Secure Clustering in Vehicular Ad Hoc Networks

Zainab Nayyar
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad
Pakistan

Dr. Nazar Abass Saqib
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad
Pakistan

Dr. Muazzam Ali Khan Khattak
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad
Pakistan

Nazish Rafique
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad
Pakistan

***Abstract*—A vehicular Ad-hoc network is composed of moving cars as nodes without any infrastructure. Nodes self-organize to form a network over radio links. Security issues are commonly observed in vehicular ad hoc networks; like authentication and authorization issues. Secure Clustering plays a significant role in VANETs. In recent years, various secure clustering techniques with distinguishing feature have been newly proposed. In order to provide a comprehensive understanding of these techniques are designed for VANETs and pave the way for the further research, a survey of the secure clustering techniques is discussed in detail in this paper. Qualitatively, as a result of highlighting various techniques of secure clustering certain conclusions are drawn which will enhance the availability and security of vehicular ad hoc networks. Nodes present in the clusters will work more efficiently and the message passing within the nodes will also get more authenticated from the cluster heads.**

***Keywords*—Vehicular ad hoc networks; secure clustering; wireless technologies; certification authority; cluster heads**

I. 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. Another system model, an Ad-hoc Network, it is a self-organizing collection of Mobile Nodes that form an infrastructure less wireless network on a shared wireless channel. Nodes which lie in the range of each other can easily communicate, while those which are far apart from each 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. Security is an important issue which is faced while deploying the ad hoc networks; the security issues under consideration are availability, confidentiality, integrity, authentication and non-repudiation [3] [4]. Availability refers that the system must survive in critical conditions such as denial of service and worm attacks. The attackers also try to create hindrance in the communication between the nodes and also try to interrupt the routing protocols. Confidentiality is the secret information requires safety so it cannot be disclosed to the unauthorized users. Integrity is that data should not be corrupted and the original information should remain original. Authentication is achieved by not to permitting those entities within the network which can harm the network and only register the trusted entities. In non-repudiation the source of the data should be safe and secure [6]. The concept of Vehicular Ad Hoc networks is derived from mobile ad hoc networks. The reason for deploying vehicular ad hoc networks was 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].

A VANET turns every participating car into a wireless router or node, allowin**g cars approximately 100 to 300** meters of each other to connect and, in turn, crea**te a network with a wide range** [5]. There are two main types of communications discussed under the section of VANETs: Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I). The former protocol is necessary to be applied on the vehicles for proper communication, Road safety and collision avoidance which are necessary for avoiding accidents. The later 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 [9].

Clustering means that different nodes in the system act as a whole system, securing a cluster means that to apply such protocols and actions on the clusters that it is not exposed to any attacker, malware etc. Securing actually belongs to the robustness of the system to certain attacks. The other issue due to which secure clustering is necessary is when there is a time of collecting and aggregating data from the nodes. At that time there are more chances of attacks for accessing the data by the attackers. Due to this reason secure clustering protocols are

used for preventing and securing the clusters from various attacks [10].

In secure clustering there are symmetric as well as asymmetric algorithms used. In a symmetric algorithm there is often a shared key whereas in an asymmetric algorithm there is a requirement of secure mapping of public keys with the user's identities using public key infrastructure. PKI is often used in certification authority where a digitally signed certificate is issued to every registered user so that they can get their public key [11].

This paper gives the state-of-the-art review of typical secure clustering techniques for vehicular ad hoc networks. It is impossible to say which technique is better for a given condition. Hence, the motivation is to compare these strategies this paper includes new technical trends such as public key infrastructure, Shamir secret key algorithm, dynamic demilitarized zone etc. The rest of the paper comprises of II literature review, III comparative analysis, IV conclusion and future work and V references.

II. Literature Review

A. Key Management in Ad hoc Networks

In [5] key management in ad hoc networks was addressed, where in ad hoc networks the old methods to achieve security were not adaptable. Due to these factors key management was very difficult in ad hoc networks. In key management technique the public key infrastructure used a centralized approach in similar clusters and a distributed key was used between the cluster heads. It resulted in suitable, economical, scalable and autonomous key management.

