Two Tier Clustering Technique in Vehicular Ad Hoc Networks in Highways' Scenarios

Zainab Nayyar[1], Muazzam A. Khan[1], Faisal Bashir[2], Cory Beard[3], Zhu Li[3], Khurram Mahmood[4]

NUST College of EME, National University of Sciences and Technology (NUST), Islamabad, Pakistan[1]
Department of Computer Sciences, Bahria University, Islamabad[2].
School of Computing & EE, University of Missouri, Kansas City, USA[4].
Ministry of Information Technology, Islamabad, Pakistan[3]

Abstract: Vehicular ad hoc network is a very innovative approach for information traffic system derived from mobile ad hoc networks in which vehicles communicate with each other in different circumstances and for different purposes like to aware other vehicles from any accidental situation, to share media files etc. VANETs have many applications for example they inform other vehicles about obstacles coming in their way through satellites, they clustered with other vehicles wirelessly and move like road trains and they inform drivers to apply brakes even if they are obscured by other vehicles. Clustering and security issues are mostly focused in vehicular ad hoc networks but they still requires more improvement. Previous studies have revealed that security and confidentiality is achieved through public key infrastructures, certification authorities and many other algorithms but somehow or the other reliability and availability aspects are affected. Some algorithms increase the delays and overheads, some increase the jitter, and some decrease the performance and throughput. To address these issues Two Tier Clustering algorithm has been used due to which stable cluster heads will form, delays in election procedures will occur and the network will be more secure and efficient.

Keywords: two tier clustering, vehicular ad hoc networks, highways, security.

1. Introduction

With The growth of wireless communication technology, two elementary wireless network models have been established for the wireless communication system [1] [2]. The fixed infrastructure wireless model consists of a large number of Mobile Nodes and relatively fewer, but more powerful, fixed nodes. The communication between a fixed node and a MN within its range occurs via the wireless medium. However, this requires a fixed infrastructure. Ad hoc networks are the new paradigm of wireless communication in mobile nodes. There are no fixed base stations or infrastructures; nodes which lie in the range of each other can easily communicate, while those which are far apart from each

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

other communicate over the routers. Their deploying cost is relatively low as compared to other wireless networks because there is no necessity of a proper fixed infrastructure [4] [5]. Mobile and vehicular network technologies belong to ad hoc networks. The reason for deploying vehicular ad hoc networks is that over the years many motor accidents were observed leading to critical injuries, fatalities, and excessive cost on vehicle repairs. Since a proper solution was not efficiently worked out, therefore just like Mobile Ad Hoc Networks (MANETS); Vehicular Ad Hoc Networks (VANETS) were introduced in the cars for the sake of additional safety and comfort for vehicle drivers [2]. The concept of VANET is based totally on performing real world tasks by turning every participating car into a wireless router or node, so it can be stated that it is a kind of real time system [3]. There are several issues which are also highlighted while emergence in vehicular ad hoc networks. These are availability, confidentiality, integrity, authentication and non-repudiation. [4][6]. There are two main types of communications in VANETs: Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) [7].

Road safety and collision avoidance is very necessary for avoiding accidents. For this purpose *vehicle to vehicle* protocol is necessary to be applied on the vehicles for proper communication.

Let's take a look at the following example of car A, B, C which are moving on the road as illustrated in Figure 1. Suddenly car A is caught in a critical situation and applies brakes; now by viewing the brake lights of A, car B will also intuitively apply the brakes. In this scenario, car C is unaware of the emergency that has occurred to A, and will reacts according to the actions performed by car B. This situation may sometimes lead to an accident. A delay of 0.7 to 1.5 seconds occur which causes the cars to collide with each other because C may not view what is happening to A and B.

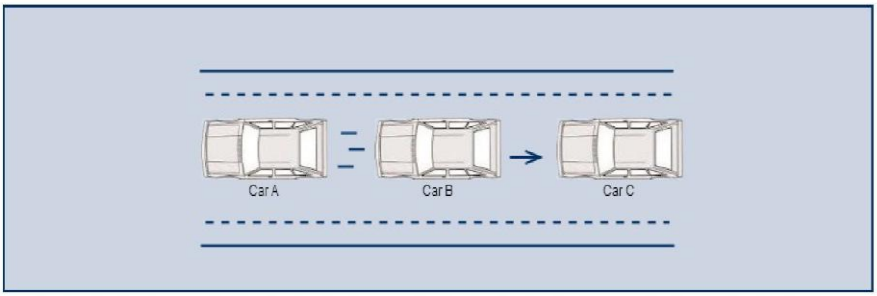


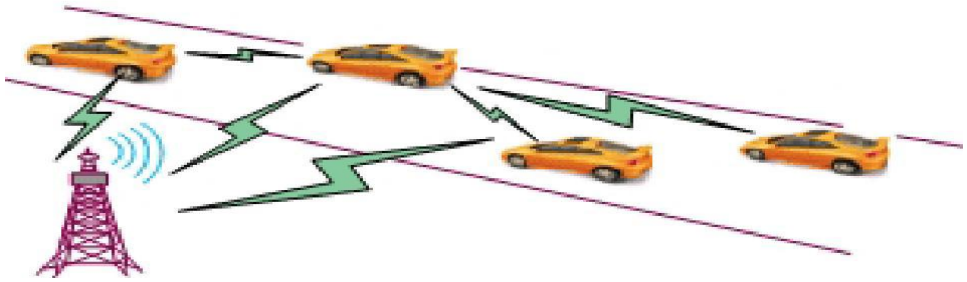
Figure 1. V2V Communication

To avoid an accident, V2V communication is used where when car A will be in a critical condition it will generate a message which will be sent to B, and car B will send a message to car C. The V2V signal will cause the drivers to alter their paths and at least avoid accidents, as shown in figure 1 [9]. All this is done by using radio technology; the

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

standards which are developed for V2V communication are based on CSMA/CD for collision avoidance [10].

The role of V2I includes the provisioning of safety related, real time, local and situation based services such as speed limit information, safe distance and warning, lane



keeping support, intersection safety, traffic jam warning and accident warning. All accidents are aimed to be saved by providing timely information related to the safety of cars and drivers [11]. As shown in figure 2.

