Taxonomy of Security in Vehicular Ad-Hoc Network

Mostofa Kamal Nasir *, A.K.M. Kamrul Islam*, Mohammad Touhidur Rahman and Mohammad Khaled Sohel*****

*Department of Computer Science and Engineering
Mawlana Bhashani Science and Technology University, Santosh, Tangail-1902, Bangladesh
**Daffodil Institute of IT (DIIT), Dhaka, Bangladesh.
*** Daffodil International University (DIU), 102 Shukrabad, Dhaka, Bangladesh

Abstract- Vehicular Adhoc NETworks (VANETs) have the high potential in commercial value and application prospect. For VANET have some specific security requirements so the routing protocols and security schemes in ad hoc networks not adapt to VANETs. As the vehicle move very quickly, hence it's necessary to a new security scheme for VANETs. In this paper we discuss the necessary requirements for security and safety in VANETs. We give detail taxonomy of security in VANET. Also describe the privacy and authenticity issue of vehicle to vehicle and vehicle to infrastructure and defined the problems of protecting privacy in VANET.

Index Terms- **Ad**-hoc network, Privacy, Authenticity, Intruder, VANETs

I. Introduction

Vehicular Ad-Hoc Networks (VANET) is a form of mobile ad-hoc networks. VANETs have the impending to optimize traffic in modern urban areas, reduce congestions and pollution, and increase passenger safety and comfort. The amount of information disseminating in VANET is enormous. This information is very wide in range to its speed, direction, emergency messages, surfing the internet and gamming information. Security for such networks represents a key point that is still under development. One of the most important aspects from the theoretical point of view is that, better communication efficiency can be achieved by sacrificing security and vice versa in VANETs. Applications design for such networks pose new security constraints[1]. The mobile devices have limited resources to spare, and the network connectivity is reduced because of the mobility of cars. We discuss the security issues design for VANET environments. Privacy of the passengers must be preserve in VANET because the security protocol is design not to rely on the driver's identity [2]. The authorities will consider authenticity to make the VANET more safe in terms of privacy deploy such as public keys encryption and the use of pseudonyms. All proposed solutions must be able to maintain the privacy of individual vehicle avoid tracing the path and the movement and check the accuracy of data with a low operating cost and handling enormous data each vehicle transmit and receive.

II. Privacy

The term privacy is Anglo-Saxon origin, originally referred the sphere of private life. But in recent decades the concept of privacy is means the right to control personal data. For last 15 years the privacy is increasingly subject to invasion to the intruder [3]. The privacy is the right to maintain the personal information and private life to be let alone. The policy often results in the ability of a person (or a group of people), to prevent the information on it becomes known to others, including organizations and institutions, if the person has not voluntarily choose to provide it, despite the enactment of special laws to protect people every day our privacy is violated more and more. The invention of new and new technology is the thread to violate the privacy [4]. The term privacy should also be applied in the field of VANET. This technology should be able to prevent any leakage of information regarding the tracking of routes carried by a vehicle and driver on the movements on road. The privacy of each vehicle and its passenger must be guaranteed in every respect to the authorities.

Privacy is obtained through the use of pseudonyms short-lived to the peer. A vehicle is given a nickname which will be changed periodically so one will not be able to trace the true identity of the vehicle. In the case of tracing of particular events (accidents, traffic jams, etc.) It make the correlation of data from the authorities involve that is associated with the nickname the real identity of vehicles [5]. The peers have a limited view of the information passing over a geographical area, so the use of pseudonyms of short duration is reasonable. The preservation of privacy requires the consideration of any peer as a potential malicious, in fact for every one of them makes use of security measures. This arises from the objective of preserving the security of the individual vehicle and the VANET.

