www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18812-18818

Trust Factor Based Secure Congestion Control For Vanet

Shanty Bala[1], Dr. Vijay Laxmi[2]

[1]Research Scholar M-Tech, Computer Science and Engineering, Guru Kashi University, India
shantygarg348@gmail.com
[2]Dean, UCCA, Guru Kashi University, India
cse_vijay2003@yahoo.co.in

Abstract: Weight-based clustering algorithm in ad hoc network is an on demand clustering algorithm for multi-hop packet radio network. These types of networks are ad hoc networks and dynamic in nature due to mobility of nodes. Clustering in mobile ad hoc network can be defined as various partitions into various groups. It is an important concept of VANNET, because clustering makes it possible to guarantee of system performance, such as throughput delay and also security issues. So in the algorithm they select the cluster head whose performance is well and formation of cluster in ad hoc network. The cluster head is elected based on weight factor, so it is called weighted clustering algorithm. Weighted clustering algorithm is basically appropriate cluster selection in wireless adhoc network where it is necessary to provide robustness in face of topological changes caused by node motion, node failure and node insertion or node removal. The WCA select the cluster head which has lowest weight among the nodes and some other factor also consider the election for cluster head. The cluster head, form a dominant set in the network, determine the topology and its stability. The weighted clustering algorithm takes into consideration the ideal degree, transmission power, mobility and battery power of nodes. Traffic efficiency applications are becoming increasingly popular over the road networks in the last few years. This type of applications aims mainly at increasing the traffic fluency over the road network, which minimizes the travel time of each vehicle towards its targeted destinations. The Vehicular Ad-Hoc Networks (VANETs) technology has been utilized to design these applications. Communications between vehicles, V2V, and between vehicles and installed Road Side Units (RSUs), V2I, helped designing these applications. Malicious, selfish and intruder drivers can take advantages of other cooperative drivers and use their trust. a Secure Congestion control protocol. This protocol aims to guarantee integrity and authenticity of transmitted data. It is designed to provide the security requirements of traffic efficiency protocols that have been proposed using the technology of VANETs. SCOOL also aims to preserve the privacy of the cooperative vehicles and drivers. The main contribution of work is new strategy for clustering a wireless ad hoc network and improvement in WCA. Author derived a simple stability model and a load balancing clustering scheme. They showed that the algorithm outperform in term of cluster formation and stability. Main idea of approach is to avoid cluster re-election and reduce the computation and communication cost. The improved weighted clustering algorithm, the goals of algorithm are maintaining stable clustering structure, minimizing the overhead for clustering set up, maximize lifetime of nodes in the system and achieving good performance.

Keyword – *Weight-based clustering,* SCOOL, WCA, *VANETs.*

I. Introduction

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.[1] Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.[2]Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks.

Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e., a contact) arises. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery. Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination (eventually and over time).

II. TRAFFIC CONGESTION CONTROL PROTOCOLS

Here, we discuss some of these traffic congestion control protocols that have been proposed using the technology of VANETs. Many researchers have investigated and evaluated the traffic characteristics of road network during a certain period of time using the communications technology of VANETs. These mechanisms and protocols collect the basic traffic data of its surrounding vehicles. Each traveling vehicle is expected to be provided by a wireless transceiver and GPS devices. Vehicles need to broadcast their basic data periodically in order to announce their location, direction and speed during a certain period of time. Receiver vehicles can compute the traffic density [4], traffic speed [5], or estimated travel time of its area using the basic gathered data about the surrounding vehicles. In order to expand the evaluated areas, Fukumoto et al. [4] used a blind forwarding mechanism where each vehicle forwards the received advertisement message. On the other hand, Dornbush et al. [5] proposed a mechanism that forwards the statistical data about the traffic situation over the area of interest. In our previously proposed work [6], we introduced a protocol that aimed to evaluate the traffic characteristics on any road segment in a downtown area. According to the road segment length, some reporting areas are virtually determined where vehicles over these forwarding areas are responsible for forwarding the gathered traffic data,

in order to deliver the traffic information between vehicles that cannot contact directly.

III. SECURE PROTOCOLS FOR VANETS

Different protocols and mechanisms have been proposed to guarantee secure communications over VANETs. The typical secure communication mechanisms are not always suitable for VANETs, due to its high mobility and geographical extension nature. Several proposals and research studies have been introduced to address the security issue over VANETs. Some researchers have investigated the security issue as an independent and general topic for VANETs technology [8], [9]. Symmetric, asymmetric and groupbased cryptography protocols have been proposed to guarantee the authenticity, confidentiality, integrity, and the privacy features [10], [11], [12]. However, some secure protocols have been proposed to provide a certain service and specifically considering the requirements of these services, such as: secure cooperative collision warnings [13], secure position information [14], secure information dissemination [15], and secure service discovery protocols [16]. To the best of our knowledge, none of the previous secure protocols took into consideration traffic efficiency applications and congestion control protocols in particular. As a consequence, we introduce a secure traffic congestion control protocol (SCOOL) in this paper. Our protocol aims at providing a security protection that prevents malicious and prankster drivers from deceiving cooperative drivers all over the road network. Moreover, it guarantees private communications that protects the real identity of drivers and guarantees conditional traceability.