Figure 2. Vehicle to Infrastructure Communication

The research work focuses on to check the malicious messages that can be sent by the authorized nodes for any mischievous purpose. To save time of the cluster head algorithm and balance a network load. Carry out detail analysis of the proposed scheme. Compare performance of the proposed approach with the other researcher's work in securing clusters in VANETs.

Sections of this thesis have been organized into following units. Section 2 provides detailed study and concepts of various secure clustering techniques in VANETs. Section 3 illustrates the methodology description and architecture of proposed system has been discussed in detail. In section 4 simulation topology and analysis of results that have been produced to validate the proposed system. Conclusion has been described in section 5. References are mentioned in section 6.

2. Literature Review

2.1. Clustering Techniques in Vehicular Ad hoc Networks

2.1.1. The Lowest ID Algorithm

In this algorithm [35] each node was assigned a unique ID number. The node with the lowest ID in its 2 hop neighborhood was elected to be a cluster head.

2.1.2. MOBIC Clustering Algorithm

In MOBIC [36] instead of forming a cluster on the basis of its node IDs, aggregate local mobility matrix was used. The node with a smallest variance of its relative mobility to its neighbors was elected as a cluster head. The relative mobility of nodes was

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

calculated by comparing the power of two consecutive messages of neighboring node. Election of a cluster head reoccurred only when two cluster heads came in range of each other. When any cluster member moved out of its cluster then it would join another cluster that would came in its range or formed a new cluster head.

2.1.3. Affinity Propagation

In [37] nodes passes messages to one another, which described the current state that each node chose another node as its exemplar. In this method the clustering process completed when message converged. This algorithm could determine a status of a node when it joined cluster head in a certain cluster.

2.1.4. APROVE:

In [38] each node sent the availability and responsibility messages to other nodes, and then independently made a clustering decision. Every node would made a cluster with every other node which would one hop from each other. Negative Euclidean distance was used to calculate the distance and position of the nodes.

2.1.5. Time Division Multiple Access (TDMA)

TDMA [39] is a channel access system where the accessible transmission capacity is opened into time divisions and each division is utilized just by a solitary sender, along these lines maintaining a strategic distance from bundle crashes. The Service Channel and Control Channel are partitioned into k equivalent estimated time spaces for exchanging control and status messages. Every vehicle is allotted a nearby id and are said to be adjusted. The fundamental thought is that in each virtual frame a vehicle listens to its given time slot for status and control messages also, sets the relating byte in. The quantity of vehicles (N) may change alterably and the Cluster Head will update the other nodes in the cluster that the new nodes are added in to the cluster.

2.1.6. Node Precedence Algorithm

In [40] a node priority calculation is proposed and adaptively recognize the 1-hop neighbors and chooses ideal CHs in light of relative node portability measurements, for example, velocity, location and direction of travel. It additionally presents the zone of interest idea that mirrors the continuous changes on the system and gives former information about the neighbors as they go into new neighborhood areas.

2.1.7. Hierarchal Clustering Algorithm

In [41] a Hierarchical Clustering Algorithm (HCA) is presented that makes a quick randomized progressive cluster with a diameter of at most four hops, without the

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

utilization of GPS. The calculation is considered profoundly strong, on the grounds that it doesn't depend on confinement frameworks like GPS, yet by inducing network from sent messages.

2.1.8. Lane based Clustering

The lane based clustering [42] consider the bearing of activity on street as one of the parameters for figuring efficient and nearly stable clusters in VANET. The upsides of a steady clustering are that it lessens the overhead of re clustering which brings about a productive system topology. Cluster head changes and cluster reconfigurations can't be maintained a strategic distance from in shifting systems like VANET. This affects the solidness of the system. For more steady clusters in the system there should be less cluster head changes. To accomplish less number of cluster head changes, cluster individuals ought to choose a node among the cluster individuals which can meet every one of the prerequisites of being a cluster head for a generally drawn out stretch of time than rest of them. The cluster head is chosen relying upon the path having the greatest movement stream. Vehicles have the learning of the path of movement on street and they telecast this data to the adjacent vehicles. This aides in deciding the efficient cluster head. All vehicles in the system figure and show their Cluster Head Level (CHL), pace, position, and so on. CHL is computed utilizing path weight, normal separation level, system network level and normal speed level of the activity. Utilizing the occasional reference points, a vehicle telecasts the computed CHL and the general activity information in the system. At that point the vehicle holding the most elevated CHL worth is chosen as the Cluster head. This procedure of cluster arrangement is rehashed for each 20 seconds.

2.1.9. ASPIRE

ASPIRE [42] is a technique proposed for vehicular ad hoc networks where clustering is done in a dispersed way. This plan helps in making substantial clusters furthermore giving high system integration. The technique brings down cluster head terms and expands the quantity of cluster head changes. It diminishes the framework costs in the system by utilizing simple vehicles on streets. Yearn structural planning comprises of vehicles that shape clusters with generally lower portability. In these clusters couple of nodes go about as Cluster Members (CM) while the other go about as Cluster Heads (CH). Each group has a solitary cluster head. These clusters thus frame Mobile Networks (NEMOs), each with a Mobile Router. Aim gives reserving possibilities between clusters shaped by vehicles and NEMOs, lessening the overhead and expense of getting to the altered administration supplier system for every vehicle demand or tying upgrade because of a topology change.

2.1.10. Node Velocity based Hierarchical Clustering of Nodes technique (NVHCN)

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

In [43] the cluster development is constrained to vehicles subject to the lease relative portability such that the term of network offered by the vehicles to different vehicles is longer. The recognizable proof of vehicles or clusters by different vehicles is done utilizing the TV of message containing self-data. Self-data of every vehicle includes node id, cluster id, cluster portability range, scope separation, and speed. In any cluster, notwithstanding which versatility range it has a place with, a cluster head in any group is chosen taking into account CHcrit. It is done in one of the nodes in the group which is termed as Pseudo CH. CHcrit choice is made by keeping up distinctive stacks for getting node need for every like mean speed, most extreme accessibility span and greatest nodes under scope. In the Pseudo CH, the voting in favor of CH is led between all nodes in the cluster. In this manner through voting a node which offers long length of time of integration for a large portion of the nodes in the cluster C is chosen as CH.