III. Authentication

Privacy against the authorities is a very complex issue. First we start with the assumption that the authorities carry out in the most honest as possible the tasks assigned to them and do not abuse their powers. In case of corruption of some internal member authorities might still be provided illegal access to unauthorized individuals to sensitive data on roads, vehicles and their movements. It must govern by the authorities to splitting the power to different independent bodies, to control the privacy and can prevent corruption. The large number of bodies to be corrupt and the involvement to leaks information is difficult than single authority. VANET attacks can be carried out by different people with different purposes [6]. An "attacker" is a node (a vehicle) which maliciously trying to steal private data of another vehicle and / or illegally trying to sabotage the proper functioning of VANET. In general, an attacker tries to convince a node by non-existent or distorted

information [7]. He achieves this goal when he manages to convince by giving decency information to a victim. The attacker will send false data to other nodes by attached knot to victim like wildfire. A malicious node can distort the data on a share network. In VANET each node receives one message from many sources. The redundancy of this message is used for verification of accuracy of the data. If the same information is receive from multiple sources then the probability of the message be valid is high [8-9]. However use of redundancy of message makes it difficult to detect an attack.

IV. TYPES OF ATTACK

Possible attacks in the network can be various types, active, passive, control of movement, falsification of data etc. Attack can be classified based on nature, based o area of interest, based on object and based on impact.

4.1 Classification Based on Nature

Depending on the nature attacks can be classified according to fig. 1.

1. **Active vs. passive:** An active attacker is a node that can generate packets and placing on the network, while passive one is that can only push the message in the network.
2. **False information:** Attackers are spread wrong information in the network to influence the behaviour of other vehicles [10].
3. **False position:** Attackers use this technique of attack to alter the fields related to their position, speed, and direction of travel by broadcast messages. In the worst case, the attacker can clone other vehicles, hiding in this way their presence in case of accidents, and avoiding any responsibility [11].
4. **Vehicle tracking:** This is the scenario of like big brother, where a global observer can control the routes of the vehicles designated to use and the observed data for various purposes (for example, some companies that rent cars can trace their cars). To make such a control the "global observer" could control infrastructure such as roads or vehicles in a given geographical location. In this case, the attack is the passive type. We assume that the attacker does not use cameras or devices for tracking physically of a vehicle which wants to discover the identity. This assumption is made to create a scenario feasible in terms of manufacturing cost even if the application of devices such as cameras would give considerable aid to the controls of vehicles.

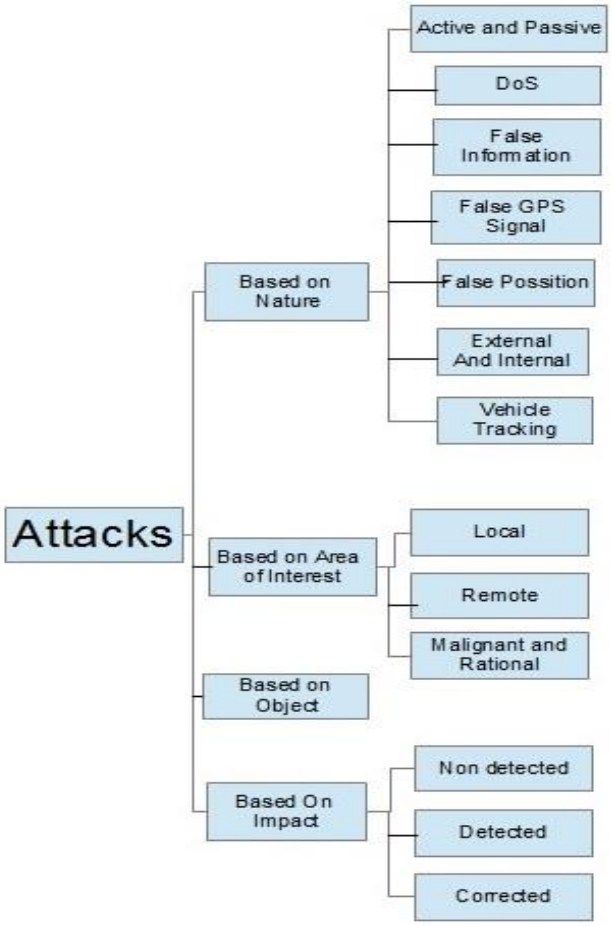


Fig. 1: classification of the attacks in VANET

5. **Internal vs. external**: Any attacks by internal nodes are part of the network. This means that the attacker node is a member of the network. Whereas any attacks by external nodes is considered by the network as an intruder. Generally attacks by internal nodes are most effective as they treats authenticated by the network.
6. **False GPS signal:** The vehicles that use GPS are easily vulnerable to various attacks such as the GPS signal.
7. **Denial of service:** In this style of attack a node may want to block the services offered by VANET or even may want to cause an accident. Examples of attack can be flooding the network with fake messages or blocking transmissions in the network itself. This kind of attack has no intention to make profit by the malignant node.

