European Journal of Scientific Research
ISSN 1450-216X Vol.36 No.2 (2009), pp.299-307
© EuroJournals Publishing, Inc. 2009
http://www.eurojournals.com/ejsr.htm

Authentic Vehicular Environment Using a Cluster Based Key Management

S. Sivagurunathan
Department of Computer Applications
Thiagarajar College of Engineering, Madurai, India
E-mail: ssncse@tce.edu, sivaguruns@yahoo.co.in

P. Subathra
Department of CSE
Thiagarajar College of Engineering, Madurai, India

V. Mohan
Department of Mathematics
Thiagarajar College of Engineering, Madurai, India

N. Ramaraj
GKM College of Engineering, Chennai, India

Abstract

Security has become a prime concern in providing communication between mobile nodes in a hostile environment. Unlike wired networks, the unique characteristics of Vehicular Ad Hoc Networks (VANETs) pose a number of non-trivial challenges to security design. This paper presents a self organized public key management mechanism with a mobility based Clustering for Open Inter Vehicle Communication Networks (COIN). Nodes that have similar moving pattern are grouped into a cluster. Unlike other clustering algorithms, the diameter of clusters is not restricted to two hops. Instead, the diameters of clusters are flexible and determined by the stability of clusters. The stability of clusters is estimated based on relative mobility of cluster members. In this paper we have proposed an on demand self-organized, public key management for VANETs based on the existence of a web of trust between the vehicles forming the network. This web of trust mechanism works on top of the cluster to provide secure routing service.

Keywords: Mobility, Clustering, Key Management, Vehicular ad-hoc networks

1. Introduction

Mobile Ad-Hoc Network(MANET) is one where there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless means, while that are those far apart rely on other nodes to act as routers to relay its messages[8]. Vehicular Ad-Hoc Network (VANET) is an important application of MANET [27]. The main difference is that the mobile routers building the network are vehicles like cars or trucks(26). The main goal of VANET is to share routing information and increase road safety. To achieve this goal the vehicles act as sensors and inform each other the abnormal and potentially hazardous traffic conditions (25).This helps the drivers to react and prepare against sudden traffic events in advance. Vehicles can also drive collaboratively to speed up the flow of traffic. This paper provides an easy way for vehicle assisted secure information exchange without any additional roadside infrastructure and special technologies.

The fundamental vulnerability of VANET comes from open peer to peer architecture. Unlike wired networks that have dedicated routers, each vehicle in VANET may function as a router and forwards packets to other nodes. The wireless channel is accessible to both legitimate network users and attackers. The attack may range from passive eavesdropping to active impersonation. Since compromising a vehicle is possible, trust relationship among them is very important in case of co-operative driving. As a result there is no clear line of defense in VANETs from the security design perspective. The salient features of VANETs pose both challenges and opportunities in achieving the above security goals. Apart from routing the messages exchanged in VANET also influence the behaviour of the drivers. Depending on the information they get, they will. e.g., drive very carefully, and slowly in case of a glaze warning or choose an alternate route in the case they are informed about the traffic jam on their desired route. Adversaries could exploit this by injecting wrong messages and slowing down traffic or getting a vehicle free road. To prevent this kind of misuse security is very important in VANETs(25).

In this paper section 2 elaborates the state of the art techniques adopted for clustering and security. Section 3 throws light on the mobility based clustering algorithm for VANET. Section 4 deals with routing security and section 5 discusses the key management service and the system model and finally Section 6 concludes the paper with future scope.

2. Background Work

Every vehicle (node) in the VANET has to rely upon the other vehicles for routing their packets. The need to store complete routing details for an entire network topology raises scalability issue. The flat hierarchy adopted by most of the existing VANET routing protocols may not be able to support the routing function efficiently, since their routing tables can grow to an immense size, if each vehicle has a complete view of the network topology. Therefore, clustering algorithm is proposed in VANETs to address scalability issues.