B. Shamir's Secret Scheme

It is observed in [6] that in ad hoc networks it was easy to launch worm, man in the middle, denial of service attacks and to inoculate a malicious node, this was all done due to the lack of data integrity. The Shamir's secret scheme along with data redundancy mechanism of certificate revocation and renewal was applied. It was a hop by hop protocol. On every hop the data got authentication from certificate authority. Each node had the authority of checking the behavior of its previous node and on the basis of that behavior it could declare that node as malicious or trustworthy. The detection of malicious node became easy. During packet delivery less overhead and delay occurred.

C. Threshold Cryptography

In the [11] architecture was proposed for securing the clusters in ad hoc networks. A network was divided into clusters and a decentralized certification of authority was implemented. Decentralization was achieved using threshold cryptography and a network secret. The reason for deploying decentralized approach of distributing a certification authority on the nodes was that the ad hoc entities were vulnerable to several attacks and their reachability was not possible for all the nodes of the network. In the intra cluster security asymmetric key distribution was used. These keys used to protect all the traffic nodes. The attackers could not break the secrets even if they got some data it was of no use to them. Scalability and availability was achieved by dividing the network into small clusters. Availability was enhanced because certificates can be issued even if some nodes were out of reach. The asymmetric key distribution was useful in a way that there were no other means needed to secure the communication.

D. Trust Based Physical Logical Domains

The aim of [12] was to achieve trust on the basis of keys in mobile ad hoc networks. The trust based physical logical domains was introduced for grouping nodes and getting distributed control over the network.

E. Secure Message Aggregation & Onion Signature

In [13] two methods were introduced – first was the approach of secure message aggregation, and second was onion signature which was declared as a part of onion routing. The highlighted problem was that asymmetric solutions were resource hungry in the case of communication and computation. The accuracy in aggregation of vehicles depends upon the density of vehicles, the higher the density the greater the accurate aggregation. The grouping of vehicles was set geographically normally the range set is 300m. When the vehicle (leader) moves out of range, the election procedure takes place and the vehicle having lowest ID is declared as a leader. For security purposes the IDs which vehicles generate were not their actual IDs instead they were pseudonyms. Grouping of several messages provide the receiver with more information regarding the specified event. Simplicity and robustness was achieved by dividing the roads into cells. Using PKI and digital signatures authentication was achieved. Reduction in the network traffic due to aggregation of messages and achieved availability. Efficiency and routing benefits are achieved due to election of leaders. Data verification is escaped due to the aggregation of messages. The division of roads into cells can cause an overhead and thus this aspect needs to be improved. Due to aggregation false data can be inserted by the attackers into the network that is why only honest nodes could apply this algorithm. Combining signatures could create security overhead and delay.

F. Secure Clustering Algorithm

Mobile ad hoc networks are increasing in size day by day so in [14] a problem aroused in which due to the growth of nodes in number it became difficult to handle them. So a secure method was to divide the nodes in an hierarchal way which was known as secure clustering algorithm that provided more effectiveness, protection and trust in increasing the size of the cluster. It also defined how much a node could be trusted and by allocating certificates protecting the nodes from certain attacks. The algorithms which were previously defined for managing clusters were not helpful for managing big clusters. Secure clustering algorithms proposed a weight based algorithm which includes the certain parameters for electing the algorithm.

G. Position Based Prioritized Clustering

In [15] due to rapid change in the positions of cars during long journeys, change of direction and network topologies some information may be lost. So for solving that issue, position based prioritized clustering was implemented and for

that CORSIM and NS-2 simulators were used. The radius regarding each cluster was taken under consideration as any node could be a part of the cluster until it gets out of the range of radio frequency. So if the radius of any node considers being the greater than the specified radius than that vehicle was no more than the part of that cluster. If the threshold between two clusters was less than that which was set, then the cluster with lesser nodes became a part of another cluster. The MDS election algorithm is followed in which the election of cluster heads is defined; this algorithm was the solution of the problem which was created due to the presence of many cluster heads formation which was caused due to other cluster head election algorithms. Using MDS technique stability in the performance of cluster heads was increased. Position based prioritized clustering was helpful in decreasing the cluster overheads.

