicles get the message from the CRL it starts to move. The destination vehicle, OBU before receiving the message checks CRL status whether the certificate of the intended OBU is revoked or not. After verification, if the certificate is non revoked, OBU receives the message and decrypt it using the public key since asymmetric key cryptosystem is used. Else progress the revocation process. After decrypting, the OBU generates a REV Check by itself using the secret key and the message. It then verifies whether the generated REV check and the received REV Check match or not. If match occurs, the message integrity is verified. Else it specifies that false information or replay attacks has been involved and indicates that the integrity is lost [17]. Once the integrity is verified, the safety-related message is accepted and displayed. Otherwise the message is ignored. Vehicle A broadcasts a safety-related message to the relevant vehicles and Roadside Units in the area. The data flows of a message exchange pattern requiring data integrity in VANETs are illustrated.

Message Verification algorithm for Sybil attack Detection in VANET.

Input : Message from the CRL (Certificate Revocation List) to the vehicles.

Output : Verify the message and reach the destination

Sender's End:

Step 1. Creation of safety-related message:

The sender initiates a safety-related message.

Step 2. Creation of a MAC code for the safety-related message:

The safety-related message and secret key is used to create a MAC code.

Step 3. Message delivery: The message and the MAC code are ready for message dissemination to the intended recipient.

Receiver's End:

Step 4. Message reception: The intended recipient receives the message (safety-related message and MAC code).

Step 5. Certificate verification: Notice that there is not a universal sequence in which these processes should be performed.

Step 5.1: To examine the validity time period of the certificate against the current time.

Step 5.2: To check if the certificate is revoked against the CRLs.

Step 6. Client authentication and data integrity verification:

Step 6.1: To authenticate the received message from the sender.

Step 6.2: To verify the MAC code on the received message by using the secret key.

Step 7. Message display: Upon successful validation, the received message is rendered to the recipient.

Fig 4: Message Verification Algorithm in VANET

The message verification algorithm has the following disadvantages, failed CLR scenario is not enclosed, if a CLR is failed in a given time, the trajectory created at that event will not contain that CLR information along the trajectory. So other trajectories with this CLR look distinct.

A. DIFFE-HELLMAN KEY ALGORITHM

The Diffie–Hellman key exchange method allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel [18]. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Diffie–Hellman establishes a shared secret key that can be used for secret communications while exchanging data over a public network.

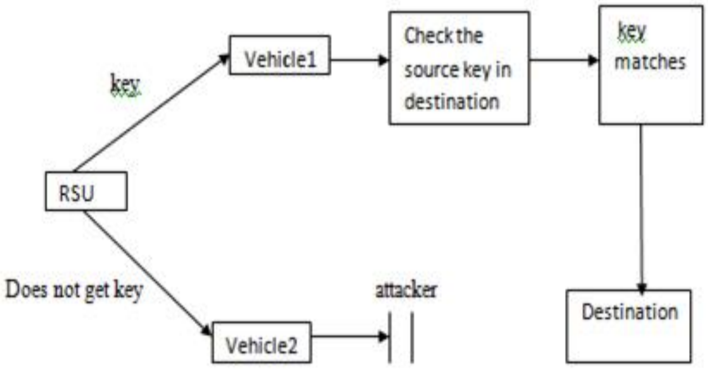

Fig 5: Working of diffie-Hellman Key exchange algorithm

In vehicular communication the source (RSU) wants to send the information to the destination through vehicles without any Sybil attack. So the RSU use the Diffe-hellman key algorithm to find the Sybil attack in VANET. Fig. 5 shows the working of the Diffe-Hellman key algorithm in VANET. The data is sent from source to destination on network through a base station. During that time any attacker can attack the data, so the secret key is generated for each node; it provides more security to avoid the data loss on the network. The source and destination

RSU provides the secret key for the vehicle to prevent the attackers. The key in the source RSU match with the destination RSU only then the vehicle reaches the correct destination.