Clustering algorithms can be performed dynamically to adapt to node mobility [14,21], VANET is dynamically organized into groups called clusters to maintain a relatively stable effective topology [13]. By organizing vehicles into clusters, topology information can be aggregated.

We make the following observations that motivate the group concept applied in our solution:

1. Vehicles in geographical proximity often share redundant information such as road and traffic conditions.
2. The mobility of the vehicles is spatially restricted and spatially dependent. Hence, vehicles in geographical proximity can navigate as a group, with the same average velocity, due to the spatial dependency, and with similar direction due to the spatial restrictions over a period of time.

We make use of these observations , and propose to enable vehicles to form cluster. Clustering algorithm in VANETs should be able to maintain its cluster structure as stable as possible while the topology changes[4,15]. Since vehicles in a cluster will move relative to each other, and on average have the same velocity, a group can be represented by a single vehicle that we refer to as the *clusterhead*. This is a mobility based clustering algorithm that forms clusters based on mobility, suggested in [2]. The formation of the clusters is determined by the mobility pattern of vehicles to ensure maximum cluster stability[8]. It has been observed that vehicles in VANET may move in groups. This is known as group mobility [9]. Hence, mobility based clustering would be a better option than the other available clustering algorithms [10,16,18,19,24].

We partition VANET into a number of clusters. In each cluster, exactly one distinguished node the cluster head (CH) - is responsible for establishing and organizing the cluster. Gateways (GWs, which need not necessarily be CHs) manage communication with adjacent clusters. The CHs are responsible for sending CH beacons in their clusters, containing administrative information for the cluster members, e.g., list of vehicles and GWs in the cluster. Also, GWs periodically transmit GW beacons to inform their respective clusters about adjacent clusters. Routing is then typically divided in to two parts: routing within a cluster (intra-cluster) and routing between different clusters (inter-cluster). In case no clusters are given from outside the security part, they are formed as needed: Nodes finding no existing clusters create some themselves, and existing clusters are merged and split on demand.

The trust relationships established between vehicles forming the network could be used for the provision of higher level security solutions, such as key management. In [1], and [5], threshold cryptography has been proposed to provide a reliable, distributive key management for MANET by exploiting some nodes as a trust anchor for the rest of the network. In these schemes, threshold cryptography involves additional computationally intensive modular exponentiation compared to the underlined asymmetric-key cryptographic protocols. Most low-powered wireless nodes do not have the resources to handle such computationally intensive operations. Capkun et al. in [6] proposed a self-organized public key management scheme in which each node issues certificates independently and manages them at its repository. In this scheme, Certificates are stored and distributed by the nodes and each node maintains a local certificate repository that contains a limited number of certificates selected by the node according to an appropriate algorithm. Key authentication is performed via chains of certificates. However, this scheme suffers from the delay and the large amount of traffic required to collect certificates. Ren et al. in [7] proposed a distributed trust model based on introducing a secret dealer to accomplish trust initialization in the system bootstrapping phase to overcome the problem of delayed trust establishment appeared in [6]. In this scheme a secret dealer provides each node with a secret short list that includes a number of entries, each entry contains a binding of node identifier and its corresponding public key: (*ID*, *Pk*). After receiving the short list, each node starts to issue certificates for the received bindings and store them locally. The existence of the secret dealer makes the scheme prone to the centralized administration problems. For example, it has a single point of attack because if the secret dealer is compromised during the bootstrapping phase, the security of the whole system will be at risk. Kitada et al. in [12], and [17] considered the problem of certificate chain discovery by introducing the Ad hoc Simultaneous Nodes Search protocol (ASNS) to find a certificate chain. In the proposed scheme by Kitada et al., each node holds in its local repository only certificates issued to it in order to reduce the memory size and collects certificates by broadcasting search packets to chained nodes. The scheme suffers from high communication cost because of broadcasting packets with certificates. Li et al in [20] proposed a public key management scheme performed by generating a public/private key pair by the node itself, issuing certificates to neighboring nodes, holding these certificates in its certificate repository. This scheme considers only the updated certificate repository to reduce the number of certificates stored in its certificate repository. Hisham Dahshan et al in [23] proposed another public key management scheme using web of trust. In this paper, we propose an on demand self-organized public key management for VANETs. The proposed scheme is based on the existence of a web of trust between mobile nodes forming the network. The proposed scheme allows each user to create its public key and the corresponding private key, to issue certificates to neighboring nodes, within the same cluster and to perform public key authentication without relying on any centralized authority. The certificate chain discovery will be performed with the aid of the routing process.Thereby it can maintain the secrecy of the information exchanged. The novelty in the approach is the implementation of self organized public key management combined with mobility based clustering algorithm for VANET.