H. Fully Distributed Trust Based Model

In [16] the problem identified was the creation of the trusted environment by applying the techniques applied on fixed networks security and trust could not be achieved therefore a fully distributed trust based model was proposed in which ad hoc networks generate and distribute a public key without any fixed mode of transmission. A threshold was also included in the public model so that the malicious nodes cannot get the authorized key from the certification authority.

I. Dynamic Demilitarized Zone Technique

In [17] the problem identified was that many anonymous nodes sometimes become successful in getting signed certificates, so the dynamic demilitarized zone technique was introduced in which the unknown nodes were not authorized to communicate with the certificate authority nodes. All the nodes have to pass through the dynamic demilitarized zone to request the certificate from the certificate authority node. There were multiple certificate authorities involved in that algorithm each of which was responsible for its own geographical area. The road side units were also combined with the central certificate authorities who worked as an intermediate between the central certificate authorities and dynamic certification authorities on the road. Along with dynamic certification registration authorities and sub cluster heads were also involved in this mechanism. Reference [21] was the extension of [17] as in [17] the issue was detected during the election of certification authorities in which denial of service was occurring. The issue was solved in [21] using VANET dynamic demilitarized zone that would handle the certificate request from the unknown vehicles and prohibit malicious communication between certification authority and nodes. Its additional feature was that each vehicle which was at 1-hop from other vehicles sent hello messages, as result the nodes which received that message saved the each and every record of the vehicle and thus response with a joint message to that node. Detection of malicious nodes became more efficient. Confidentiality increased, overhead decreased. Shifting from one cluster to another enhanced due to the presence of sub cluster heads. It removed the issues of denial of services.

J. Distributed Algorithm:

In the [18] the distributed algorithm was used in the protocol for the security and formation of the cluster, the system also checked that if the claimed data was reliable and authentic. The cost delivery protocol, cluster head designation protocol and cluster management protocol are used for cluster formation. It provided the reliability and authenticity of data. The biggest risk of deploying this technique is that according to the supposition all the data is considered to be correct and authenticated.

K. Vehicular Clustering Based On Weighted Clustering Technique:

In [19] three suitable scenarios that are mainly for highway traffic were discussed. The first was that was used for choosing the cluster heads giving different parameters which could improve stability, connectivity and security of VANETS. The second technique was the Adapter allocation of transmission range which used hello messages and ensured connectivity among the vehicles. The third scenario was Monitoring of malicious vehicles to detect abnormal vehicles in the system. The re-affiliation issue in which the swapping of clusters occurred caused the great overhead, so this problem was also resolved by reducing the swapping of clusters. In [22] secure and stable vehicular clustering based on weighted clustering algorithm was proposed in which secure and stable cluster formation along with malicious node detection was done. The issue which was resolved due to its deployment was that if a cluster was very large then the Cluster head could not deliver the messages efficiently and if it was very small then the clusters may not be stable and thus re-affiliation took place. Secure and stable vehicular clustering based on weighted clustering algorithm worked on cluster creation and cluster maintenance. Communication cost for joining the cluster increased. It provided better ways of creating and maintaining clusters.

L. Virtual Forces Virtual Clustering:

The algorithm which was mentioned in [20] was virtual forces virtual clustering which was used to create stable clusters in an urban environment. Virtual clustering virtual forces not only took care of current positions but future positions also and their relative velocities also but only for those vehicles which keep their lane.

III. Comparative Analysis

In [5] clustering consisted of grouping of nodes whereas every cluster had a cluster head. The proposed solution i.e key management in ad hoc networks split the nodes into groups known as clusters. It used a threshold scheme to distribute the key in the cluster to achieve security of the cluster, and protection of the key against denial of service attacks. By applying this technique not only the certificates for the cluster heads are generated but also the nodes can join the new cluster heads by getting certificates from them. Inter and intra cluster authentication, integrity, confidentiality and non repudiation were achieved.