Alongside CH determination, a CH Time Out is situated which empowers directing re-decision toward the end of most extreme span of integration which could be offered by the then CH. This idea of framing a cluster in view of minimum relative portability is appropriate in highway street situations also, different less thick street ways where the speed of every vehicle is by all accounts fluctuating occasionally.

2.1.11. 2-layer stable clustering scheme

[44] Is dependent on multiple metric that combine features of both static and dynamic clusters. The cluster head is selected from the vehicles of the same group based on that matric named as suitability value. It is obtained from relative speed, mobility and time to leave the cluster from mobility metrics. Quality of Service metrics included available bandwidth, neighborhood degree and RSU link quality. Due to these parameters cluster stability and high quality of service achieved.

3. Methodology

In VANETs clustering is done among the vehicles to make inter and intra-vehicular communication better and to avoid accidents. In this scenario ignoring security parameters during clustering of vehicles can lead to loss of valuable information about the adaptation to send data securely among the vehicles. The number of received packets contain useful information about different vehicles. Detailed study of secure clustering in VANETs has revealed that applying security on data transmission and carrying out election procedure for a new cluster head faces many problems.

3.1. Malicious Messages Send by Valid Nodes

Consider a clustered network of VANETs in which 4 nodes are a part of cluster. All nodes are validated by certification authority and thus are communicating with in the network as shown in figure 3.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

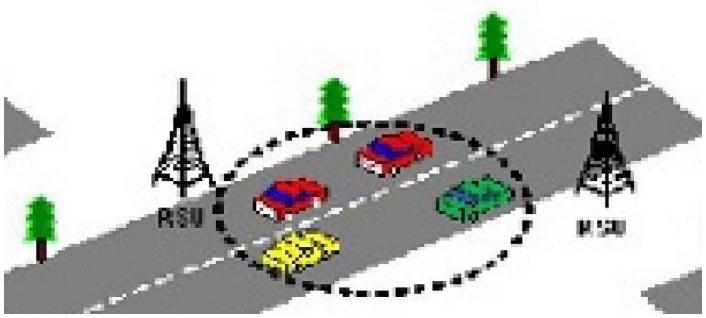


Figure 3.Nodes in a Cluster Communicating with each other

All of a sudden one node will send a malicious message to the remaining nodes in a cluster that will cause collision among the vehicles. As shown in figure 4.

Figure 4.Accident Caused by the Message send by Malicious Node to the other nodes

3.2. Delays and Overheads during Cluster Head Election Algorithm

In VANETs clusters most of the time Cluster Head election process take place repetitively which causes delays and overheads in clusters and the communication process among the nodes fail. Unstable clusters cause a lot of issues in vehicular ad hoc networks.

3.3. Proposed Algorithm

To solve the above mentioned issues a technique named *two tier clustering in vehicular ad hoc networks* has been proposed in which the load balancing phenomena is introduced for clustering of nodes and also for the election process. There is a Primary Cluster Head and a Secondary Cluster Head as well. Clustering will be done on the basis of the average speeds, locations, directions and IDs of nodes.

Figure 5 shows the architectural view of the system. Ubuntu 12.04 is used as an operating system. For simulation and implementation purpose Network Simulator 2.35 is used. There will be a Certification Authority and a Demilitarized Zone which will validate and assign rights to the nodes.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

After this all the validated nodes will be clustered according to the specified parameters. Election process will be carried out after grouping of nodes after which Primary and Secondary Cluster heads will be decided.

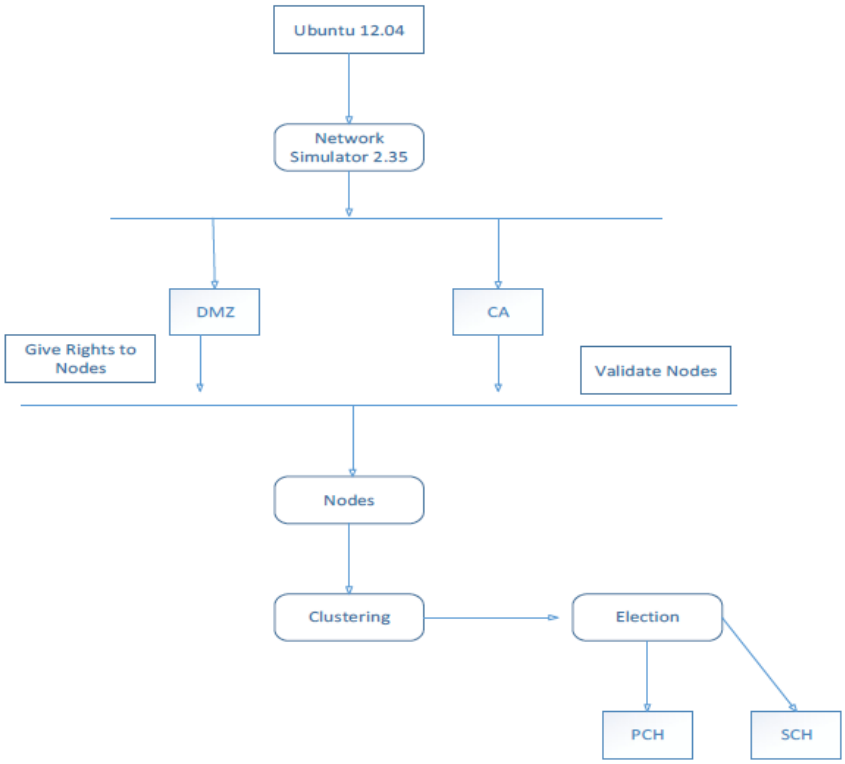


Figure 5.Architectural Diagram of Proposed Algorithm.

In the proposed technique instead of one hop clustering multihop clustering is done to reduce the number of clusters. The criteria of clustering is depending upon the specified speed ranges such as:

- Range 1: 100-80 kmph
- Range 2: 79-60 kmph
- Range 3: 59-40 kmph

In first cluster all the vehicles having speeds between 100-80 kmph will lie. In second cluster the vehicles having speeds between 79 – 60 kmph will grouped together. In third the vehicles having 59 – 40 kmph will clustered together. The vehicles whose speeds are greater than 100 kmph will lie in the cluster of 100 – 80 kmph. While those which are below 40 kmph will lie in the cluster of 59 – 40 kmph.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

In cluster creation process there are two main functions. Certificate Authority (CA) and Demilitarized Zone (DMZ). Each entity will perform number of functions. When nodes will enter on the highway and request for validation. CA will assign IDs to the nodes and maintain a table which will consists of node ID, speed of the node and location of the node. After that Cluster will be created on the basis of pre-defined speed ranges and each node will become the member of respective cluster. Each cluster will be represented with its ID which will be maintained by DMZ. As shown in figure 6.