3. Clustering for Open Inter vehicle communication Networks (COIN)

The generic MANET algorithms have been tested under random nodal mobility, which does not reflect vehicular movement. Vehicular mobility is highly constrained by the layout of road network, by traffic control devices, and by surrounding vehicles. Vehicle movement is characterized by high rates of speed, producing very high relative velocities. Driver behavior has a significant impact of mobility patterns both in the near term and in the long term. In the near term, vehicle movements vary very dramatically based on individual lane changing, braking, and passing behaviors. In the long term, mobility is affected by the variations in the intended destination of a driver. Since they do address vehicular mobility, previous MANET clustering approaches have limited applicability for inter-vehicle networks. Even the clustering algorithms that consider nodal mobility produce unstable clusters [9].

Ideally, the relative mobility between a cluster head and a member node should be low, so that they remain in radio contact as long as possible. Low mobility nodes will often have a very high relative mobility with nearby vehicles and therefore fleeting radio contact. Consider a car that is parked, but idling. It will have lower mobility than the vehicles passing it, but it is an unsuitable cluster head because the cluster membership will not be stable. Similarly, if there is stop and go traffic on one side of a highway, free moving nodes on the other side should not choose these low mobility nodes as cluster heads.

However, the use of previous observations of low relative mobility will not necessarily yield a stable clustering. Consider two vehicles that have traveled together on the same road for some time. One of the vehicles merges into the exit lane. Here the driver’s intention to exit conveys much more information about their future relative mobility, than the previous observations of this value.

Finally, IVC clustering stability will degrade with the requirements that no two cluster heads communicate with one another and that all nodes be in constant radio communication with their-cluster heads. The distances between vehicles with low relative mobility will often exhibit oscillatory behavior. Examples of this phenomenon can be found in stop and go traffic; as vehicles pass through four-way stop signs, or as vehicles slow to navigate curves in the roadway.

In an attempt to build more stable clusters, this algorithm COIN extends previous work in MANET clustering and seeks to address these limitations. Like the previous algorithms, it attempts to preserve cluster head election and uses mobility information for clustering. One of the contributions of the algorithm is its use of driver intentions as input to the clustering algorithm. Furthermore, to accommodate oscillatory inter-vehicle distance, the algorithm allows for limited situations in which radio links can exist between cluster heads.

4. Secure Routing

To achieve availability, routing protocols should be robust against dynamically changing topology and malicious attacks. Routing protocols proposed for MANET cope well with the dynamically changing topology [10, 16, 18, 19]. However, none of them seem to have accommodated mechanisms to defend against malicious attacks. There is no single standard routing protocol that addresses this issue. Hence, the aim is to capture the common security threats and to provide guidelines to secure routing protocol.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information or distorting routing information, an attacker could successfully partition the network or introduce excessive traffic load into the network. The second and also the most sever kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult. Merely requiring routing information to be signed by each node would not work because compromised nodes are able to generate valid signatures using their private keys.