IV. ADVERSARY THREATS OF TRAFFIC EFFICIENCY PROTOCOLS

Some traveling vehicles try to deceive their surrounding vehicles and RSUs by generating fake traffic evaluation reports and producing false congested area alerts. They mean to encourage other drivers to avoid going through the same path that they are traveling. In that case, these malicious drivers enjoy lighter traffic and faster trips. Moreover, malicious and selfish drivers may deliver fake traffic report to the located traffic lights to eliminate the queuing delay at the signalized road intersections and smoothly pass the intersection. Some malicious attackers seek only to decrease the network functionality without the intent of personal gain, so they broadcast fake and misleading reports all over the communication network. In addition, some intruder and criminal drivers aim at stalking other drivers and retrieve their locations and targeted destinations over the road network. In the following, we discuss the possible attacks and the adversary threats on congestion control protocols. 1) Sybil Attacks: Some vehicles broadcast beacon messages with different identities and locations over a certain road segment. A fake traffic congestion over that road segment would be reported in that case. Hence, these vehicles deceive their surrounding vehicle, path generator units and intelligent traffic lights. 2) Forgery: Some attackers alter the reading of the sensors within their own nodes. They broadcast a periodic beacon with fake data of the vehicle including its position, speed and direction. On the other hand, some vehicles that are used as router to forward messages between adjacent hops over VANETs can alter and compromise the forwarded data or initiate a fake report. 3) Masquerading: Some attackers claim the identity of another vehicle or RSU over the network. These attackers aim at utilizing some facilities and functionalities illegally. This can be achieved by spoofing the identity of other nodes or replaying some legal packets; that have been sent previously. Masquerading can cause a serious danger situation, for example, in the case that criminal driver pretends to be a traffic light node it can easily create a severe accident at the road intersection by informing two conflicted flows of traffic to pass the intersection simultaneously. 4) Non-repudiation: Some attackers can deny sending and/or receiving a certain packet. The authorized agencies will therefore not be able to determine the identity of the sender. In this case the senders can send a damage data without being asked to take responsibility of sending such a data. 5) Denial of Service: In this case, attackers overload the communication channel or make its utilization difficult. It could be performed by compromising a number of fake RSUs, or by making a vehicle broadcast large number of messages in a short period of time. 6) Black-hole Attack and Selfish Behavior: Some attackers and malicious nodes drop all or few selected packets, aiming to serve their own benefits or only to destroy the communication services all over the network. This can construct a bad path towards each destination and may produce a bad schedule of each located traffic light. These scenarios may happen as a consequence of inaccurate traffic evaluation of the traffic flows. 7) Privacy: The privacy of cooperative nodes over VANETs has two main threats: traceability and link ability. The first threat refers to the case that the different actions of a certain vehicle can be traced. On the other hand, link ability refers to the case that an unauthorized entity can link a vehicle identity to its driver/owner.

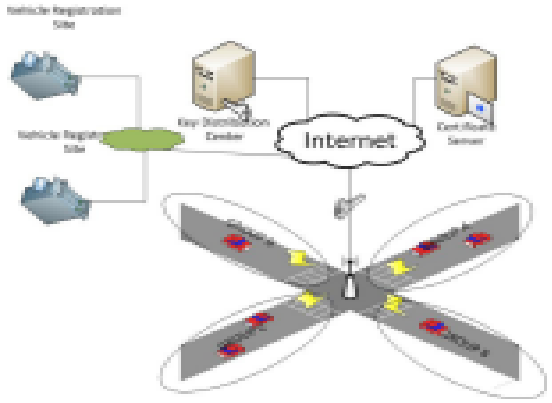

Figure 1.1: SCOOL Authentication Scenario [9]

V. LITERATURE SURVEY

In this paper have studied the different papers to review my research topic. The different authors papers studied each have followed the different techniques and methods.

Maram Bani Younes et.al.(2015) have studied Traffic efficiency applications are becoming increasingly popular over the road networks in the last few years. This type of applications aims mainly at increasing the traffic fluency over the road network, which minimizes the travel time of each vehicle towards its targeted destinations. The Vehicular Ad-Hoc Networks (VANETs) technology has been utilized to design these applications. Communications between vehicles, V2V, and between vehicles and installed Road Side Units (RSUs), V2I, helped designing these applications. Malicious, selfish and intruder drivers can take advantages of other cooperative drivers and use their trust. This paper introduces a Secure COngestion contrOL (SCOOL) protocol. This protocol aims to guarantee integrity and authenticity of transmitted data. It is designed to provide the security requirements of traffic efficiency protocols that have been proposed using the