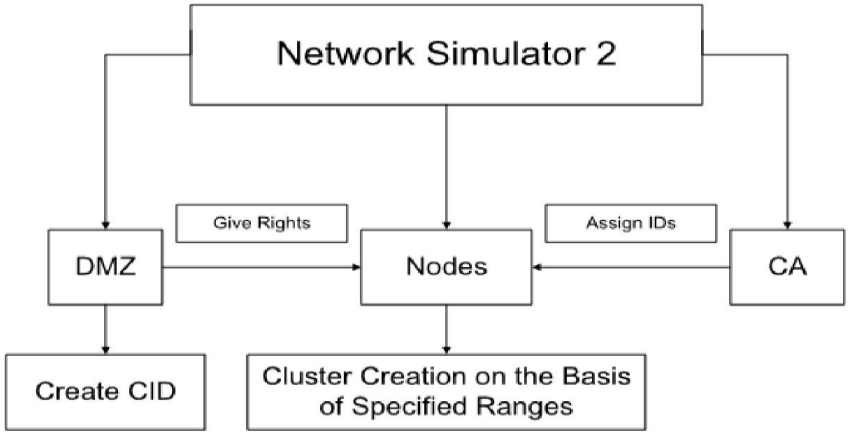


Figure 6.Cluster Creation

After cluster creation the main phase is to initiate the election process for the selection of Primary Cluster Head and Secondary Cluster Head for the management of the cluster nodes. This process will initiate by the DMZ and check whether any PCH and SCH exists. If they will found one of them the election process will terminate and move to the next process otherwise will continue with its current process as shown in figure 7. Due to the presence of secondary cluster head the delays in the election process will occur and the cluster will work stably. If Primary Cluster Head will leave the cluster the secondary cluster head will become the primary cluster head and the next node which has speed nearest to average speed will become a Secondary Cluster Head. If multiple vehicles have the same speeds than the node with the lowest ID becomes the cluster head. The average speeds for the cluster formation will be calculated by DMZ by taking the minimum and maximum speed and maximum speed from the each cluster speed range. The following formula will be used to calculate the average speed of the cluster:

$$\textbf{Avg-Spd} = (\textbf{min}_{\textbf{spd}} + \textbf{max}_{\textbf{spd}})/2$$

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

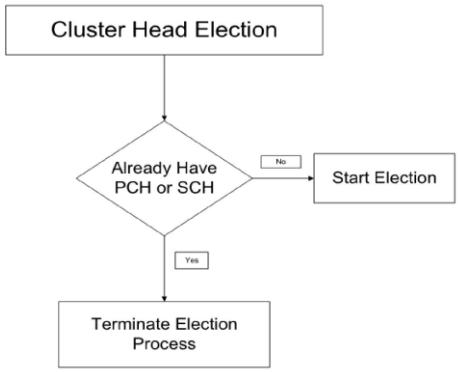


Figure 7.Election Process

For the selection of PCH and SCH, election process DMZ will find the total number of cars in the cluster and find out the average speed of the cluster according to the formula mentioned above and the node which will have the speed equal or close to the average speed will become the PCH and the next closest node with the smallest ID than the node selected as PCH will become the SCH. If two or more cars will have the same speed closest to the average speed then, in this case node with the smallest ID will become the PCH and second next will become the SCH. As shown in figure 8.

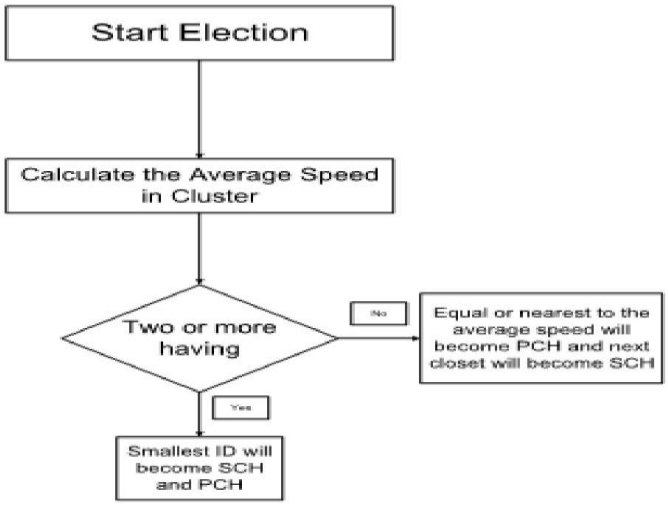


Figure 8.Primary & Secondary Cluster Head Selection Process

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

In each cluster PCH and SCH will necessarily exists. If PCH will leave the cluster or declared dead node the SCH will take over the responsibilities and will become PCH and next one will become SCH. The same process will continues without initiation of election process again and again. As shown in figure 9.

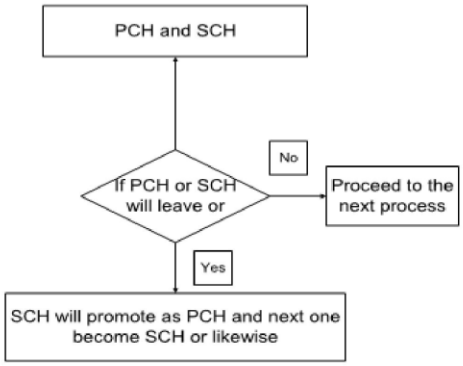


Figure 9.Upgrading SCH to PCH

Now the probability of a node to become a cluster head is calculated by calculating the node position '$\mathbf{n_{pos}}$'. $\mathbf{n_{pos}}$ is determined by adding node location '$\mathbf{n_{loc}}$', node direction '$\mathbf{n_{dir}}$', speed '**v**' and '**id**' of a node.

$$\mathbf{n_{pos} = n_{loc} + n_{dir} + v + id}$$

For Cluster Head Selection:

$$\mathbf{PCH = (ni_{pos} - p_{mean}) / avg\text{-}spd}$$

Whereas 'p_{mean}' is the mean position of the node.