The aim of [6] was to achieve data integrity using three components which were monitoring routing cum forwarding, certificate renewal and certificate revocation. The routing cum forwarding scheme detected the problems with the routing

protocols and data; whereas, certificate renewal method by sending more than one shared key to the node guarantees the presence of original nodes in the network. Certificate revocation assured the removal of malicious nodes from the network. The certificate authority while approving certificates to the nodes mentions the node ID, initiation time and expiry time. These approaches altogether deployed in Shamir's Secret Sharing Model. Thus the integrity of data is achieved.

The problem highlighted in [11] due to the usage of centralized certification authority was solved by using decentralized scheme and thus a secret sharing scheme known as proactive secret sharing is used in ad hoc networks. In this technique secret keys changed periodically without changing the secrets, so it is difficult for the attacker to break the secret keys. A clustering technique was also mentioned in which all the nodes (cars) were divided into small clusters there were cluster heads and gateways. Gateways were also cluster heads but they were helpful in communicating between different clusters, whereas cluster heads were only responsible of maintaining communication among the nodes of the cluster. Cluster Heads had information regarding the different nodes and their actions within the clusters whereas Gateways also had information of other clusters too. To make clustering secure a private key was distributed among all the cluster heads by the certification authority and from cluster heads a public key was distributed among the nodes of the cluster. If a node found no cluster to be attached with it, it declares itself as a cluster. There was an inter network communication which is between different clusters and intra network communication which was among the network. In an intra network, an asymmetric communication is observed at cluster heads level but symmetric level communication was held between nodes of a cluster for making communication smoother and better. Apart from these the ways of merging the clusters, logging on of the nodes and routing strategies are also discussed. The advantages which were observed in this method were that the merging techniques of clusters were elaborated in a cost effective way. Secondly availability was enhanced because certificates could be issued even if some nodes were out of reach. The security infrastructure was more resistant to the intruders so integrity was achieved.

In [12] the author derived the trust formalization from watch dog and path rater used for grouping the nodes in ad hoc networks. In the evaluation of trust model the approaches used were namely, optimistic or greedy approach, simple average weighted products, weighted average and double weighted approach.

In [13] the resource hungry solutions of cryptography were eliminated by introducing the concept of secure message aggregation and onion signature. The technique for the symmetric group key distribution was secure VANETs Group Protocol. In this technique roads were divided into cells having a leader which distributes a public key to the nodes. The basic advantage of this was simplicity and robustness but the overhead that was produced left the large space for improvement. The grouping of vehicles was set geographically normally the range set was 300m when the vehicle (leader) moved out of the range, the election took place in the vehicle having lowest ID was declared as a leader, for the security purposes the IDs which vehicles generate were not their actual IDs instead they were pseudonyms. In the secure message aggregation technique several sort of signature methodologies were observed which includes combine signatures, concatenate signatures, onion signatures and hybrid signatures. In combine signatures to save time of data verification and cheated messages, the entire distributed signature from the group were combined to check the validity of the message and then sent to the group so that the combining of signatures was evidence that the message was verified and correct. In concatenated signatures a vehicle that received a correct message appended its signature with the already existing signatures and rebroadcasted the message. The message was then distributed over the group with the appended new signature with the already existing signature of each node that also eliminated data verification but could cause overhead. Another difficulty was to reduce the size of signature as the signature size was considered as constant. Therefore, the Onion signature strategy was deployed in which the vehicle only kept the signature of the last one which sent a message and on the next hop sent the message with its signature so the new vehicle which would receive its message would overwrite the message signature with its own and the process continued.

In [14] the basic parameters which were derived for deploying secure clustering algorithm were max value, min value, d-hop clusters, identity ID and weight these parameters were also involved in the election criteria. To elect the cluster heads several criteria were defined in secure clustering algorithm such as trust value in which it was analyzed how much any node could be trusted by its neighbors. Degree was another criteria which was defined in terms of specified radius, it was checked that whether a node with in a given radius servers maximum nodes or not. In battery power it was observed that for how much time a node could serve and the max value determined the cluster head which could handle more neighbors. Stability was decided on the basis of distance and average distance, distance between the two nodes tell the hops between the nodes and average distance checked the mean distance so by checking these parameters the most stable node as cluster head could be decided. Clusters heads regularly sent beacons to the nodes where the structure of beacon composed of cluster head certificate and the command which was assigned to the node by the cluster head. The election algorithm invoked when the nodes of a cluster needed to maintain their architecture so it required several stages such as discovery stage for selecting a node to participate in the election algorithm and the computed weight on the basis of which the node could be selected as a cluster head.