Diffe-Hellman key algorithm for detecting the Sybil attack

```
Initialization : V(Vehicle); K(secret key); D(Destination); RSU
Input          :  Get the key from the RSU
Output         : Using the key for find the Sybil attacker

Step 1: RSU provide the key to the vehicle for the security. Distribute the key (k) to the vehicle.
Step 2: Vehicle get the key (k) from the source RSU
            Get k ();
Step 3: After get the key Vehicle starts to move toward the destination
Step 4: Destination send the key request to the Vehicle.
          { D= send request
Step 5: Vehicle match the source RSU key with the destination RSU key.
           V= Vehicle match the K()
           $k_s = k_d$
Step 5 : if (K match)
           Vehicle reach the destination
           { else
Step 6: The request node is suspected as a malicious node or attacker node.
            }
Step 7: Mark the attacker and block the attacker node.
          }
```

Fig 6. Diffe-Hellman key algorithm for detecting the Sybil attack

V. EXPERIMENTAL ANALYSIS

Simulations are conducted to analyze the performance of proposed Diffe-Hellman algorithm for Sybil attack in VANET. The reputation surroundings are produced using NS-2 for VANET.NS-2 came as extension of Tool Command Language (TCL).The execution of NS-2 is carried out by means of cluster surroundings of wireless vehicle nodes. The simulation area or open area topology of NS-2 execution is 1200 meters x 1200 meters. Simulation path is used to indicate the source and destination connections. The parameters and their values used for simulation configuration settings are tabulated in Table 1

Table 1. NS-2 Simulation Configuration Settings

Parameters	**Value**
Version	**Ns-allinone 2.28**
Number of Nodes	**63**
Simulation Area	**1200m x 1200m**
Broadcast Area	**250 m**
Data size	**512 bytes**
Simulation time	**360 sec**
MAC Protocol	**IEEE 802.11**
Routing Protocol	**EMAP**

NS-2 is used to build nonreal wireless environment at low cost. The performance of the proposed method is analyzed using the evaluation metrics such as Throughput, Vehicular Ratio and RSU performance. The shortest descriptions of these parameters are discussed below.

The amount of data transferred in a given amount of time from source to destination is called throughput. The network performance is good when the throughput is high and increases the packet delivery ratio and decreases the packet delay. Throughput is defined as

$$\textbf{Throughput} = \frac{P}{T}$$

where P is Total number of received Packets and T is Transmission Time.

Table 2: Throughput

Time (sec)	Throughput	
	Message Verification	Diffe-Hellman key
30	15	21
60	28	35
90	40	53
120	52	64
150	71	80

© 2015, IJCSMC All Rights Reserved

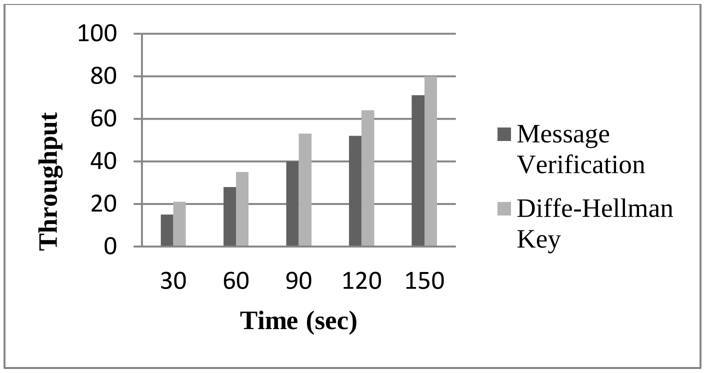

Fig 7: Throughput comparison between Message Verification and Diffe-Hellman key mechanism

The simulation results showed that the Diffe-Helman Key algorithm achieved the high throughput than the Message Verification algorithm. The results in the table 2 show the throughput earned by the Diffe-Helman Key and the Message Verification algorithm and the same is flashed in fig 7. In the time duration of 30seconds the throughput earned by the Message Verification algorithm is 15% where as the Diffe-Helman Key achieves 21% which is 6% higher than the Message Verification approach.