DMZ will assign rights to the nodes in the cluster and only PCH will be allowed to do two way communication rest of the nodes only send data to the PCH. PCH will maintain the table which will have Node ID, Node Speed, Location and its Status. PCH will replicate the entire table with SCH for future. Each node will send three consecutive hello packets in 10 ms to the PCH to show that the node is alive as shown in figure 10.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

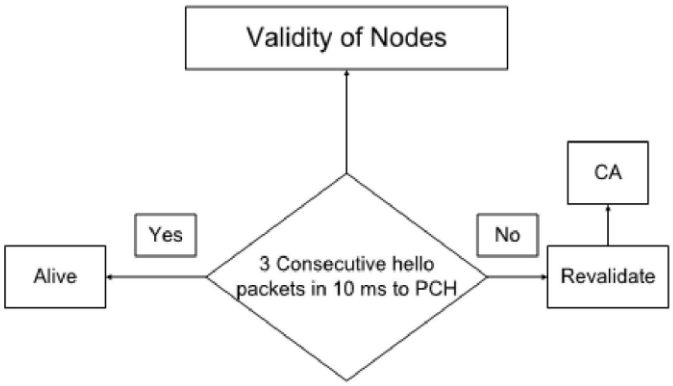


Figure 10.Validity of Nodes

In some circumstances when the respective node will not send hello packets to the PCH due to any reason PCH will re-validate that node. The dead interval will be 20 ms, if the node will not send hello packets to the PCH within specified time then PCH will declare the node dead and intimate to the CA that the ID is free as shown in figure 11.

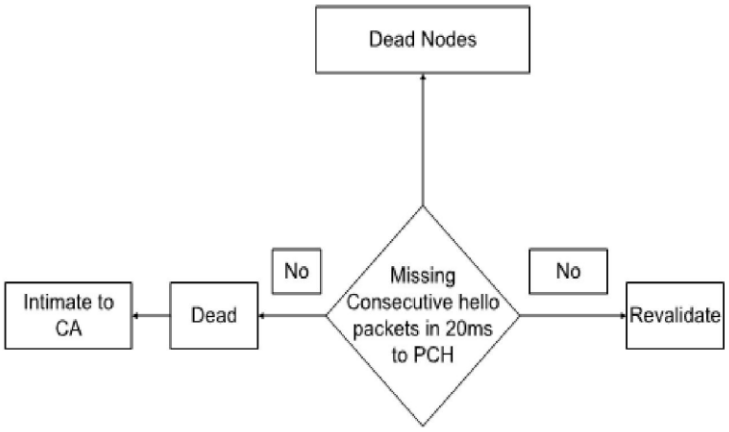


Figure 11.Dead Nodes

3.4. Security Mechanism

3.5. Diffie Hellman Key Exchange Algorithm

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

The security algorithm used is Diffie Hellman Key Exchange [23] [24] in which two users exchange a key over the network channel. The key is then used by both parties for data encryption and decryption. No authentication server is required for key exchange. Assume there are two publicly known numbers: a prime number q and an integer α, which is a primitive root of q. User A selects a random integer XA < q and computes YA = α XA mod q. Similarly, user B independently selects a random integer XB < q and computes YB = α XB mod q. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as K = (YB) XA mod q and user B computer the key as K=(YA) XB mod q. These two calculations produce identical results:

$$\mathbf{K = (YB)\ XA \bmod q}$$
$$\mathbf{= (\alpha\ XB \bmod q)\ XA \bmod q}$$
$$\mathbf{= (\alpha\ XB)\ XA \bmod q}$$
$$\mathbf{= (\alpha\ XA)\ XB \bmod q}$$
$$\mathbf{= (\alpha\ XA \bmod q)\ XB \bmod q}$$
$$\mathbf{= (YA)\ XB \bmod q}$$

And hence the keys are exchanged between the two parties. Every time the parties will select a new integer and for protection they exchange a new key every time. The Diffie Hellman Key Exchange Process is shown in figure 12:

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

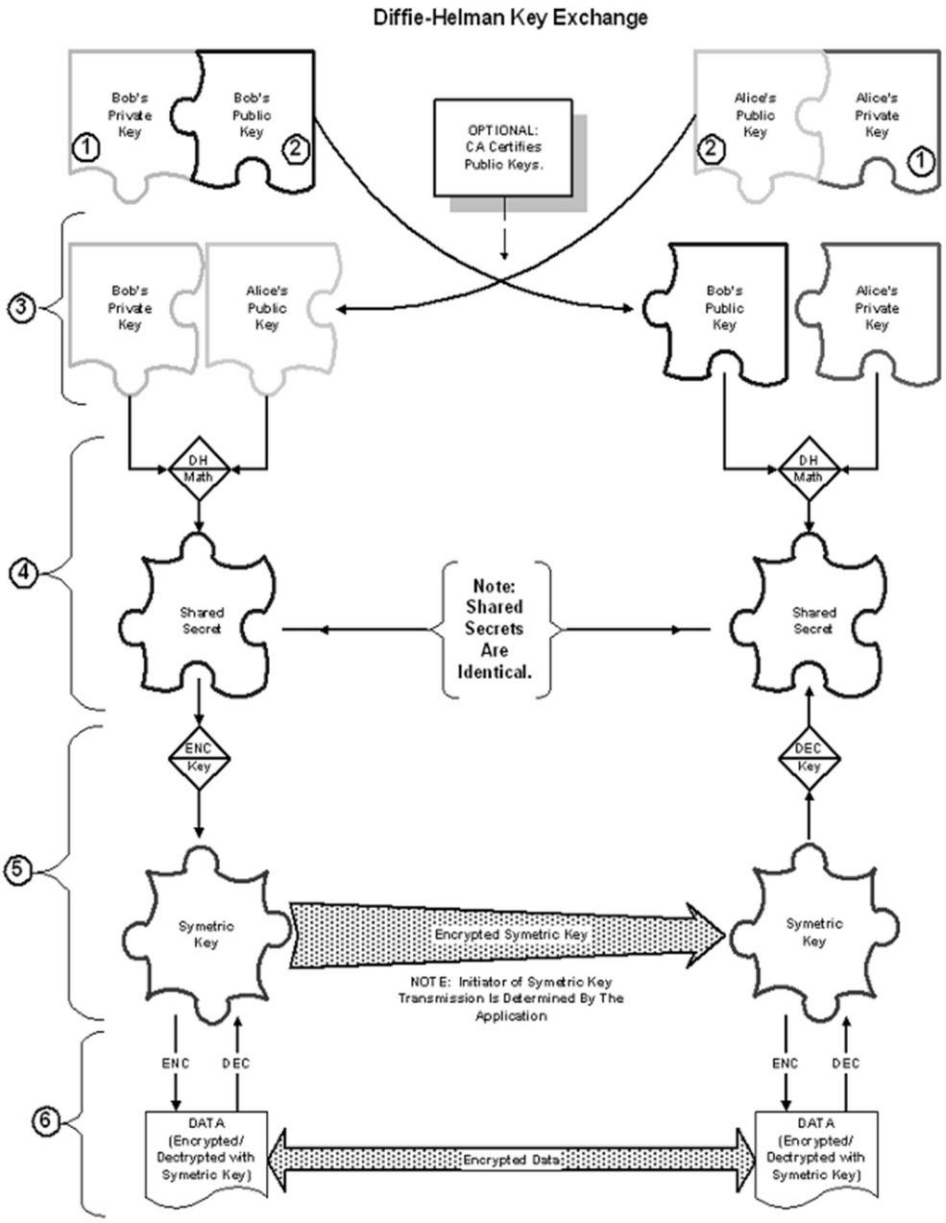


Figure 12.Diffie Hellman Key Exchange Process

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

4.0 Results

The proposed scheme has been implemented using the Network Simulator (NS-2), using Linux (Ubuntu 12.04) environment. Clustering technique has been used to simulate the proposed scheme. The CBR traffic has been generated to test the performance of the proposed Algorithm. The simulation has been run for 2.7 hours and nodes are moved away and then moved nearer to each other. Table 1 shows the Simulation Configuration.

Table 1.Simulation Configuration

Mobility model	Manhattan
Propagation	TwoRayGround
Antenna	Omni Antenna
Number of Nodes	15, 50, 100
Routing Protocol	AODV
Channel Type	Wireless Channel
Topology in Meters X & Y	900
MAC Type	MAC / 802.11
Simulation Time	2.7 Hours

Manhattan mobility model is used for creating mobility among the nodes in highway scenario. Omni Antenna is used for transmitting and receiving signals. Number of nodes in the simulation is 15, 50 and 100. AODV routing protocol is used for routing data packets. Nodes are functioning over the wireless channel network. Maximum 900 meters topology area is considered for the movement of nodes. 802.11 MAC type is used. Total simulation time is 2.7 hours.

Performance of two tier clustering algorithm has been observed with the help of simulation results. The results describe the enhanced throughput and stability of data rates. For all data rates, CBR rates have been decided, that provide the maximum throughput. Simulations have been performed to evaluate the multiple scenarios.

4.1 Availability

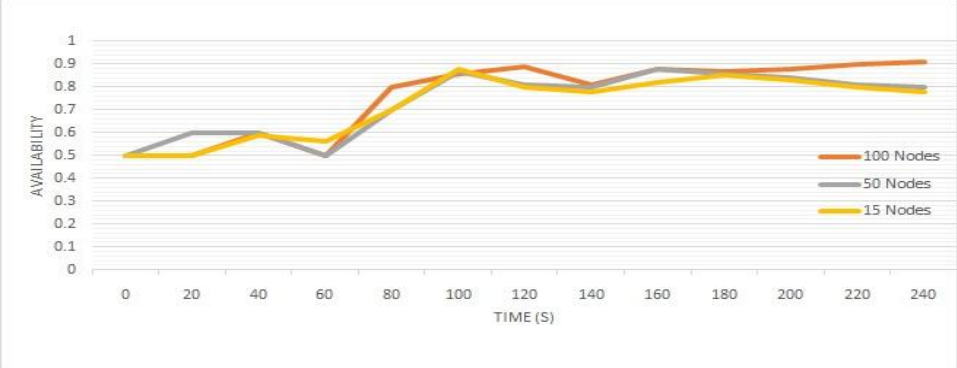
Availability means that the system's resources are available over a period of a year even if some failures or crashes occur with the system. Availability has been calculated by the formula in which mean time to failure is divided by mean time to failure plus mean time to restore the system.

$$\mathbf{A = MTTF / (MTTF + MTTR)}$$

The availability of a system is checked against 15, 50 and 100 number of nodes. When the node count was 15 at 0 seconds the availability was 0.5 and increased till 0.8

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

when the time was 240s. When the node count was 50 at 0 seconds availability was 0.5 and keep on increasing till 0.8 when time was 240s. When the node count was 100 at 0 seconds availability was 0.5 and keep increasing till 0.9 when time was 240 seconds. It means that the increase in node count and time does not affect the system availability

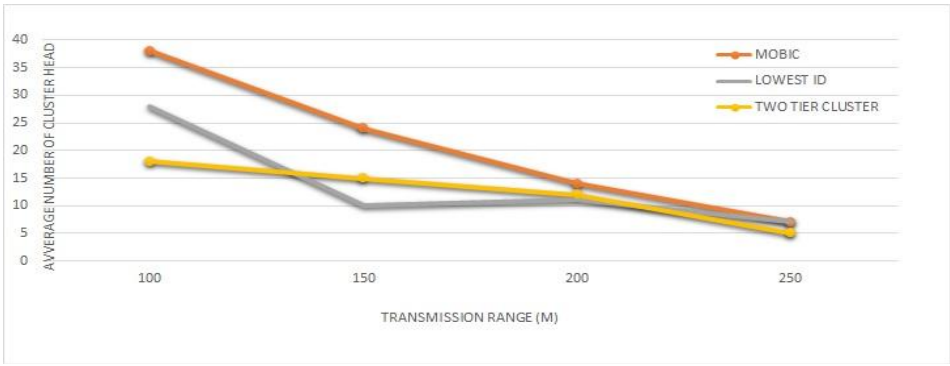


factor. As shown in graph mentioned 13.