technology of VANETs. SCOOL also aims to preserve the privacy of the cooperative vehicles and drivers. From the experimental results we can infer that SCOOL detects the malicious nodes over the road network which enhances the correctness of the traffic efficiency applications [5]. Sofiah.W.I., et.al (2014)have studied Wireless sensor network and its applications are interesting research that have been focused recently. Battery consumption of sensor nodes is the main problem in the family of wireless sensor that should be solved. So, to increase the scalability of the network, and to reduce the energy usage for overall sensor operations, clustering techniques and data aggregation are the main focus. The multi-tier techniques has been designed precisely and the selection of the cluster head using Fuzzy Logic based on the three selected parameters are well used along with its limited resources of wireless sensor network. In this study, the main primary and secondary cluster head are the important entities of the algorithm for receiving and transmitting data to the base station. The contribution of is mainly on the selection of a secondary cluster head and the routing protocol which the data transmission will involve the nearest cluster head for both tier one and tier two. Due to multi-tier clustering in sensor network, the operations of the sensor network will eventually increase the lifetime of the network compared to LEACH and SEP protocols [1]. Grover.A., et.al (2014) have studied energy models to cluster based energy efficient routing in Wireless sensor networks (WSNs). In wireless sensor networks, nodes execute on confined force batteries that brings about reducing its lifetime, henceforth WSNs are viewed as a force devouring plans. As the wireless sensor nodes are greatly energy based, the energy efficient routing protocols are necessary with the aim of balancing and reducing energy consumption over the whole network. Subsequently, several specialists have proposed distinct routing protocols for sensor networks, especially routing protocols depending on clustering scheme to minimize the energy utilization in wireless sensor network. This is on the account of the utilization of cluster based routing that has various benefits like to minimize control messages, re-usability of bandwidth and diminishing the energy consumption by aggregating data at intermediate sensors. This article presents a multi-tier multi-hop clustering scheme to reduce the energy consumption of wireless sensor network in which, multipath-AODV routing protocol is used to route the data from source to destination. In the demonstration of simulation results, as compare to LEACH the proposed algorithm provides higher performance and longer network lifetime[2].

VI. METHODOLOGY

This section defining the way of implementation that is to done in this research work. In this work WCA is designed with the help of Network Simulator. The main objective of our approach is to cluster the network efficiently around a few high-energy cluster head nodes. Clustering extends the life of the network by allowing the cluster heads to conserve energy through communication with closer nodes and by balancing the load among them. Since we assume that all nodes are identical and produce data at the same rate, to balance load in the system we have to balance the number of nodes in a cluster and the communication energy required per cluster head.

The node degree of a node v_i is deduced as the cardinality of the set $N(v_i)$:

$$deg(v_i) = |N(v_i)| \quad (4.1)$$

Based on the previous equations, we set our stability factor for each node v_i as:

$$STF(v_i) = virD(v_i)/deg(v_i) \quad (4.2)$$

We propose to calculate the relative dissemination degree. This parameter reflects the relative deviation of the number of neighbors in a current setting from that ideal.

$$\beta(v_i) = \frac{|\delta - deg(v_i)|}{deg(v_i)} \quad (4.3)$$

It is known that more power is required to communicate to a larger distance. Therefore, we are motivated to evaluate the energy consumption. For this purpose, for every node v_i, we compute the sum of the distances $D(v_i)$, with its neighbors, as:

$$D(v_i) = \sum_{j=1}^{n} dis(v_i, v_j) \quad (4.4)$$

The cluster head selection process is composed of the following steps:

1. Find the neighbors (degree) of each node using (4.1).
2. For each node, calculate the stability factor using (4.2).
3. For each node, calculate the relative dissemination degree using (4.3).
4. Evaluate the energy consumption using (4.4).
5. Calculate the remaining battery energy of each node (RBE(vi))
6. Calculate the combined weight W(vi) for each for each Node vi: W_{vi}=D(Vi)*0.2+β(Vi)*0.5+STF*0.1+Mv*0.2
7. Select the node not situated on the border and having the minimum weight Wvi as a cluster head.
8. Delete node vi and all itsN(vi) from G.
9. Repeat the 7th and 8th steps until G is empty.

Awaiting Factor =1

6.1 NETWORK COMPONENTS

This section talks about the NS components, mostly compound network components. The root of the hierarchy is the TclObject class that is the superclass of all OTcl library objects (scheduler, network components, timers and the other objects including NAM related ones).

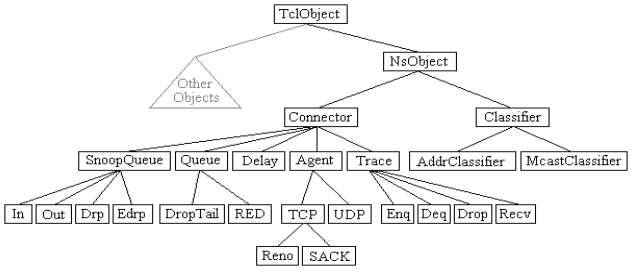

Figure 1.2: Class Hierarchy (Partial)

Node and Routing

A node is a compound object composed of a node entry object and classifiers as shown in Figure 1.3. There are two types of nodes in NS. A unicast node has an address classifier that does unicast routing and a port classifier. A multicast node, in addition, has a classifier that classify multicast packets from unicast packets and a multicast classifier that performs multicast routing.