An example of attack in VANET shows in Figure 2. In this figure two vehicles A2 and A3 enter false information within a network for changing the flow of traffic of the road and obtain a useful result.

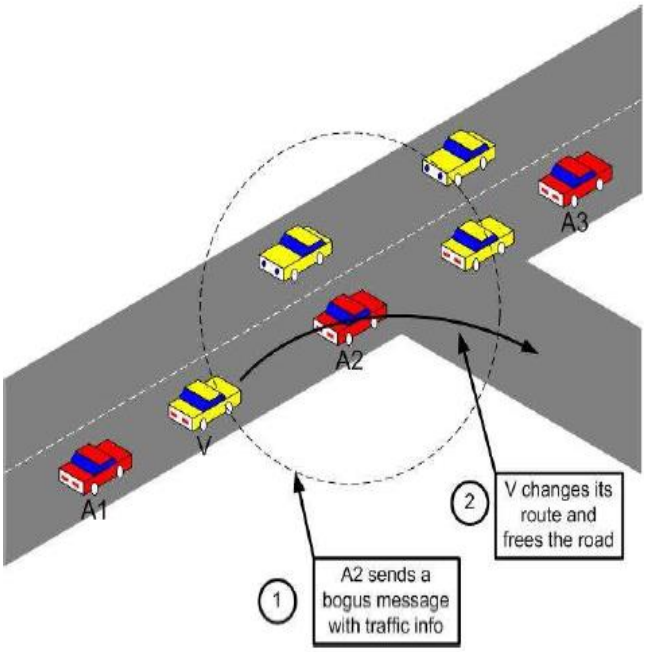


Figure 2: Attack with false information A2 and A3 disseminate false information to influence network.

4.2 Classification of attacks according to the region

Attacks based on the area of interest are those attacks based on geographical data. We define the attack nodes of an area of interest by "victim nodes ". The area of interest may be limited or extended. Characteristic of this kind of attack is the potential expansion of the infected areas where there is the presence of data corrupted by malicious nodes. The expansion can take place in peripheral area when one or more infected node passing bogus information into another area.

1. **Local attacks:** Attackers unleashed by malicious nodes to neighbouring nodes by sending false data in order to change the status of evaluation and decision of victim node. Such attacks can be very effective located in the vicinity of one or more malignant nodes. The victim node cannot make comparisons with other nodes in the network; therefore unable to test the veracity of the received data is valid.
2. **Remote attacks**: Attackers are attacks to targets node that is distant from the malicious node. The message sending by attackers node contain the fake information, it can arise conflict on a qualitative level between the message and the received message by neighbouring nodes to a target node.
3. Rational vs. evil: A malicious attacker does not seek personal benefits from attacks that push into network. This attack in the network does not consider the financial benefits; in contrast to a rational attacker seeks personal profit. To gain a personal profit, a rational attacker much more predictable than a malicious attack in terms of goals and objectives.

4.3 Classification of attacks according to the objectives

They may be also guided by well-defined objectives. The objectives can be traffic control in a given area, the control of vehicle movement, the induction to change the trajectory of vehicles, blocking a service or even block all the services offered by the VANET.

4.4 Classification of attacks based on Impact

The attacks may have different impacts depending on the technique and technology that the attacker uses. The classification according to the impact is as follows:

1. **Non Detected:** Attack is not detected by the target nodes. A target node cannot detect an attack if it is isolated or completely surrounded by the malignant nodes. It continuously transmits false information and a victim node accepts incoming fake messages. But as soon as the victim node is in the vicinity of an honest node, can re-evaluate the integrity of the data receive so far and then correct the message.
2. **Detected:** Attack detected by the target nodes. A victim node can detect an anomaly attack, because of the small amount of available correct data, remains in doubt about the contents of the receive data. This doubt remains until it encounters a sufficient number of honest nodes that provide a sufficient amount of information for a correction of the data. An example of node surrounded by evil nodes is represented in Figure 3

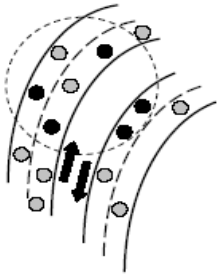


Figure 3: A node is surrounded by many malicious nodes and only one honest node

3. **Corrected:** A node detects a malicious node due to the data received from node that are in contradiction with the data of observations by honest nodes. Some nodes have the opportunity to correct the false messages, in addition to identifying the malicious node. An example of node surrounded by honest nodes and by some malicious node is represented in Figure 4.

