

Security Issues & Clustering Based Solutions in Mobile Ad-hoc Networks - A Survey

Sandeep Kr. Agarwal

Department of Computer Applications
Bharat Institute of Technology, Meerut (U.P.)
Email: bit.sandeep@gmail.com

Amit Garg

Department of Computer Applications
Meerut Institute of Engineering & Technology, Meerut (U.P.)
Email: foramitgarg@gmail.com

K. V. Arya

Department of Information Technology
ABV-Indian Institute of Information Technology & Management (IIITM), Gwalior

(Received December 22, 2011)

Abstract: Mobile Ad-hoc Network (MANET) is a new type of communication network, which can be used for data communication between groups of mobile nodes using wireless channels. The nodes in MANET act as host as well as router and hence, they are responsible for dynamically discovering other nodes for forwarding packets to their destination. In multi hop ad-hoc environment, it is difficult to maintain routes due to the mobility of intermediate nodes, nature of radio communication etc. In the absence of an authentication based security mechanism, malicious nodes can easily corrupt routing tables, caches and other network management information. It has been observed that the wireless MANETs face a larger security problem than conventional wired and wireless networks.

Clustering has been evolved as an important research topic in the area of MANETs. A cluster based approach for ad-hoc network in a large region enables mobile node management, security, fault tolerance, network key management and routing. In MANETs, clustering based routing schemes are used to reduce channel contention in large networks. Implementation of a secured routing protocol among the nodes of a MANET, while keeping intact the benefits of clustering, is a tough task.

In this paper, we are discussing the various security issues and their current solutions, especially the clustering based solutions in the Mobile Ad-hoc network. Initially the main vulnerabilities in the Mobile ad-hoc networks are analyzed, which have made it much easier to suffer from

attacks. Then the security criteria of the Mobile ad-hoc networks and the main attack types that exist in it are represented. Finally we are summarizing the present clustering based security solutions for the Mobile ad-hoc networks.

Keywords: MANET, Security, Clustering, Authentication, Intrusion Detection

1. Introduction

The use of wireless communication among mobile users is becoming increasingly popular due to recent advancements in computer and wireless technologies. There are two distinct approaches for enabling wireless communications between mobile hosts. The first approach is to use a fixed network infrastructure with wireless access points. Another approach is to form an ad-hoc network among mobile devices wishing to communicate with each other. All the nodes of these networks behave as routers and take part in discovery and maintenance of routes. This form of networks is limited in range, node mobility, security of data, lack of proper communication and limited bandwidth. However, advantages of ad-hoc networks over traditional cellular systems include 'on-demand' setup, fault tolerance, and unconstrained connectivity.

Mobile Ad-hoc Network (MANET) is a new type of communication network, which can be used for data communication between groups of mobile nodes, which are highly mobile and dynamically join and leave the network using wireless channels²⁰. Some typical features of the Mobile ad-hoc network are as following¹⁷:

- Nodes in the MANET exhibit dynamic behavior by freely migrating within some area, dynamically creating and breaking associations with other nodes. Nodes can communicate with each other at any time and without restrictions. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes are not consistent.
- Mobile ad-hoc networks are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links. The nodes are free to move anywhere randomly and organize them arbitrarily. This may result in rapid and unpredictable changes in topology such as route changes, frequent network partitions, and may cause packet losses.
- Within a MANET, there can be significant variations in speed, direction, or restrictions on paths. In spite of such volatility, the MANET is expected to deliver diverse traffic types.
- MANET does not depend on any established infrastructure or centralized administration. Each node operates in distributed peer-to-

peer mode, acts as an independent router and generates independent data. Network management has to be distributed across different nodes, which brings added difficulty in fault detection and management.

The various challenges reported in literature²⁸ include energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes etc. In the absence of an authentication based security mechanism, malicious nodes can easily corrupt routing tables, caches and other network management information². Recent wireless researches indicate that the wireless MANETs face a larger security problem than conventional wired and wireless networks. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability⁶.