DOI: 10.18535/ijecs/v5i11.16

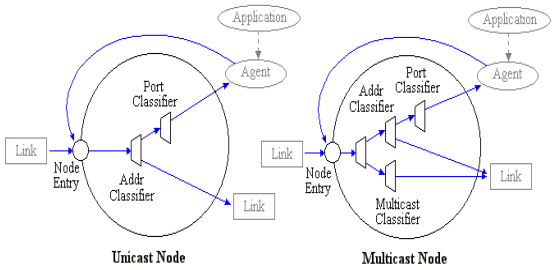

Figure 1.3: Node (Unicast and Multicast)

6.1.1. Unicast

- $ns rtproto type
- type: Static, Session, DV, cost, multi-path

6.1.2. Multicast

- $ns multicast (right after set $ns [new Scheduler])
- $ns mrtproto type
- type: CtrMcast, DM, ST, BST

6.1.3. Link

A link is another major compound object in NS. When a user creates a link using a duplex-link member function of a Simulator object, two simplex links in both directions are created as shown in Figure 1.4.

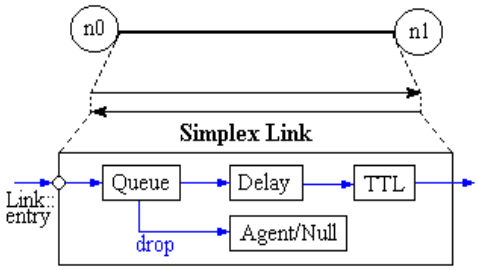

Figure 1.4: Link

6.1.4. Tracing

In NS, network activities are traced around simplex links. If the simulator is directed to trace network activities, the links created after the command will have the following trace objects inserted as shown in Figure 1.5.

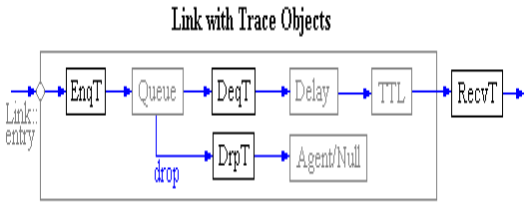

Figure 1.5: Inserting Trace Objects

6.1.5. Queue Monitor

Basically, tracing objects are designed to record packet arrival time at which they are located. Although a user gets enough information from the trace, he or she might be interested in what is going on inside a specific output queue.

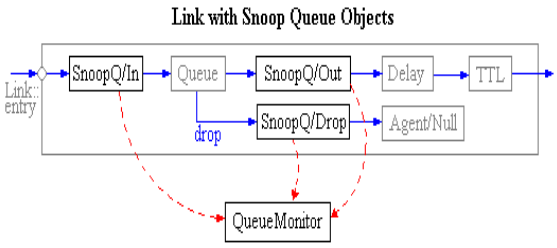

Figure 1.6: Monitoring Queue

6.1.6. Packet Flow Example

Until now, the two most important network components (node and link) were examined. Figure 1.7 shows internals of an example simulation network setup and packet flow.

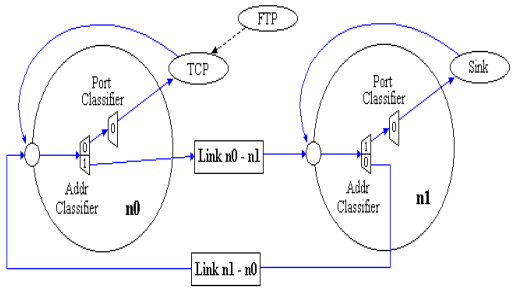

Figure 1.7 Packet Flow Example

6.2. ADVANTAGES AND DISADVANTAGES OF NS2

6.2.1. Advantages

1. Cheap- Does not require costly equipment
2. Complex scenarios can be easily tested.
3. Results can be quickly obtained – more ideas can be tested in a smaller time frame.
4. Supported protocols
5. Supported platforms
6. Modularity
7. Popular

6.2.2. Disadvantages

1. Real system too complex to model. i.e. complicated structure.
2. Bugs are unreliable

VII. RESULTS

This chapter Experimental result displays the different snapshots that are on research work. These are given below:

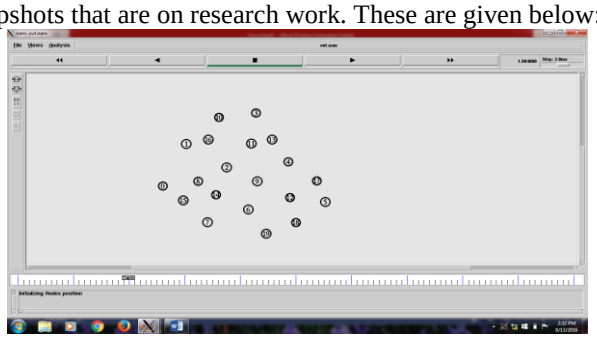

Figure 1.8: Input node distribution

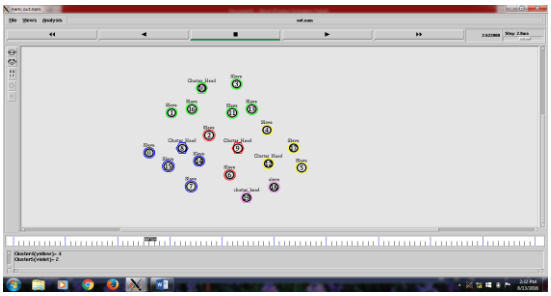

Figure 1.9: Node and Cluster distribution with color

In the figure 1.8, is the processing of node and the distribution of node in the WSN and the figure 1.9 is the processing of nodes with their color.