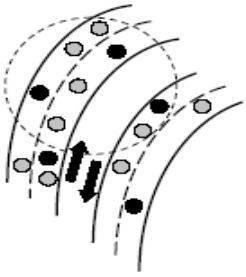


Figure 4: A node is surrounded by many honest nodes and only 3 nodes malignant

V. TECHNIQUES TO ENSURE SAFETY IN VANET

As seen in [12], attacks on a VANET or its subnet can be varied and with different purposes. Such attacks could undermine the road system, potentially creating a hazardous situation for vehicles and passengers. To avoid this type of dangers is necessary for a safety system that allows preserving the accuracy of messages transmitted and consequently the safety of the passengers.

5.1 Requirements for achieving security

Data exchange in VANET is safe if meets the following requirements:

Authentication: authentication is required by sender's messages; so that response of the vehicles to roads events is based on messages from legitimate senders.

Consistency: in addition to authentication, it is necessary to check the consistency of the data. It may happen that the sender is found to be authenticated but the data are sent to be false.

Availability: It is necessary to have alternative forms of communication even in the presence of strong communication channels, for denial of service attacks (DoS) attacks in some cases can create serious problems in the operation of the network.

Identification: In case of accidents, must be identify the drivers of the vehicles in order to study the flow of data elapsed between vehicles and neighbours in times prior to the accident.

Privacy: The privacy of vehicles should be ensured as much as possible. It should be avoid the unauthorized control of users to the tracking the vehicle movements.

Real-time constraints: Due to the high mobility of vehicles in the network, one needs the ability to react in real time to various events.

Verification of the positions: It is a necessary to verify the data received from the GPS through their neighbour nodes, to avoid the attacks on GPS coordinates.

5.2 Properties of Security protocol in VANET

1. A vehicle V periodically sends messages of a hop length of every 300 ms (the minimum range is 110 meters and the maximum is 300meters)
2. The interval between messages is sent to every100ms if the vehicles have low speeds or completely stop (10 miles / h ~ 16km / h)
3. Vehicles make decisions base on messages receive and send new message. For example, if a vehicle V receives a distress message from a vehicle W, V concludes that this danger also may include other vehicles in its time can send a warning message.

VI. PREVENTING THE THREAT IN VANET

The received data must be authenticated and verified to ensure security for protecting data from both internal and external nodes. The packets exchanged sensitive data between the vehicles. The lack of such data that does not require any form of encryption, but only a few form of authentication. There are two types of authentication mechanisms, symmetrical and asymmetrical. Public Key Identification (PKI) is use to verifying the identity of a vehicle. The PKI is managed and controlled with competence. Heuristics method is used to determine the nature of the attacks and targets, in order to predict the possible effect of the network and nodes. In symmetric authentication based solutions add sensors. In the following sections we will discuss in detail these three authentication solutions. We will also study the various features by that application.

6.1 Asymmetric Authentication

There are several methods on safety in VANET and the possibility of using asymmetric authentication associated with digital signatures, certificates and public keys [13]. The digital signature may be the best possible solution in VANET since the safety messages sent in this kind of network typically stand-alone and have need to sent as quickly as possible. In fact, in VANET a hand-shake prior to a communication between nodes, may create an overhead is not acceptable to the entire system [14]. Moreover, the huge number of nodes of the network and the connection of these sporadic to authentication servers, makes the use of public key identification (PKI), the most suitable way to implement an authentication system [13]. Though security is a vital issue, a very few protocols proposed for safety and security purpose.