Figure 13. Availability Graph

4.2 Cluster Head Stability

The cluster head stability factor was compared with MOBIC and Lowest ID clustering technique. The transmission range was 250 meters and it was observed that in Lowest ID the cluster head number was fluctuating, when the transmission range was 100 meters was 25 and decreased to 5 when the transmission range was 150m. When transmission range was 250 meters the cluster head level decreased to 2. In MOBIC technique when transmission range was 100m there were 40 and gradually decreased to 5 when reached at range of 250m. Whereas in the two tier clustering technique the cluster head count was remain constant between 10 to 15 cluster heads. Figure 14 is depicting the results.



https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure 14. Cluster head Number Graph

4.3 Malicious Nodes

The malicious nodes detection rate of two tier clustering technique is also compared with the MOBIC and Lowest ID techniques. In Lowest ID technique when the malicious nodes were 10% the system success rate was 80% but when the malicious nodes were 80% the system success rate was 10%. In MOBIC when malicious nodes were 10% the system success rate was 60% but when the malicious nodes were 80% the system success rate was approximately 0%. In the proposed technique when malicious nodes were 10 % the system success rate was 90% and when the malicious nodes were 80% the system success rate was 20%. Hence it is observed that two tier clustering technique is more robust to the malicious conditions. The figure 15 is showing the results.

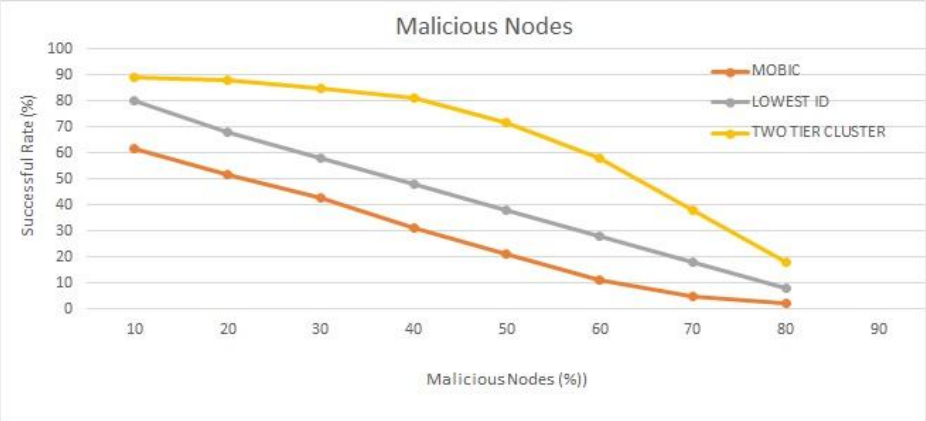


Figure 15. Malicious Nodes

4.4 Overhead

Overhead is a sum of indirect and excessive processing time, memory, and bandwidth. In the proposed technique the overhead is analyzed by varying the number of nodes. When the node count was 15 overhead was 2. When the node count was 20 overhead increased to 7 and when the nodes were 50 the overhead was 4 after that the overhead rate remains constant and between 60 to 80 number of nodes the overhead was 8 and when the nodes were 100 overhead was 9 as mentioned in the figure 16.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

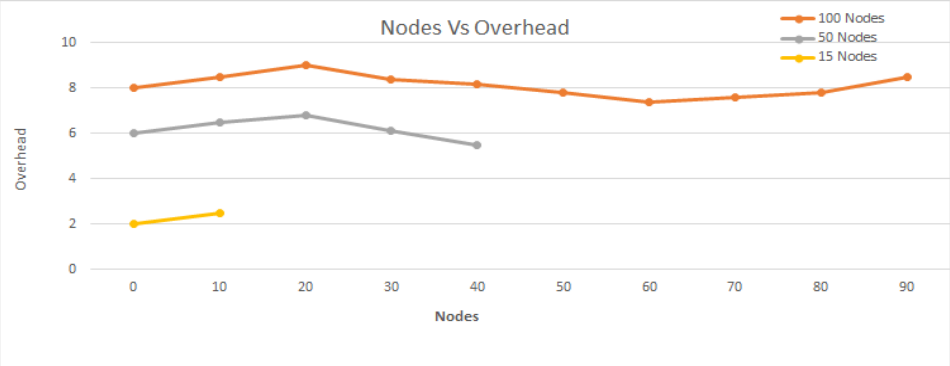


Figure 16. Overhead

4.5 Speed Vs Delay

The speed vs delay is observed against 15, 50 and 100 nodes. It has observed that with the increasing speed delay is also increasing but with the increasing number of nodes the impact of delay is constant and not increasing. When the number of nodes were 15, with in the range of 0 to 40 m/s the delay of 4 seconds is observed. When speed range was between 40 to 60m/s the delay was between 4 to 6 seconds. When the speed range was above 60m/s the delay of 8 seconds was observed. The same rate has been observed in 50 and 100 number of nodes. As shown in figure 17

Figure 17. Speed Vs Delay

4.6 Throughput

Throughput is the rate in which something has been processed. Throughput is calculated by the ratio of packet size and round trip time multiply by packet loss. Let ‘R’

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

is the average throughput, 'MSS' is the packet size, 'RTT' is the round trip time and 'p' is the packet loss then the throughput will be calculated as.

$$R = MSS/RTT * 1.2/p^{0.5}$$

The throughput of the system is calculated with MOBIC and lowest ID. In MOBIC and lowest ID the throughput is continuously increasing whereas in two tier the throughput is only increased when the system is performing some process otherwise the bandwidth is not consumed by the system as shown in figure 18.