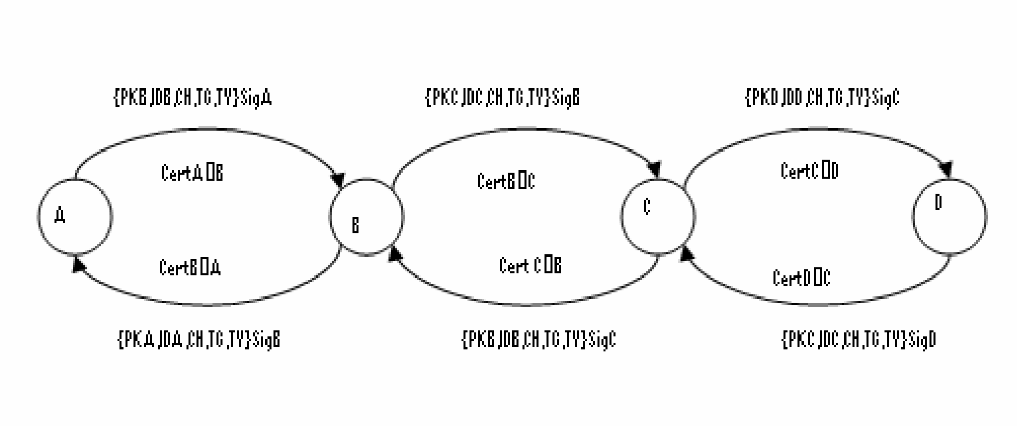
Detection of compromised nodes through routing information is also difficult in MANET because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases.

5. Key Management System Description

Trust Model

The trust model of our proposed scheme is based on the existence of public-key certificates as bindings of the public keys and the corresponding user identities *IDs*. The certificate should also contain the node's identity/network address, certificate generation and validity dates. We denote *CertA→B* as the certificate signed by node *A*'s private key *SKA* to represent its assurance in the binding of node *B* and its public key *PKB*. For simplicity we denote *Sigi* as the digital signature of node *i*. It is assumed that there exist sparse trust relationships among the nodes so that any node that wishes to join the network can establish independent trust relationship with some of the existing member nodes in the network. Each node in the network has a certificate repository to store valid certificates it issued or certificates issued to it by other entities. In order for a node *A* to authenticate the public-key of another node *D* as shown in Figure 1, it has to acquire a chain of valid certificates from node *A* to node *D*. The first certificate of the chain which is the certificate of a directly trusted node by node *A* will be verified by node *A*, by using its public key *PKA*. Each remaining certificate in the chain will be verified using the public key of the previous certificate of the chain. The last certificate in the chain holds the public key of the target node *D*. The certificate chain from node *A* to node *D* in this example is *{CertA→B, CertB→C, CertC→D}*, and the certificate chain from node *D* to node *A* is *{CertD→C, CertC→B, CertB→A}*.

Figure 1: Certificate Chain


{PKB ,IDB ,CH ,TG ,TV}SigA
{PKC ,IDC ,CH ,TG ,TV}SigB
{PKD ,IDD ,CH ,TG ,TV}SigC
CertA □B
CertB □C
CertC □D
A
B
C
D
CertB □A
Cert C □B
CertD □C
{PKA ,IDA ,CH ,TG ,TV}SigB
{PKB ,IDB ,CH ,TG ,TV}SigC
{PKC ,IDC ,CH ,TG ,TV}SigD

System Description

The proposed on demand self-organized public key management scheme involves four processes: public key and public key certificate generation, certificate chain discovery, certificate verification, and certificate revocation. We describe our proposed scheme in detail according to these four processes.