The Vehicular Ratio refers to the ratio of Vehicular packets transmitted and received from the source to destination successfully over the network. The Vehicular ratio is measured in the percentage as

$$\text{Vehicular Ratio} = \frac{P_r}{P_s} \times 100$$

where P_r is the received packets and P_s is the sent packets.

Table 3: Vehicular Ratio Ratio

Time (sec)	Vehicular Ratio	
	Message Verification	Diffe-Hellman key
30	12	19
60	25	32
90	37	49
120	56	70
150	69	81

© 2015, IJCSMC All Rights Reserved

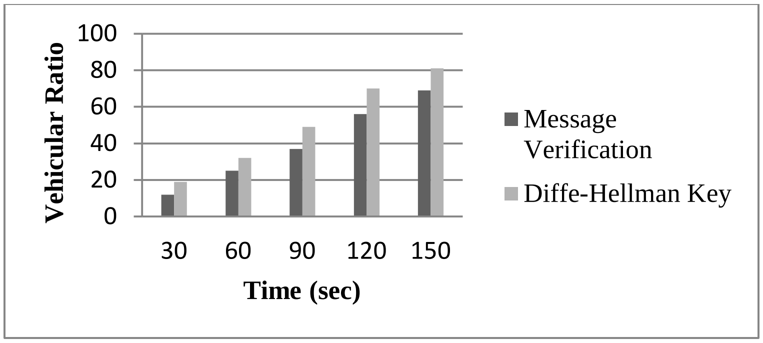

Fig 8: Vehicular Ratio comparison between Message verification with Diffe-Hellman Key mechanism

Vehicular Ratio is the ratio between sum of total number of vehicular packets received by destination and sum of total number of vehicular packets sent by source. The simulation results clearly show that Vehicular Ratio value will be low in transmission time by 30 seconds. The results in the table 3 show the Vehicular Ratio of Message verification with Diffe-Hellman Key approach and the same is projected in fig 8. Vehicular Ratio values are increased while the transmission time increases from 30 seconds to 150 seconds for both Message verification approach and Diffe-Hellman Key. The approach which yields high Vehicular Ratio is considered as better attack detector approach. While comparing Message verification approach with Diffe-Hellman Key, the Diffe-Hellman Key yields highest Vehicular Ratio. From this study, it is found that the reliability of Diffe-Hellman Key is better than Message Verification approach and it is noted that Diffe-Hellman Key approach is efficient than the other approach.

The RSU provides secrete key to the vehicle from the source which helps to provide security to the vehicle information. In Message Verification, the CLR is used to send the information securely. Using Diffe-Hellman the RSU generate the secret key for detecting the Sybil attack in VANET. Let h be the total number of the source-destination pairs between which the certificate can be updated before it expires when no RSU is allocated in the city. Then h is calculated as follows:

$$h = \sum_{s.d\varepsilon I, s \neq d} h(A_{\phi}, s, d)$$

Let A; be the allocation pattern in which no RSU is allocated in the city. Let h(A;; s; d) be an indicator that whether the source-destination intersection pairs between which the certificate can be updated or not before it expires when no RSU is allocated in the city. Note that when no RSU is allocated in the city, only the source-destination intersection pair (s; d) with driving time T(s; d) less than.

Table 4: Performance of RSU

Time (sec)	Performance of RSU	
	Message Verification	Diffe-Hellman Key
30	17	23
60	29	36
90	41	58
120	53	69
150	72	84

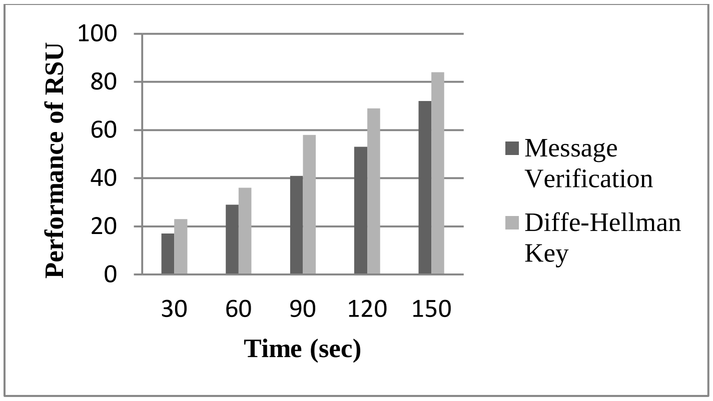

Fig 9: RSU Performance comparison between Message verification with Diffe-Hellman Key mechanism