With the use of PKI, each vehicle is assigned a key pair (public / private) and a session key which provides efficient authentication. A vehicle, before sending a message about road safety must sign it with its private key and must include CA (Certification Authority) as follows:

$$V = *: M, Sig_{\Pr Kv}[M|T], Cert_v$$

Where V= is the vehicle
*=Sender indicates all recipients,
M=is the message,
Sig $_{PrKv=}$ indicates the private signing of V,
| = indicates the concatenation of messages,
T=is the timestamp and
$Cert_V$ =indicates the public certificate of V.

The CA can be issued uniquely to each individual vehicle by a competent body. The receiver of the message must extract and verify the public key of V with the certificate and then use the certified public key to verify the signature of V. To perform these tasks, the receiver should be in possession of CA will have prior loaded. If the message is sent in a context emergency, it will be saved in an EDR (Event Data Recorder) so you can then make prospective investigation of an event that happened.

A. The use of keys for authentication

The use of private keys in VANET for transmitting message among vehicle is intended to arouse the interest of attackers. Attackers are interested in possession of the keys so you can send messages and sign them on behalf of other vehicles. Physical access to safety devices installed on vehicles shall be restricted to authorized personnel. The private key must renewed periodically to further increase the security. In market already have some commercial products which perform such task. Electronic ELP (Electronic License Plate) [15] issued by the administrative staff, or an ECN (Electronic Classic Number) issued by manufacturers of motor vehicles. These identities assigned to the vehicle, must be unambiguous and verifiable with controls by the competent authorities. A pair of keys anonymous fitted to preserve the privacy. This pair is a public / private key certified by the authentication authority, which does not contain information on the vehicle or its owner. Normally, every vehicle will be equipped with a set of keys anonymous set that will be able to prevent or control the tracking his movements. The ELP could also be installed by the authorities involved in the carriage on the vehicle, and the owner may periodically update the keys.

B. Certification and revocation of keys

Certifications, as mentioned above, can be attributed to government agencies (engine) or directly from manufacturers. It may happen, however, the need for the withdrawal of a key. Two scenarios that require the withdrawal of a key are as follows:

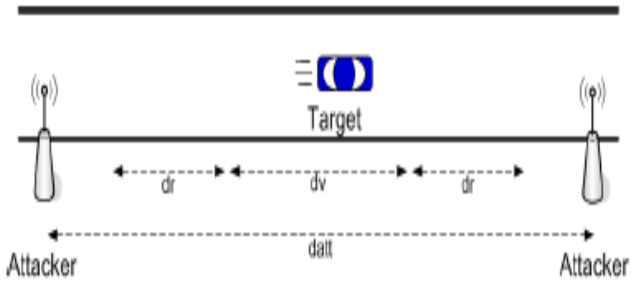
All cryptographic material of a car is compromised. To avoid overloading the network, the organization dedicated to the withdrawal sends a request for waiver to the receiving device of the vehicle. A particular vehicle key has been compromise. In this case sending a revocation for each key possessed by the vehicle would create a strong network overhead. In the literature [16] there are several options for the withdrawal but all have as a prerequisite a permanent connection to the control bodies. This condition is not satisfied in VANET. The use of certificates associated with keys of short duration, which at the expiration of the certificate the associated keys are cancelled. The system of certificates on the keys, however, requires a large storage capacity of data by vehicle; because the vehicles must replace their keys.

C. Analysis of the security provided by asymmetric authentication

It is need a verification of the data by the vehicles, to prevent network attacks from fogging techniques scenarios, false fog, and fake accidents and so on. This verification consists in comparing a node receives the data of neighboring nodes, in order to find a comparison of truthfulness. This technique is known as the "correlation of data" [17]. The study of the correlations of the data makes

Figure 5: The identity of the attacker nodes attached keys

the system much more stable to external attacks. In addition, the correlations combined with the use of certificates, greatly reduce the types of attacks that can deliver to vehicular networks. As shown in Figure 5, the anonymity of the vehicle is



vulnerable long distance. This means that even if the vehicle changes its key frequently in short distances, the attacker is able to correlate the keys of the vehicle with good probability of success along the distance.

D. Implementation issues for asymmetric authentication

The size of the keys anonymous should be small so as reduce the space required for storing them on vehicles. On the other hand, the duration of the certificate should be short, so minimize the window of vulnerability in the case of public / private key compromised.