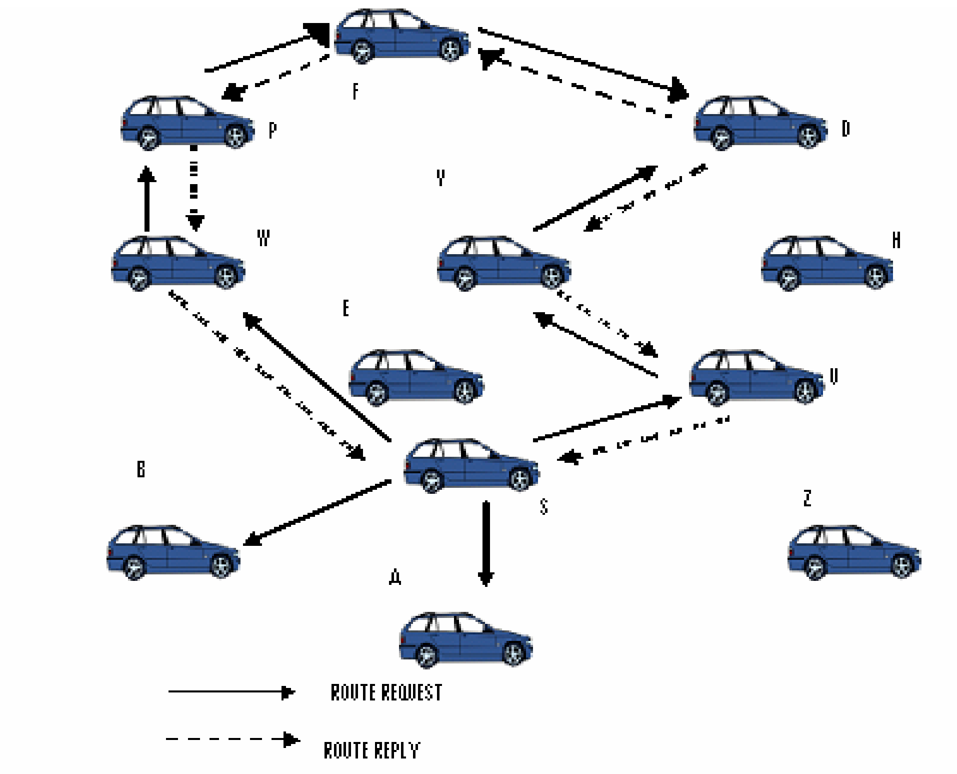
1. Public Key and Public-Key Certificate Generation

In our proposed scheme, each node generates its public key and the corresponding private key locally before joining the network by the node itself. Public-key certificates are issued by the nodes based on nodes information about other nodes in the network. If a node *u* believes that a public key *PKi* belongs to a certain user *i*, it has to issue a certificate to node *i* signed by its private key *PKu* representing its assurance of the binding of the user's identity *IDi* and its corresponding public key *PKi*. Issued certificates to or from the user should be stored in its certificate repository with a validity time.

2. Certificate Chain Discovery

In this process, the certificate chain discovery is performed by exploiting the routing infrastructure. We assume that a certain number of direct trust relations have been established between each node and its neighbors during the network initialization. The number of directly trusted nodes per node is assumed to be uniformly distributed. The proposed on demand self-organized public key management scheme work in support of an ad hoc on demand routing protocol (such as AODV [8]). Considering the example in Figure 2, the certificate chain discovery process can be explained as follows:

Figure 2: Certificate Chain Discovery



- The source node *S* sends a route request packet to nodes that the source node directly trusts.
- When a directly trusted node by the source node (such as node *U*) receives the route request packet from the source node, it searches for the certificate of the source node signed by this node in its certificate repository and adds it to the route request packet before forwarding the route request packet to nodes it directly trusts as shown in the following message.
- *U→V : {RREQ,CertU→S}*
- As node *V* directly trusts the destination node *D*, it will do the same as node *U* and forwards the following message to the destination node *D*.
- *V→D : {RREQ,CertU→S, CertV→U}*
- After receiving the route request packet from node *V*, the destination node *D* has the whole certificate chain required to recover the source node's public key PK_S.
- The destination node *D* sends a route reply packet to node *V*.
- Node *V* searches in its certificate repository for the certificate of the destination node *CertV→D* , adds it to the route reply packet, and forwards the route reply packet to node *U* as shown in the following message.
- *V →U :{RREP, CertV→D}*
- Node *U* receives the route reply packet from node *V*, searches for the certificate of node *V* *CertU*

- *V* in its certificate repository, adds it to the route reply packet, and forwards the route reply packet to the source node *S* as shown in the following message.
- *U →S :{RREP, CertV→D, CertU→V }*
- The source node *S* receives the route reply packet from node *U* and recovers the public key of the destination node *PKD* from the received certificate chain. If the source node received more than one route reply for the same route request, it will choose the route which has the minimum number of certificates. Un trusted nodes such as nodes *E*, *H*, and *Z* will not receive the route request packets.
- Successful communication result in increasing trust between certificate chain entities and signing more certificates for each others.