In the position based prioritized scheme [15], each node and cluster head was assigned a unique ID, node geographical location, and the ID of next node to whom it would communicate and the priority number of the node. So in that way a stable cluster structure came to its existence. If a cluster got out of the radio frequency area, it could join the new cluster on the basis of the attributes given to it. A special cluster head election algorithm was designed which told about the selection of new cluster heads under different situations. In MDS clustering algorithm the node which had a longer trip or

remained in travel longer could be declared as the cluster heads and that vehicle assigned the higher priority. To avoid the cluster heads loosing connectivity the cluster head had the authority to work as the cluster head until its velocity remained within the average speed otherwise the cluster would again calculate the priorities and chose a new cluster head.

In [16] a fully distributed public secret sharing key trusted model was applied which aimed to maintain a trust relationship in mobile ad hoc networks and prevented the network from the authorization of a malicious nodes without the involvement of any third party. For achieving the objective threshold cryptography was also included in the network. This technique generally included four basic operations namely initialization phase, joining the system, partial certificates creation and exchange and public key authentication. In the initialization phase the nodes get initialized with the inclusion of threshold cryptography. In the joining phase each node could enter or leave the system without any restriction. In the certification creation and exchange a private and public key was issued to the user if the public key belonged to the user, the user signed a certificate. In the public key authentication phase when the nodes needed to authenticate a public key of another node they merged their partial trust graphs according to the trust model.

In [17] dynamic demilitarized zone technique was a one hop from the certificate authority. Its goal was to register only known and trusted nodes whereas all the other nodes which were unknown and untrusted nodes would not be registered. So all the nodes which wanted to get registered would pass from dynamic demilitarized zone. All the trusted nodes would maintain a trust table in which the record of each trusted node would be maintained along with its public key. There were multiple certificate authorities involved in this algorithm each of which was responsible for its own geographical area. The road side units were also combined with the central certification authorities that worked as an intermediate between the central certification authorities and dynamic certification authority on the road. There was a trust matrix defined in which for untrusted node the value of Tm=0.1 and for trusted node = 1. Registration Authority was responsible to act as a Dynamic demilitarized zone as it checked the level of trust of each node and then moved that node to get signed certificate. A Sub cluster head was responsible to create communication between many clusters. If a node left a cluster, the Sub cluster head was responsible for adding that node into another cluster on the basis of its trust level. In [21] a concept of dynamic key distribution was observed in which there were multiple central certificate authorities present at their respective geographical areas and an asymmetric key distribution algorithm was used. All the vehicles had to pass from VANET dynamic demilitarized zone to request a certificate from a certificate authority. Its additional feature was that each vehicle which was at 1-hop from other vehicles sent hello messages as result the nodes which received this message saved each and every record of the vehicle and thus respond with a joint message to that node. Hello messages were also used during election algorithm.

In [18] there was a global Certificate authority and a local Certificate authority. The global Certificate authority was responsible for issuing certificates if different clusters wanted to communicate with each other whereas local Certificate authority was responsible for issuing certificates with in the cluster for proper communication. They used symmetric key distribution algorithm along with many protocols such as cluster management protocol, cluster head designation protocol and cost delivery protocol. However, the biggest risk of deploying this technique was that according to this supposition all the data was considered to be correct and authenticated.