2. Vulnerabilities of the Mobile Ad-hoc Networks

a. Lack of Centralized Management

The absence of centralized management makes the detection of attacks a very difficult problem due to highly dynamic nature of ad-hoc networks⁷. Second, lack of centralized management will obstruct the trust management for the nodes in the ad-hoc network¹⁷. Third, some algorithms in the Mobile ad-hoc network rely on the cooperative participation of all nodes and the infrastructure. In absence of a centralized authority, the adversary can perform some attacks that can break the cooperative algorithm²⁶.

b. Power Supply Limitation

The first problem that may be caused by the limited power supply is denial-of-service attacks¹⁷. The adversary can continuously send additional packets to the target and ask it routing those additional packets. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service.

c. Internal Threats

Threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network. The compromised nodes may make use of the flaws and inconsistencies in the routing protocols to destroy the routing mechanism of the network, may provide fake link state information, or even flood other nodes with routing traffic¹⁷. Furthermore, It is difficult for the mobile nodes to work out some effective policies to prevent the possible malicious behaviour of some nodes.

d. Insecure Boundaries

The nature of the Mobile ad-hoc network promotes freedom to join, leave and move inside the network. Once the adversary is in the radio range of any other nodes in the Mobile ad-hoc network, it can communicate with nodes in its radio range and thus join the network automatically. Insecure boundaries makes the Mobile ad-hoc network susceptible to the attacks like passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service¹⁷.

E. Scalability

The scale of the ad-hoc network keeps changing all the time because of the mobility of the nodes. As a result, the protocols and services should be compatible to the continuously changing scale of the ad-hoc network. Because of the vulnerabilities discussed above, the Mobile ad-hoc network will need more robust security scheme to ensure the security of it. The security criteria to MANETs are discussed in following section.

3. Security Criteria to the Mobile Ad-hoc Networks**a. Authentication**

Authentication is the assurance that participants in communication are genuine and not impersonators¹⁷. In absence of an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

b. Authorization

Authorization is a process in which an entity is issued a credential by the certificate authority, which specifies the privileges and permissions it has. There should be an authorization process before the network administrator accesses the network management functions.

c. Availability

Availability means that a node should maintain its ability to provide all the designed services regardless of its security state¹⁷. This security criterion is challenged during the denial-of-service attacks, in which some selfish nodes make some of the network services unavailable²⁸.

d. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it.

e. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways⁵:

- Malicious altering - A message can be removed, replayed or revised by an adversary with malicious goal.
- Accidental altering -The message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors.

f. Non-repudiation

Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not.

g. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving.

Besides above, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Now let us have a look at various types of security attacks, which can take place in Mobile Ad-hoc Networks.

4. Security Attacks in Mobile Ad-hoc Networks

Security attacks in MANETs can be classified as following²⁶:

(i) **External attacks**, in which the attacker creates congestion, propagates fake routing information or disturbs nodes from providing services. External attacks can be prevented and detected by the security methods such as membership authentication or firewall.

(ii) **Internal attacks**, in which the adversary wants to gain the normal access to the network and participate the network activities.

Following are the main attack types that emerge in the Mobile ad-hoc networks:

1. Denial of Service (DoS)

The denial of service (DoS) attack aims to disturb the availability of certain node or even the services of the entire network. In MANETs, the attackers use the radio jamming and battery exhaustion methods to conduct DoS attacks.

2. Impersonation

In Impersonation attack, the adversary can capture some nodes in the network and make them look like normal nodes. In this way, the compromised nodes can join and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3. Eavesdropping

The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes.

4. Attacks against Routing protocols

Attacks on routing protocols aim to block the propagation of the routing information to the victim. The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack²⁶. There are some well known attacks against routing⁷:

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Modifying a Route Reply message to inject a false route.
- Suppressing Route Error to mislead others.

There are some more sophisticated routing attacks, which include Wormhole attacks⁸ and Rushing attacks⁹.

5. Attacks against packet delivery

The attacks on packet forwarding/delivery are not easy to detect and prevent²⁶. There are two main attack strategies in this type: one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save its own battery power; the other is denial-of-service, in which the adversary sends out overwhelming network traffic to the victim to exhaust its battery power.

In the following section, several security schemes for Mobile ad-hoc networks, which are based on the concept of clustering, are explored in a reviewing manner.

5. Clustering based Security schemes for Mobile Ad-hoc Networks

a. Cluster-based Intrusion Detection Technique for Ad-hoc Networks

According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems¹². Zhang and Lee²⁷ described a distributed and cooperative intrusion detection model where every node in the network participates in intrusion detection and response. In such cooperative intrusion detection architecture, participation of all nodes may cause huge power consumption. To solve this problem, Huang et al.¹⁰ presented a cluster-based intrusion detection technique for ad hoc networks. They organized a MANET into a number of clusters in such a way that every node is a member of at least one cluster, and one node per cluster will be designated as Cluster Head that will take care of the monitoring issue in a certain period of time. The finite state machine of the cluster formation protocol is shown in Figure 1.