E. Duration of the certificate

Each anonymous key should be used only in a consecutive sequence of messages and for a limited time. The attacker would be able to seize it and may extract information from this key at other valid times. A certificate should last about one day in order to limit possible damage from correlations. The duration of a certificate is also a function of the path traveled by the vehicles. The longer route will take longer duration of the certificate. The different durations of certificates arise from the need to try to reduce the number of keys circulating in the network. For example, if a vehicle did long trips, the use of certificates in the short term lead to a continuous flow of keys in the network and therefore more exposure to security risks. The number of these circulating keys would be reduced considerably, if the duration is a day or more. The opposite case, if a vehicle did short trips, a certificate to long-term exposes to security risks the vehicle. In fact, if the key had been intercepted and corrupted by an attacker, this could use it for the duration of its validity.

6.2 Symmetric Authentication

There are many proposals based on asymmetric authentication, the application of symmetric encryption to VANET is quite rare. One explanation for the low use of symmetric encryption is due to the low flexibility of its use. A study on symmetric encryption is discussed in [18]. Authors make use of fixed infrastructure that performs authentication and message store. As mentioned previously, even though the system of symmetric-key encryption is less flexible than asymmetrical, in many aspects, for messages small size, this system requires less computing power and is more resistant to attack by crypto analysis. These two features are very attractive to VANET. In VANET the exchange of messages between vehicles must be carried out in the shortest possible time, also one must try to reduce as much as possible the loss or duplication of packets. The symmetric encryption in this case brings a benefit to the system since the calculation operations for encryption of each

package are minimal. Other advantages of the solution with respect to that asymmetric symmetric encryption are:
There is no need to keep the current public key infrastructures (PKI) certification, which were reached at times with BS, something that is required for asymmetric authentication. No need to establish connection link between vehicle and CA .No need to establish connection link between vehicle and CRL (Certificate revocation list).

A. Network model with symmetric encryption

The authenticity problem in VANET can be solve in two different ways vehicle to vehicle and vehicle thought as Hybrid model and Opponent. Now we explain the characteristics of malicious nodes in detail. Hybrid Model consists of vehicle to vehicle and vehicle to infrastructure type VANET. It would be difficult to create a hybrid network with no infrastructure and no monitoring body as the mobility of vehicle is high that certificate various transmitter vehicle. We classify VANET in two types vehicle to vehicle and vehicle to infrastructure. We need a synchronize system between vehicle and Infrastructure. An attacker has the ability to listen to all messages in transmission in a communication channel, compromise a node, to launch attacks in the node. A node compromise is usually disabled or used as a communication bridge for other attacks. These systems are used in a variety of contexts such as e-marketing. The anonymous routing techniques that attempt to provide anonymity to the nodes. This model is used in a system of storage and verification from third parties of the real identities of the nodes and their associated aliases.

B. Digital Signature:

Digital signatures applied to end-to-end, hop-to-hop to protect the routing message from being tampered by malicious nodes, and assistant to backward evaluation mechanism. Another part of the evaluation mechanism is forward evaluation mechanism. It mainly used to detect the drop-malicious nodes. The main idea of the solution is that the problem which the cryptosystem can't deal with has been solved, such as drop packets to ruins the efficiency of the routing protocol.

VII. CONCLUSION

In this paper, we demonstrated the need for security in vehicular networks (VANETs), and why this problem requires a specific approach. When talking about the security aspect of VANETs we encounter some major problems that are discussed in this paper. The first problem would be that there is a privacy problem. Secondly, we discuss about authenticity which also take into consideration. The main purpose of a VANET which is the creation of efficient traffic condition for that we need a secure network. Road side units, trust components, privacy and many aspects have to be discussed in this papers in order to create a complete picture of this problem regarding VANETs. Attackers can become an important part in VANETs if the security aspect of these type of network is not analyzed correctly. The goal of this paper is to avoid the situations like in those in which the attacker becomes more important due to the information he sends to the other participants of the VANET. As the privacy protection in VANET is necessary to keep the confidentiality of the routing message and data and the routing scheme needs to adjust parameter to optimize the network performance.