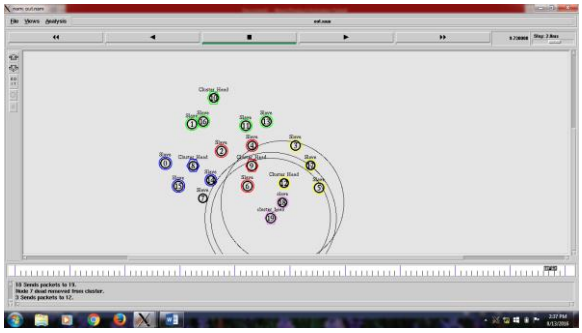

Figure 1.10: The transmission of signals in nodes and clusters

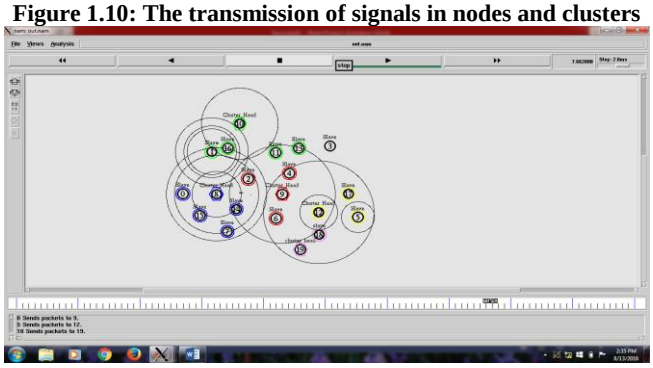

Figure 1.11: Node and cluster transmission of signals

The figure 1.10 is the processing of signals from nodes and the cluster head and the figure 1.11 is the broadcasting of the signals from node to node and the clusters in VANNET.

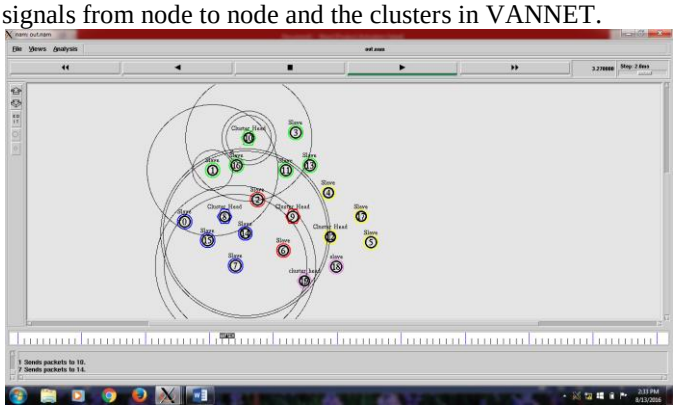

Figure 1.12: Fully transmission of signals between nodes

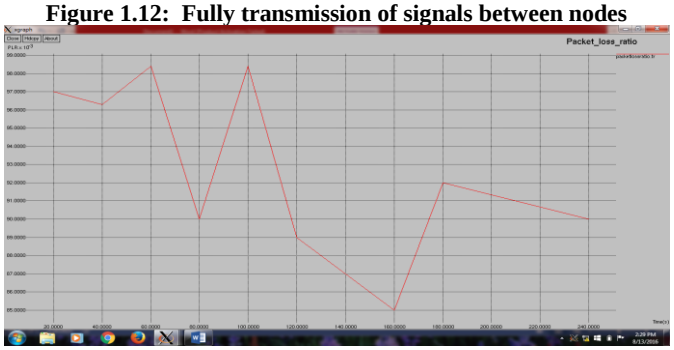

Figure 1.13: Packet loss ratio w.r.t to time

The figure 1.12 is the fully transmission of signals from node to node and node to the cluster head. The figure 1.13 is the packet loss ratio graph w.r.t. to the time of the network.