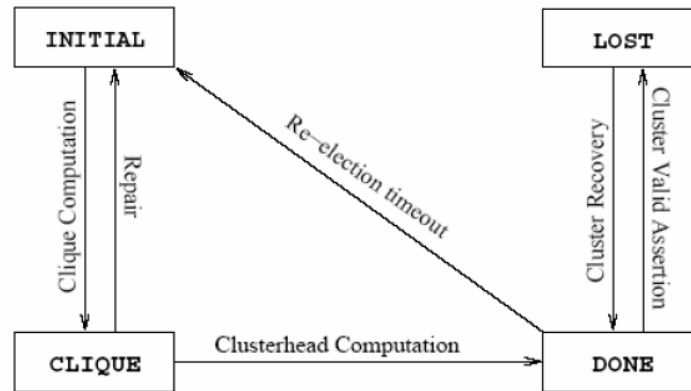


Figure 1: Finite State Machine of the Cluster Formation Protocol¹⁰

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, means they will monitor their own traffic and detect intrusion behavior independently. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. The technique in [10] used the clique based cluster formation algorithm described in [15] and at the completion of clique formation process every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the Cluster-Head. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol.

Huang et al.¹⁰ found that the CPU speedup is increased for the cluster-based IDS method than the per-node based IDS method; at the same time the network overhead for the cluster-based IDS methods is lower than that for the per-node based IDS method. However, the detection rate of the cluster-based IDS method is slightly lower than that of the per-node IDS method.

b. Cluster Based Authentication Model for Mobile Ad-hoc Networks

The basic wireless nature MANET makes it susceptible to various kinds of attacks. For a secure communication among the nodes of the mobile network, authenticity is of greater importance, which can be realized either through symmetric key algorithms, like DES, AES or through asymmetric public key algorithms like, El Gamal, Schnorr or RSA¹⁹. Since nodes in MANET's do not rely on any central authority like base stations or access points for their communication and due to the dynamic nature of the nodes, many researchers define the idea of using a central trusted authority for MANET's³. Instead many researchers have proposed distributed architectures for implementing security among the nodes^{3, 29}. Zhou et al.²⁸ proposed an idea of breaking a secret key into n parts and to reconstruct the secret from the parts, knowledge of at least k parts were necessary. It was named threshold cryptography and the idea formed the basis of distributed certification authority. It was further developed in the COCA system²⁹ as a general distributed authentication service. Hubaux et al.¹¹ used idea of threshold cryptography to come up with distributed security architecture for cluster based networks. In order to avoid any distributed certification mechanism, the authors relied on every participant to issue certificates for other nodes in a web-of-trust manner. Each participant has to store a number of certificates, and two nodes can only communicate securely when the union of their local stores contains a certificate path between them. This idea was further extended by Bechler et al.³. In their work, each new node that enters in to the network has to get certified from at least k trusted nodes in the network-to be considered as a trusted node. A (k,n) threshold cryptography system needs $2k$ messages for requesting and receiving certificates. An additional $2w$ messages are required to be transmitted if the requests to and replies from w warrants are to be transmitted over the ad hoc network. Thus a maximum of $2(k+w)$ messages needs to be passed for the whole procedure of warranting and key certification.

J. Chandra and L. L. Singh⁴ had proposed an architecture that deploys a mixed architecture using both Public key infrastructure (PKI) as well as distributed architecture for MANETs that divide the network into groups of

overlapping clusters. If the arriving node has a certificate that is valid in the region of the cluster, it takes just two messages to certify the node. In the other case when the node has a certificate from a certifying authority (CA) that is valid in the different region, restricting the network diameter to w clusters will lead to a transfer of $4w$ number of messages for certifying a node by another cluster head. In the case when a node has no certificate from any CA, it requires $2(k+w)$ messages to be transferred for certifying a node.

Although distributed security models in cluster based networks frees a network from relying on a central authentication body, but the cost incurred in terms of messages transferred for very dynamic clusters can be very large. A hybrid scheme in these cases can reduce the amount of messages transferred for warranting nodes and provide secured communication in the network.

c. Efficient and Secure On-Demand Routing in Clustered Wireless Ad-hoc Networks

Providing security and anonymity are critical in wireless ad-hoc networks. Therefore, it is necessary to design a secure anonymous routing which not only protect the privacy of nodes and routes but also ensure the security of networks in ad-hoc networks.