The RSU performance achieved by the methods Message verification with Diffe-Hellman Key mechanism for various time slots are provided in the table 4 and the same is flashed in Fig 9. From the simulation result, it is noted that the high RSU performance is achieved by the Diffe-Helman Key than the Message Verification approach. The RSU Performance achieved by the Message Verification in the time duration of 30 seconds is 17% where as the Diffe-Hellman Key achieves high performance of 23% which is 6% higher than the Message Verification approach.

VI. CONCLUSION

In this paper the Sybil attack detection and localization scheme such as Message Verification and Diffe-Hellman Key approaches are analyzed in VANET using NS2 simulator. The existing Message Verification approach is performed to send the information packets securely through the vehicle from source to destination. The Diffe-Hellman key approach with EMAP is proposed to detect the Sybil attack in VANET and provide security to the vehicle. The simulation results showed that the performance of the Diffe-Helman Key with EMAP is better for efficient data transmission securely from source to destination by updating the information in RSU. In future, researchers may concentrate on Sybil attack detector approaches to facilitate high throughput, high Packet Delivery Ratio (PDR) and high RSU performance even though complex scenarios may occur.

REFERENCES

[1]. Arkus Kuhn," Probabilistic counting of large digital signature collections", In Proceedings of USENIX Security Symposium, 2000.

[2]. J. J. Wylie, M. W. Bigrigg, J. D. Strunk, G. R. Ganger, H. Kilite, P. K. Khosla, "Survivable Information Storage Systems", IEEE Computer 33 (8), IEEE, 2000, pp. 61-68.

[3]. R. Douceur, "The Sybil Attack," 1st Int'l. Wksp. Peer-to-Peer Systems, Mar. 2002

[4]. S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong," Tag a tiny aggregation service for ad-hoc sensor networks", In Proceedings of the Fith Annual Symposium on Operating Systems Design and Implementation (OSDI), 2002.

[5]. L. Hu and D. Evans," Secure aggregation for wireless networks". In Workshop on Security and Assurance in Ad hoc Networks, 2003.

[6]. Bartosz Przydatek, Adrian Perrig, Dawn Song," SIA: Secure Information Aggregation in Sensor Networks", 2003

[7]. Philippe Golle, Dan Greene, Jessica Staddon," Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in ACM International Workshop on Vehicular Inter-Networking (VANET), October 2004.

[8]. W. Junior, T. Figueiredo and H. Wong. Malicious node detection in wireless sensor networks. In Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS 2004)

[9]. Jeremy Blum and Azim Eskandarian, "The Threat of Intelligent Collisions," IT Professional, vol. 6, no. 1, pp. 24–29, 2004.

[10]. Jean-pierre hubaux, Srdjan capkun, and Jun luoepfl, "The security and privacy of smartvehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May 2004

[11]. Elaineshi and Adrianperrig," designing secure sensor networks", IEEE Wireless Communications December 2004.

[12]. T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode."Traffic view: Traffic data dissemination using car-to-car communication. In IEEE International Conference on Mobile Data Management (MDM), 2004.

[13]. B. Parno and A. Perrig. Challenges in securing vehicular networks. In Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[14]. S. Capkun and J.P. Hubaux. Secure positioning of wireless devices with application to sensor networks.In Proceedings of INFOCOM, March 2005.

[15]. E. Shi, A. Perrig, and L. van Doorn. Bind: A time-of-use attestation service for secure distributed system. In Proceedings of IEEE Symposium on Security and Privacy, 2005.