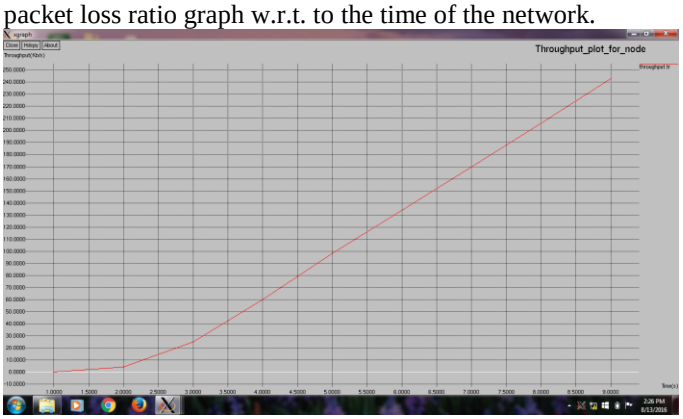

Figure 1.14: Throughput plot for node w.r.t time

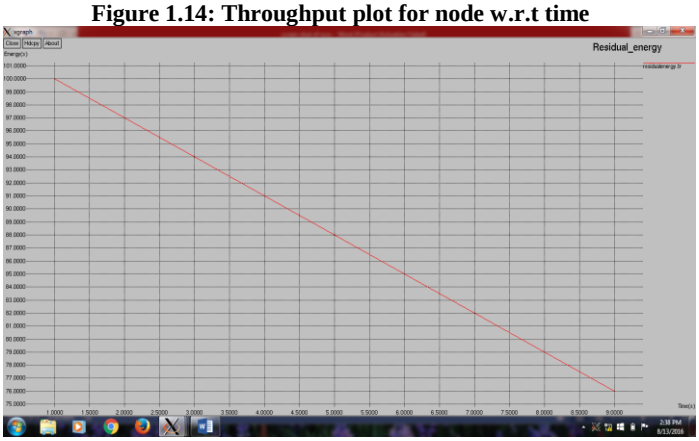

Figure 1.15: Residual energy on the network

The figure 1.14 is the processing of throughput of the network with respect to the time. In this the throughput is varied with the time of the network. But the figure 1.158 is the processing of the residual energy on the network.

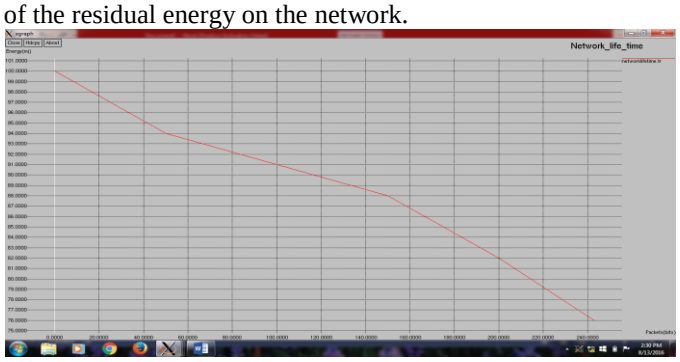

Figure 1.16: Network Life time

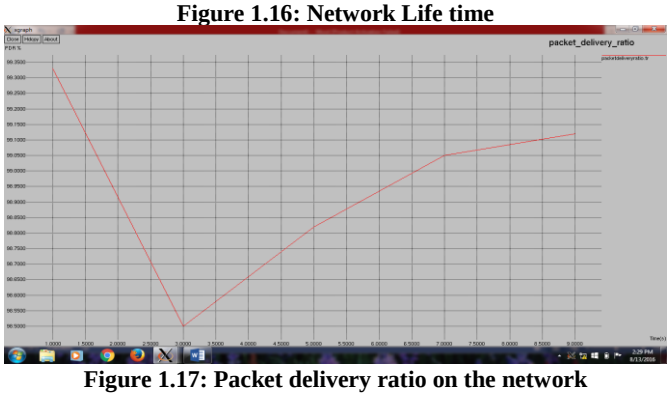

Figure 1.17: Packet delivery ratio on the network

The figure 1.16 is displaying the network life time of the nodes and their transmission. But the figure 1.17 is the Packet delivery ratio on the network. It is varied with time of the network.

Table 5.1: Parameter Performances

Nodes	Neighbours	D(V1)	D(V2)	STF	Mv	Wvi
0	3	1.9	1	0.6	1	1.19
1	4	2.8	0.5	0.7	1	1.71
2	6	4.2	-0.14	0.6	0.5	1
3	3	2.1	1	0.3	1.5	1.29
4	5	3.5	0.2	0.7	1.5	1.39
5	3	2.1	1	0.7	0.5	1.09
6	5	3.5	0.2	0.7	0.5	0.97
7	4	3.2	0.5	0.7	1	1.12
8	7	4.2	-0.14	0.6	0.5	0.93
9	7	4.2	-0.14	0.6	0.5	0.93
10	5	3	0.2	0.6	0.5	0.86
11	7	5	-0.14	0.7	1	1.2
12	6	3.6	0	0.6	0.5	0.88
13	3	2.1	1	0.7	0.5	1.07
14	7	4.9	-0.14	0.7	0.5	1.01
15	4	2.5	0.5	0.62	1	1.01
16	5	3.5	0.2	0.7	0.5	0.97
17	4	2.8	0.5	0.7	1.5	1.08
18	4	2.8	0.5	0.7	1.5	1.11
19	3	1.6	1	0.5	1	1.07