In [19] three algorithms were introduced; the first one was the vehicular clustering based on weighted clustering. Some parameters were needed to be set while deploying this technique. T_d was set as distrust value and sigma was the threshold. Two lists were maintained by the vehicles if the T_d value of the vehicles was less than the threshold then they were maintained in the white list and if T_d value was greater than they were sent in black list. The copy of black list was sent to all the nodes and clusters that came under the area of particular Certificate authority. For each vehicle setting itself as a cluster head sent its user name and ID to all the nodes. On the basis of certain criteria the node could declare itself as a Cluster head. The criteria could be decided by performing five steps mentioned in [19]. Another algorithm was the adaptive allocation of transmission range algorithm which catered to the problem where sometimes messages cannot transfer to their neighbors on time due to topology changes or variable frequency. Thus through the application of this algorithm, the vehicles could find their neighbors dynamically. This algorithm also involved three steps mentioned in [22]. The third and last algorithm was monitoring of malicious vehicles. This algorithm would simply monitor the abnormal vehicle and cater out its abnormality factor. The algorithm mentioned in [22] named as Secure and stable vehicular clustering based on weighted clustering algorithm was similar to that mentioned in [19]. But the issue which was resolved due to its deployment was that if a cluster is very large then the Cluster head could not deliver the messages efficiently and if it was very small then the clusters might not be stable and thus re-affiliation took place. Secure and stable vehicular clustering based on weighted clustering algorithm worked on cluster creation and cluster maintenance.

The Virtual clustering vehicle forces [20] applied Coulomb's law to assign the virtual forces to the network; vehicles were considered as charged particles, and force was applied on the vehicles which needed to be communicating on the basis of relative velocity and distances. When vehicles moved away from each other, they gave negative force and vice versa. "$\mathbf{F_{rel}=k\ q_i q_j / r^2_{ij}}$", the charge of every vehicle was proportional to many parameters of that vehicle. 'r' was the distance, q_i q_j are the vehicles at certain directions and k depends on the factors present in the equation.

Table 1 mentioned below shows the brief comparison of the related works and comparative analysis.

TABLE I. COMPARATIVE ANALYSIS OF VANET TECHNIQUES

R. No	Technique	Availability	Confidentiality	Integrity	Non repudiation	Authentication
[7]	Public key Infrastructure & threshold cryptography	Decrease	Increase	Increase	Increase	Increase
[8]	Shamir's secret scheme	Increase	Medium	Increase	Increase	Increase
[13]	Proactive Secret sharing	Increase	Increase	Increase	Medium	Increase
[14]	Trust based model	Decrease	Medium	Medium	Increase	Increase
[15]	Secure VANET group protocol	Decrease	Medium	Increase	Increase	Increase
[16]	Secure clustering algorithm	Increase	Medium	Medium	Increase	Medium
[17]	Position based prioritized clustering, MDS	Increase	Decrease	Decrease	Decrease	Decrease
[18]	Fully distributed trust based model	Decrease	Medium	Medium	Increase	Increase
[19]	Dynamic demilitarized zone	Decrease	Medium	Medium	Increase	Increase
[20]	Distribution algorithm	Decrease	Medium	Increase	Medium	Increase
[21]	Vehicular clustering based on weighted clustering	Increase	Increase	Decrease	Increase	Increase
[22]	Coulomb's Law	Increase	Decrease	Decrease	Decrease	Decrease
[23]	VANET dynamic demilitarized zone	Increase	Increase	Medium	Medium	Increase
[24]	Secure and stable vehicular clustering based on weighted clustering algorithm	Increase	Medium	Medium	Medium	Increase

IV. CONCLUSION & FUTURE WORK

A. Conclusion

In summary, secure clustering can efficiently support a wide variety of applications that are characterized by a close degree of collaboration, typical for many VANETs. And the design of the secure clustering algorithms are driven by specific goals and requirements based on respective assumptions about the network properties or application areas.

This paper presents a comprehensive survey of the secure clustering techniques for VANETs. The purpose of this paper is to survey the secure clustering techniques and study their primary principles. It discuss the characteristics, security properties of each of these clusters selected from the class of similar approaches, which can reflect the state of- the-art research work on secure clustering techniques. The classifications of the primary secure clustering principles can simplify the task of a network designer in deciding the clustering strategies to be adopted at a given condition.

Then, it is believed that this survey will be very useful to the research community and also serve as a great introductory material for someone embarking on VANETs.