3. Cluster Head Identification

In this scheme, the Id of the cluster head CH is encrypted as part of the signature to identify the membership of the node in the existing cluster. It helps us in ensuring the identity and to share the intra cluster routing information.

4. Public-Key Certificate Verification

The verification of the public-key certificate is performed by checking the validity time *Tv* in the certificates forming the certificate chain. After verifying the certificates of the certificate chain the authenticity of the public keys of both the source and the destination nodes is performed by the certificate chain from the source node to the destination node and vice versa.

5. Public-Key Certificate Revocation

Each node can revoke a certificate it issued if it believes that the binding between the public key and the node’s identity is no longer valid. Each node can revoke its own certificate if it believes that its private key is compromised. A node can revoke a certificate it issued by broadcasting a certificate revocation message to nodes it directly trusts. When a node receives a certificate revocation message, it deletes the revoked certificate from its certificate repository. A node can revoke its own certificate by broadcasting a certificate revocation message to nodes it directly trusts includes the revoked certificate and the new one. When a node receives the certificate revocation message it replaces the revoked certificate by the new one.

6. Conclusion and Future Research Scope

In this paper, we have presented a security solution for VANET using self organized public key management combined with the clustering. To achieve the scalability COIN is used and it forms variable-diameter clusters, which allows cluster members to be more than two hops away from their cluster head. The diameter of clusters is dependent on the mobility behavior of vehicles in the same cluster. As long as the nodes are moving towards the same direction, they can be grouped into the same cluster. This is justified by the assumption of group movement, in which the members of a group tend to move towards a same destination in real life scenarios. This paper also provides a mechanism for performing secure routing and establishing a secure key management service in a VANET. To build a highly available and secure key management service, a self organized public key management scheme is being proposed. The idea of using the self organized public key management combined with mobility based clustering schemes is worth examining further by varying the parameters further, to establish its full potential..

References

[1] L.Zhou and Z.J. Hass,1999, “Securing ad hoc network”, IEEE network, Vol.13., no.6, pp.24-30.

[2] P. Basu, N. Khan and T. D. C. Little, 2001, “Mobility based metric for Clustering in Mobile Adhoc Networks”, IEEE ICDCSW’01, Pages: 413-418.

[3] Emanuel Fonseca, Andreas Festag, 2006, “ A Survey of Existing Approaches for Secure Ad Hoc Routing and TTheir Applicability to VANETS”, NEC Technical Report NLE-PR-2006-19, NEC Network Laboratories.

[4] Charalampos Konstantopoulos, Damianos Gavalas,Grammati Pantziou, 2008, “Clustering in mobile ad hoc networks through neighborhood stability-based mobility prediction”, Elsevier.

[5] S.Yi and R. Kravets, 2003, “ Moca: Mobile certificate authority for wireless ad hoc networks”, in Proceedings of the 2nd Annual PKI Research Workshop (PKI 2003).

[6] S.Capkun, L.Buttyan , and J.-P. Hubaux, 2003, “ Self-organized public – key management for mobile ad hoc networks”, IEEE Transactions on Mobile Computing, vol. 2., no.1, pp.52-64.

[7] K.Ren, T. Lib, Z.Wanb, F.Baob, R.H.Dengb, and K.Kima, 2004, “Highly reliable trust establishment scheme in ad hoc networks”, The International Journal of Computer and Telecommunications Networking, ElSEVIER . Vol.45, no.6, pp.687-699.

[8] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, 2004, “Security in mobile Ad-Hoc networks- Challenges and Solutions”, IEEE Transactions On Wireless Communications.