Figure 18. Throughput

5.0 Conclusion

The main objective of this research was to design and implement an efficient methodology that provided efficient and stable clusters in VANETs. This stability in cluster formation lead towards the most appropriate communication among nodes, which gave the higher throughput. Goal was to analyze the correct clustering, election and security mechanism for appropriate communication that could provide increased availability and throughput. The main task of this research was to implement a secure and stable clustering and election algorithm that provided precise assessment of malicious and trusty nodes in the network and within the cluster, which was best suited to increase the security, availability and throughput. For the estimation about the node status, to maintain the consistency of the node, 3 consecutive packets would decide either the node was alive or dead. To make the stable clusters, multi hop communication among the nodes was done. With the help of consecutive packets, state of wireless nodes could be estimated and then suitable node according to that status had been selected. Appropriate action would be taken by certification authority on the intimation of cluster heads for the dead nodes. To avoid the initiation of the election process again and again a new entity called Secondary Cluster Head was introduced in the methodology. The secondary head would take over the responsibilities of cluster head in case of cluster head would be declared as dead. The system had been implemented using Linux (Ubuntu 12.04) environment with the network simulator NS-2.35. The clustering and election processes were implemented along with security mechanisms in NS-2. Trace files were analyzed using AWK scripts. The

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

performance of the proposed system had been analyzed through the simulations. Detailed study of results indicated a remarkable increase in the overall throughput of the system.

6.0 References

[1]. Christian Lochert, Hannes Hartenstein, Jing Tian, Holger Füßler, Dagmar Hermann and Martin Mauve. A Routing Strategy for Vehicular Ad Hoc Networks in City Environments Traffic Assistance Systems. Intelligent Vehicles Symposium. Proceedings. IEEE, pages 156 – 161, 2003.
[2]. Syed R. Rizvi, Stephan Olariu, Cristina M. Pinotti, Shaharuddin Salleh, Mona E. Rizvi and Zainab Zaidi. Vehicular Ad Hoc Networks. International Journal of Vehicular Technology, Volume 2011, 2 pages, 2011.
[3]. Maxiam Raya and Jean Pierre Hubaux. Securing Vehicular Ad hoc Networks. Journal of Computer Security - Special Issue on Security of Ad-hoc and Sensor Networks, Volume 15, pages 39-68, 2007.
[4]. Lidong Zhou, Zygmunt J. Haas and Cornell. Securing Ad Hoc Networks. Network, IEEE, Volume 13, pages 24 – 30, 1999.
[5]. Christian Bettstetter, Hannes Hartenstein, Martin Mauve. Ad Hoc Networking. Tutorial ,Ad Hoc Networking, 2003.
[6]. Drs. Baruch Awerbuch and Amitabh Mishra. Introduction to Ad hoc Networks. CS-647: Advanced Topics in Wireless Networks, 2008.
[7].Mohamed Elhoucine Elhdhili, Lamia Ben Azzouz and Farouk Kamoun. A Totally Distributed Cluster Based Key Management Model for Ad hoc Networks.
[8]. Rajaram Ayyasamy and Palaniswami Subramani. An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks. The International Arab Journal of Information Technology, Volume 9, pages 291-298, 2012.
[9]. Xue Yang, Jie Liu, Feng Zhao and Nitin H. Vaidya. A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning. Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference, pages 114 – 123, 2004.
[10]. Marc Torrent-Moreno, Jens Mittag, Paolo Santi, and Hannes Hartenstein. Vehicle-to-Vehicle Communication: Fair Transmit Power Control. Vehicular Technology, IEEE Transactions, Volume: 58, pages 3684 – 3703, 2009.
[11]. Pavle Belanovi´c, Danilo Valerio, Alexander Paier, Thomas Zemen, Fabio Ricciato and Christoph Mecklenbr¨auker. On Wireless Links for Vehicle-to-Infrastructure Communications. Vehicular Technology, IEEE Transactions, Volume: 59, pages 269 – 282, 2010.
[12]. Akhtar Hussain, Ram Shringer Raw, Brajesh Kumar and Amit Doegar. Performance Comparisn of Topology and Position Based Routing Protocols in Vehicular Network Environment. Volume 3, number 4, pages 289 – 303. International Journal of Wireless and Ad hoc Networks. August 2011.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

[13]. P. Basu, N. Khan, and T. Little, “A mobility based metric for clustering in mobile ad hoc networks,” Distributed Computing Systems Workshop, 2001 International Conference on, pp. 413–418, Apr 2001.
[14]. C. Lin and M. Gerla, “Adaptive clustering for mobile wireless networks,” Selected Areas in Communications, IEEE Journal on, vol. 15, no. 7, pp. 1265–1275, Sep 1997.
[15]. B. J. Frey and D. Dueck, “Clustering by passing messages between data points,” Science, vol. 315, pp. 972–976, 2007.
[16]. Christine Shea, Behnam Hassanabadi and Shahrokh Valaee. Mobility-based Clustering in VANETs using Affinity Propagation.
[17]. Mr. J.Jayavel, Dr. R.Venkatesan Mr. S. Ponmudi. A TDMA-Based Smart Clustering Technique for VANETs. Volume 65, pages 429 – 436. Journal of Theoretical and Applied Information Technology. 20th July 2014.
[18]. R. T. Goonewardene , F. H. Ali and E. Stipidis "Robust mobility adaptive clustering scheme with support for geographic routing for vehicular ad hoc networks", IET Intell. Transp. Syst., vol. 3, no. 2, pp.148 -158 2009.
[19]. Dror, E.; Avin, C.; Lotker, Z., "Fast randomized algorithm for hierarchical clustering in Vehicular Ad-Hoc Networks," Ad Hoc Networking Workshop (Med-Hoc-Net), 2011. The 10th IFIP Annual Mediterranean, vol., no., pp.1, 8, 12-15 June 2011.
[20]. Tadiparthi Priyanka and T. P. Sharma. A Survey on Clustering Techniques in Vehicular Ad hoc Networks. Pages 174 – 180. Proceedings of 11th IRF International Conference, 15th June- 2014, Pune, India.
[21]. N. Sakthipriya and P. Sathyanarayanan. A Reliable Communication Scheme for VANET Communications Environment. Volume 7, page 31–36. Indian Journal of Science and Technology. June 2014.
[22]. Hamid Reza Arkian, Reza Ebrahimi Atani, Atefe Pourkhalili and Saman Kamali. A Stable Clustering Scheme Based on Adaptive Multiple Metric in Vehicular Ad-hoc Networks. Pages 361 – 386. Journal of Information Science and Engineering. 2015.
[23]. David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, Paul Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice.
[24]. Jean Francois Raymond and Anton Stiglic. Security Issues in the Diffie-Hellman Key Agreement Protocol.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500