B. Future Proposition

As mentioned earlier, research in the area of secure clustering algorithms over VANETs is far from comprehensive. Much of the effort so far has been on devising secure clustering techniques to support effective and efficient communication between nodes that are part of a same group. However, there are still many topics that deserve related to security while clustering the VANETs.

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, 2003, 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

[4] Drs. Baruch Awerbuch and Amitabh Mishra: Introduction to Ad hoc Networks, CS-647: Advanced Topics in Wireless Networks, 2008

[5] Mohamed Elhoucine Elhdhili, Lamia Ben Azzouz and Farouk Kamoun: A Totally Distributed Cluster Based Key Management Model for Ad hoc Networks

[6] 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

[7] 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

[8] Marc Torrent-Moreno, Jens Mittag, Paolo Santi, and Hannes Hartenstein: Vehicle-to-Vehicle Communication FairTransmit Power Control, Vehicular Technology, IEEE Transactions, Volume:58, pages 3684 – 3703, 2009

[9] 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

[10] Sanaz Sadeghi and Behrouz Sadeghi: Designing Secure Clustering Protocol With The Approach Of Reducing Energy Consumption In Wireless Sensor Networks, The International Journal of Computer Networks & Communications (IJCNC), Volume 5, 2013

[11] M. Bechler, H.-J. Hofi, D. Kraftt, E Pmket and L. Wolf: A Cluster-Based Security Architecture for Ad Hoc Networks, Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Volume 4, pages 2393 – 2403, 2004

[12] Mohit Virendra, Murtuza Jadliwala, Madhusudhanan Chandrasekaran and Shambhu Upadhyaya: Quantifying Trust in Mobile Ad-Hoc Networks, Integration of Knowledge Intensive Multi-Agent Systems, 2005, International Conference, pages 65-70, 2005

[3] Lidong Zhou, Zygmunt J. Haas and Cornell: Securing Ad Hoc Networks, Network, IEEE, Volume 13, pages 24 – 30, 1999

[13] Maxim Raya, Adel Aziz and Jean-Pierre: Efficient Secure Aggregation in VANETs, Proceedings of the 3rd international workshop on Vehicular ad hoc networks, Pages 67-75, 2006

[14] B. Kadri, A. M'hamed, M. Feham: Secured Clustering Algorithm for Mobile Ad Hoc Networks, IJCSNS International Journal of Computer Science and Network Security, volume 7, pages 27-34, 2007

[15] Zhigang Wang, Lichuan Liu, MengChu Zhou and Nirwan Ansari: A Position-Based Clustering Technique for Ad Hoc Intervehicle Communication, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions, Volume 38, pages 201 – 208, 2008

[16] Mawloud Omar, Yacine Challal, and Abdelmadjid Bouabdallah: Fully Distributed Trust Model based on Trust Graph for Mobile Ad hoc Networks, Published in Computers & Security, 2009

[17] Tahani Gazdar, Abdelfettah Belghith and Abderrahim Benslimane: A cluster based secure architecture for vehicular ad hoc networks, Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference, pages 1 – 8, 2010

[18] Helena Rifà-Pous, Jordi Herrera-Joancomartí: A Fair and Secure Cluster Formation Process for Ad Hoc Networks, Journal Wireless Personal Communications, volume 56, pages 625-636, 2011

[19] Ameneh Daeinabi, Akbar Ghaffar Pour Rahbar and Ahmad Khademzadeh: VWCA: An efficient clustering algorithm in vehicular ad hoc networks, Journal of Network and Computer Applications, Volume 34, Pages 207–222, 2011

[20] Leandros A. Maglaras: Clustering in Urban environments, Virtual forces applied to vehicles. Communications Workshops (ICC), 2013 IEEE International Conference, pages 484 – 488, 2013

[21] Tahani Gazdar, Abderrahim Benslimane, Abdelfettah Belghith and Abderrezak Rachedi: A secure cluster-based architecture for certificates management in vehicular networks, 2013.

[22] Ankit Temurnikar, Dr.Sanjeev Sharma and RGPV Bhopal: Secure and Stable VANET Architecture, Journal IJCSN publisher, volume 2, pages 37-43, 2013.