REFERENCES

[1] G. Samara, *et al.*, "Security Analysis of Vehicular Ad Hoc Networks (VANET)," in *Second International Conference on Network Applications Protocols and Services (NETAPPS)*, 2010, pp. 55-60

[2] M. Burmester, *et al.*, "Strengthening Privacy Protection in VANETs," in *IEEE International Conference on Wireless and Mobile Computing Networking and Communications, WIMOB '08.*, 2008, pp. 508-513.

[3] Chim, TW, Yiu, SM, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," Ad Hoc Networks, Volume 9, Issue 2, March 2011, pp. 189-203.

[4] G. Samara, *et al.*, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," in *4th International Conference on New Trends in Information Science and Service Science (NISS)*, 2010, pp. 393-398.

[5] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A.Woodward, "A distance routing effect algorithm for mobility (DREAM)," in ACM MOBICOM '98. ACM, press. 1998, pp. 76 – 84.

[6] A. Tajeddine, *et al.*, "A Privacy-Preserving Trust Model for VANETs," in *IEEE 10th International Conference on Computer and Information Technology (CIT),*, 2010, pp. 832-837.

[7] B. K. Chaurasia, *et al.*, "Attacks on Anonymity in VANET," in *International Conference on Computational Intelligence and Communication Networks (CICN)*, 2011, pp. 217-221.

[8] S. Behera, *et al.*, "A secure and efficient message authentication protocol for vehicular Ad hoc Networks with privacy preservation(MAPWPP)," in *IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application (IMSAA)*, 2011, pp. 1-6.

[9] D. Balfanz, D. K. Smetters, "Authentication in Ad Hoc Wireless Networks". In the Proceedings of the network and distributed system security symposium (NDSS), 2002.

[10] P. Golle, D. Greene, "Detecting and Correcting Malicious Data in VANETs". In Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks, pp. 29-37, 2004.

[11] N. Sastry, U. Shankar and D. Wagner. "Secure Verification of Location Claims". In ACM Workshop on Wireless Security. WiSe 2003.

[12] M.S. Corson, S. Batsell and J. Macker, "Architectural considerations for mobile mesh networking" (May 1996) Request for comments draft; http://tonnant.itd.nrl.navy.mil/mmnet/mmnetRFC.txt.

[13] A. Wasef, *et al.*, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Communications*, vol. 17, pp. 22-28, 2010.

[14] A. Benslimane "Optimized Dissemination of Alarm Messages in Vehicular Ad-hoc Networks (VANET)" Published by Springer Berlin / Heidelberg. ISSN: 0302-9743. Volume 3079 / 2004. Chapter: pp. 655 – 666. France, June 30 - July 2, 2004. Laboratoire d'Informatique d'Avignon LIA France.

[15] R. Das Samir, R. Castañeda and J. Yan, "Simulation Based Performance Evaluations of Mobile, Ad hoc Network Routing Protocols", division of computer science The University of Texas San Antonio.

[16] H. Fußler M. Mauve H. Hartenstein "A Comparison of Routing Strategies in Vehicular Ad-Hoc Networks". Kasemann March 2002

[17] G. PEI , M. GERLA, and X. HONG, "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility", IEEE/ACM MOBIHOC 2000, Boston, MA, pp. 11-18. August 2000.

[18] B. Karp and H.T. Kung, "GPSR : Greedy Perimeter Stateless Routing for Wireless Networks", MOBICOM'00, Boston, MA, USA, pp. 43-54, 2000.

Mostofa Kamal Nasir is serving in the Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University (www.mbstu.ac.bd), Santosh, Tangail-1902, Bangladesh.
E-mail: kamal.mostofa@gmail.com

A.K.M Kamrul Islam is serving in the Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University (www.mbstu.ac.bd), Santosh, Tangail-1902, Bangladesh
E-mail: kamrul3000@gmail.com

Mohammad Touhidur Rahman is serving in the Daffodil Institute of Information Technology (DIIT), Dhaka, Bangladesh
E-mail: rahmantm@gmail.com
and
Mohammad Khaled Sohel is serving at Daffodil International University (DIU), 102 Shukrabad, Dhaka, Bangladesh . E-mail: ksohel@gmail.com