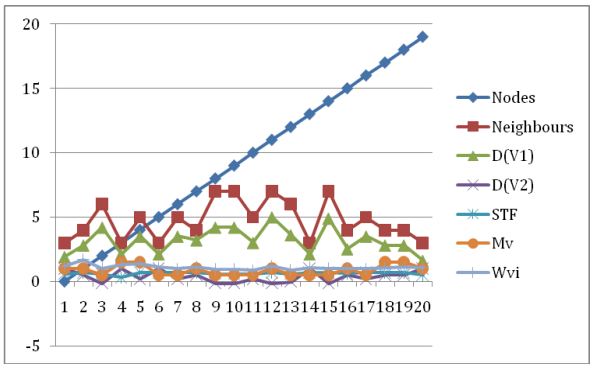

Figure 5.11: Graphical representation of parameter performances

VIII.CONCLUSION

Clustering is one of important method to be applied in order to prolong the network lifetime of wireless sensor network. The selections of cluster head also are important parts to be considered so that the lifetime of sensor nodes remains longer than usual. The main problem in wireless sensor network is the battery consumption. The sensor node battery cannot be recharged once it is depleted and there is no power supply. The existing protocols are not applicable to those WSNs that are deployed in large regions because it uses single hop routing where each sensor node can communicate directly to the cluster head and the base station. So, it causes problems of energy imbalanced. The problem of unbalanced energy dissipation in cluster based WSNs is investigated. Another problem is cluster-based and homogeneous WSNs in which cluster heads transmit data to base station by one -hop communication. We have thought-about the matter of constructing a framework for dynamic organizing mobile nodes in wireless ad-hoc networks into clusters wherever it's necessary to produce hardiness within the face of topological changes caused by node motion, node failure and node insertion/removal. Extending previous works, we've got conjointly mathematically derived a replacement clump stability theme. Within the same objective we have a tendency to derived a straightforward clump load equalization theme. The introduced protocol controls the traffic congestion problem over the urban areas in secure and efficient manners. It uses the public cryptography to authenticate the existing RSU at each road intersection. Moreover, the group signature and identity-based authentication principles are used in the communications between vehicles at each road segment. The located RSUs manage the group cryptography among all vehicles. Over each road segment the traveling vehicles are treated in a separate group.

In this I even have designed wireless clump rule with the assistance node degree, Stability issue, and weight and cluster head choice. During this we have a tendency to square measure increasing the node and node degree and that we are becoming the utmost weight of the network nodes.

IX. FUTURE SCOPE

In the future work it is improved with the help of other routing protocols to get the better results on dead nodes and the live nodes to find the energy loss and packet loss during the transmission of data.

REFERENCES

[1]. Sofiah.W.I., et.al (2014), "MAP: The New Clustering Algorithm based on Multitier Network Topology to Prolong the Lifetime of Wireless Sensor Network" 10th International Colloquium on Signal Processing & its Applications (CSPA2014), 7 - 9 Mac. 2014.

[2]. Grover.A., et.al (2014), "AOMDV with Multi-Tier Multi-Hop Clustering in Wireless Sensor Networks" Advanced Engineering Technology and Application,Adv. Eng. Tec. Appl. 3, No. 3, 29-33 .

[3]. Tripathi.A., et.al (2014)," "Survey on Data Aggregation Techniques for Wireless Sensor Networks " International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July2014.

[4]. Meng., et.al (2013), "An Energy Efficient Clustering Scheme for Data Aggregation in Wireless Sensor Networks." Journal of Computer Science and Technology 28, no. 3.

[5]. Maram Bani Younes et.al. (2015), "SCOOL: A Secure Traffic Congestion Control Protocol for VANETs" Wireless Communications and Networking Conference (WCNC): - Track 3: Mobile and Wireless Networks 2015 IEEE.

[6]. Dawood.M.Sheik., et.al (2012), "Study of Energy Efficient Clustering Algorithm for Wireless Sensor Networks" International Journal of Emerging Research in Management &Technology .

[7]. Yuea.Jun., et.al (2012), "Energy efficient and balanced cluster - based data aggregation algorithm for wireless sensor networks." Procardia Engineering 29: 2009-2015.

[8]. Tharini,C., et.al (2011), "An Energy Efficient Spatial Correlation Based Data Gathering Algorithm for Wireless Sensor Networks" International Journal of Distributed and Parallel Systems 2(3), 16–24.

[9]. Rahmani.N., et.al (2010), "CAT: The New Clustering Algorithm Based on Two-Tier Network Topology for Energy Balancing in Wireless Sensor Networks,"in Computational Intelligence and Communication Networks(CICN), 2010 International Conference on, 2010.

[10]. Dehni.L., et.al (2006), "Power Control and Clustering in Wireless Sensor Networks," in Challenges in Ad Hoc Networking. vol. 197, K. Agha, et al., Eds., ed: Springer US.

[11].