[9] Jeremy Blum, Azim Eskandarian and Lance Hoffman, 2003, “ Mobility management in IVC Networks “Intelligent VehiclesSymposium,2003.Proceedings of IEEE Volume , Issue , 9-11 Page(s): 150 – 155.

[10] B. Das, and V.Bharghavan , 1997, “ Routing in Ad-Hoc networks using Minimum Connected Dominating Sets” , in Proc. IEEE ICC’97, pp.376-80.

[11] B.Parno, and A.Perrig, 2005, “Challenges in Securing Vehicular Networks”, In Proceedings of ACM workshop on Hot Topics in Networks(HotNets-t), page 6, College Park, MD, USA.

[12] Y.Kitada, Y. Arakawa, 2005, “On demand distributed public key management using routing information for wireless ad hoc networks”, IEICE Transactions on Information and Systems, vol. J88 D1 no. 10, pp. 1571-1583.

[13] C.R. Lin and M. Gerla, 1997, “Adaptive clustering for mobile wireless networks”, IEEE Journal on Selected Areas in Communications, 15(7): 1265-1275.

[14] A.B. McDonald and T.F. Znati, 1999, “A mobility-based framework for adaptive clustering in wireless ad hoc networks”, IEEE Journal on Selected Areas in Communications, 17 (18): 1466-1486.

[15] Martha Steenstrup, Bolt Beranek, Newman, 2001, “Cluster-based networks” in Ad hoc networking, C.E. Perklins, Addison Wesley.

[16] T.J.Kwon et al., 2003, “Efficient Flooding with Passive Clustering – and Overhead - Free Selective Forward Mechanism for Ad-Hoc/Sensor Networks”, in Proc. IEEE Vol.91, no.8, pp.1210-20.

[17] Y.Kitada, A. Watanabe, K. Takemori, and I.Sasase, 2005, “ On demand distributed public key management for wireless ad hoc networks”, in IEEE Pacific Rim Conference on Communications, Computers and Sinal Processing (PacRim).

[18] J.Gomez et al., 2003, “PARO: Supporting Dynamic Power Controlled routing in Wireless Ad Hoce Networks” Wireless Networks , Vol. 9, pp. 443-60.

[19] T.Ohta,, S. Inoue, and Y.Kakuda, Apr.2003, “ An Adaptive Multihop clustering Scheme for Highly Mobile Ad Hoc Networks”, in Proc. 6th ISADS’03.

[20] H.K.R. Li, J. Li, and P.Liu, 2004, “ Localized public key management for mobile ad hoc networks”, in IEEE Global Telecommunications Conference (Glomocom), pp. 1284-1289.

[21] Sung-Ju Lee,William Su and Mario Gerla, 1999, "Ad hoc Wireless Multicast with Mobility Prediction", Proceedings of IEEE ICCCN'99, Boston, MA.

[22] C.E. Perkins and E.M. Royer, 1999, “ Ad-hoc on demand distance vector routing”, in 2nd IEEE Workshop on Selected Areas in Communication, New Orleans, LA, pp. 24-30.

[23] Hisham Dahshan, James Irvine, 2009, "Key Management in Web of Trust for Mobile Ad Hoc Networks," aina, pp.363- 370, 2009 International Conference on Advanced Information Networking and Applications.

[24] P.Subathra, S.Sivagurunathan, G.S.R.EmilSelvan, 2006, ”Securing Mobile Ad-Hoc Networks through AntTree Clustering and Threshold Cryptography”, In Proceedings of the ISAHUC, NITK, Surathkal, pp: 48-51.

[25] Klaus Plobi, Thomas Nowey, Christian Mletzko, 2006, “ Towards a Security Architecture for Vehicular Ad Hoc Networks” Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on Volume , Issue , 20-22 , Page(s): 8 pp. –

[26] Soyoung Park and Cliff C.Zou “ Reliable Traffic Information Propagation in Vehicular Ad-Hoc Networks” *Security in Ad Hoc and Sensor Networks*, to be published by World Scientific Publishing, Inc

[27] J.Munoz and N.Syracuse,2002, Proceedings of the 53rd internet engineering task force.