[12]. Heinzelman.W.R., et.al (2000), "Energy-efficient communication protocol for wireless micro sensor networks," in

System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on.
[13]. Stankovic John A., Abdelzaher T, Lu C, Sha L, and Hou J (2003), "Real-time communication and coordination in embedded sensor networks," Proceedings of the IEEE, vol. 91, no. 7, 2003.
[14]. Hashmi S and T. Moufth, (2003), "A New Transport Layer Sensor network protocol", IEEE Transactions, vol. 5,pp.118-156, Mar.2003
[15]. Annoa, J., Barollib, L., Durresic, A., Xhafad, F., & Koyamae, A. (2008), "Performance evaluation of two fuzzy-based cluster head selection systems for wireless sensor networks", Mobile Information Systems, 4, 297– 312.
[16]. Khalid Hussain, Abdul Hanan Abdullah,(2013), "Cluster Head Election Schemes for WSN and MANETǁ: A Survey", ISSN 1818-4952 © IDOSI Publications.
[17]. OssamaYounis And Sonia Fahmy, Heed: ―A Hybrid, Energy-Efficient, Distributed Clustering Approach For Ad-Hoc Sensor Networksǁ, (vol-3,issue- 4I 2009n 47907– 2066, Usa).
[18]. Anno, J., Barolli, L., Xhafa, F., &Durresi, A. (2007). A cluster head selection method for wireless sensor networks based on fuzzy logic. In IEEE region 10 annual international conference, TENCON 2007 1–3 (pp. 833– 836).
[19]. Zhou, W., Chen, H. M., & Zhang, X. F. (2007). An energy efficient strong head-clustering algorithm for wireless sensor networks. In 2007 international conference on wireless communications, networking and mobile computing, WiCOM 2007 (pp. 2584–2587).
[20]. Mohamed Aissa, Abdelfettah Belghith "An Efficient Scalable Weighted lustering Algorithm for Mobile Ad Hoc Networks" IEEE 2013.
[21]. DAMLA TURGUT "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks" Cluster Computing 5, 193–204, 2002 2002 Kluwer Academic Publishers. Manufactured in The Netherlands.
[22]. Amine Dahane "A Distributed and Safe Weighted Clustering Algorithm for Mobile Wireless Sensor Networks" The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015).
[23]. Matthias R. Brust, Adrian Andronache and Steffen Rothkugel "WACA: A Hierarchical Weighted Clustering Algorithm optimized for Mobile Hybrid Networks" Cluster Computing April 2002, Volume 5, Issue 2, pp 193-204.
[24]. R. Pandi Selvam et al, Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (2), 2011,824-828.
[25]. R. Pandi Selvam et al, Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (2), 2011,824-828.
[26]. Suchismita Chinara, Santanu Kumar Rath. A Survey on One-Hop Clustering Algorithms in Mobile Ad Hoc Networks. Journal Network System Management; 17:183–207; 2009.
[27]. Naveen Chauhan et al. A Distributed Weighted Cluster Based Routing Protocol for MANETs. Wireless Sensor Network; 2011; 3, 54-60, doi:10.4236/wsn.2011.32006 Published Online February 2011 (http://www.SciRP.org/journal/wsn)
[28]. M. Chatterjee, S. K. Das, and D. Turgut. WCA: a weighted clustering algorithm for mobile Ad Hoc networks. Cluster Computing 5, 193-204; 2002.
[29]. Christian Bettstetter. The Cluster Density of a Distributed Clustering Algorithm in Ad Hoc Networks. IEEE International Conference Communications; Page(s): 4336 - 4340 Vol.7; 2004.
[30]. S. Basagni. Distributed clustering for ad hoc networks. In: Proc. Intern. Symp. Parallel Architectures, Algorithms, and Networks (ISPAN); (Perth/Fremantle, Australia); June 1999.
[31]. S. K.B. Rathika and J. Bhavithra. An Efficient Fault Tolerance Quality of Service in Wireless Networks Using Weighted Clustering Algorithm; Bonfring International Journal of Research in Communication Engineering; Vol. 2, Special Issue 1, Part 4; February 2012.
[32]. Tolba, Magoni, D. ; Lorenz, A stable clustering algorithm for highly mobile Ad Hoc networks, P. Second International Conference on Systems and Networks Communications, 2007. ICSNC 2007.
[33]. W. Jin,et al. A load-balancing and energy-aware clustering algorithm in wireless ad-hoc networks; Embedded and Ubiquitous Computing – EUC 2005 Workshops; Lecture Notes in Computer Science Volume 3823; pp 1108-1117; 2005.
[34]. Xi'an Jiaotong, et al. WACHM: Weight based adaptive clustering for large scale heterogeneous MANET; Communications and Information Technologies; ISCIT '07; 2007.
[35]. Hui Cheng, et al. Stability-aware multi-metric clustering in mobile ad hoc networks with group mobility. Wireless Communications and Mobile Computing; 9:759–771, Published online 21 April 2008 in Wiley InterScience, B. Bollbas. Random Graphs; Academic Press; 1985.
[36]. M. Amine Abid, Abdelfettah Belghith. Stability routing with constrained path length for improved routability in dynamic MANETs. The International Journal of Personnal and Ubiquitous Computing, Springer, Volume 15, Issue 8, pp. 799-810, 2011.