Kong and Hong¹⁴ proposed a solution, named ANODR, for anonymous on demand routing in Mobile ad-hoc networks. It is based on a network security concept called “broadcast with trapdoor information”. By substituting the destination ID in the route request with a trapdoor that only the destination can open, destination-anonymity can be preserved. However, in its route response the proof of opening the trapdoor is inefficient and the adversaries can forge easily a lot of invalid route reply packets. Zhu³⁰ has solved this problem by introducing Asymmetric source routing (ASR) which supports the destination verification through intermediate node. It provides more security properties than ANODR¹⁴, and presents a stricter and more detailed definition of anonymity. But it has large processing overhead, bad scalability and efficiency. Qian²¹ presented the first secure and anonymous routing based on clustered ad-hoc network (SARC). SARC adopts a hash value to identify the next hop, but the hash value is static so that it can be used for tampering and forging attacks by adversary in data transmission.

Yihui Zhang and Li Xu²⁵ proposed the design of an effective secure and anonymous on-demand routing protocol in clustered wireless ad hoc networks (ESODR). They have assumed that each cluster is made up of a

cluster head (CH) and multiple gateways (GWs) and other cluster members. All nodes can communicate with other nodes in the same cluster directly. Each source and destination shares a symmetrical secret key. ESODR combines hash function, symmetric key cryptographic algorithm, and public key cryptographic algorithm together. In ESODR, the computational complexity is low and has got good efficiency and scalability, as compared to other routing protocols, as shown in Table 1.

Table 1: Comparison of Security-Related Properties²⁵

Protocol Item	ANODR	SARC	ASR	SDDR	ESODR
Passive Attacks	Yes	Yes	Yes	No	Yes
Tampering Attacks	No	No	No	Yes	Yes
DoS Attacks	No	Yes	Yes	No	Yes
Replay Attacks	No	No	Yes	No	Yes
Packet Dropping or injection	No	No	No	No	Yes
Wormhole Attacks	Yes	No	Yes	Yes	Yes
Rushing Attacks	Yes	No	Yes	Yes	Yes

d. Cluster based Multi-hop Security Protocols in MANET

In Mobile ad-hoc networks, the placement of centralized entity to perform all management activities is not feasible due to the nature of the network. Moreover, the usage of PKI based approach is difficult due to its high computational power requirement. At the same time, the provision of security infrastructure is obligatory in MANET environment to offer secure communication among communicating entities¹³. So, authentication of communicating nodes before the transmission of actual data is a prerequisite in wireless transmission medium. An authentication protocol proposed by Ammayappan et al.² achieves the security requirements and also requires less computational power due to the deployment of elliptic curve cryptography and minimum transmission overhead due to less number of handshaking messages. This scheme was further improved by them in¹, where nodes and cluster heads are initially registered with the Trusted Third Party (TTP) and chipped with the certified token after successful verification of its credentials. Their proposed protocol uses hash functions and requires less number of symmetric encryption / decryption operations. Also cluster heads are not storing any secret information in terms of key pairs of the entire nodes and shared secret keys generated for each pair of nodes. Thus cluster heads are not a single point of attack in the proposed protocol.

Varadharajan et al.²⁴ have proposed a protocol on security for cluster based ad-hoc networks, using timestamp concept. They have employed Public Key Infrastructure and Pre Key Distribution approach in their protocol. When a mobile node enters into the transmission range of a cluster head, it executes the authentication phase and executes communication phase to communicate with another node. All the nodes involved in the process have to share a secret key with their respective cluster heads and each cluster head needs to share a secret key with other cluster heads. Storage overheads are much higher in this approach since cluster heads need to store the shared keys with respect to each individual node within its cluster and with each individual cluster heads. Pre key distribution approach is not suitable for MANETs due to its inherent nature of manual distribution of keys and scalability problems.

Nargunam and Sebastian¹⁸ proposed a cluster based security scheme to protect mobile ad hoc network link layer and network layer operations of delivering packet over the multi hop wireless channel. A well behaving node becomes a cluster member after the initial trust verification process. The membership validity period of a node depends on how long it has stayed and behaved well. In this routing protocol, the packets are routed only through the trusted members. The trust factor of a mobile node is verified and monitored by neighbor verification and monitoring modules. Based on the calculated credits other cluster members maintain their routing table. In fully secured mode all transmissions are protected by encoding the network layer packet header in addition to data encoding. Analysis shows that the secured cluster creation and maintenance overhead does not increase as the network size increases.

Jung-San Lee et al.¹⁶ have proposed a protocol for cluster based ad-hoc networks, using node identities to provide secure communication. Their protocol is based on identity based scheme. When a node wants to join with the cluster it needs to be authenticated by the cluster head by executing the authentication phase to get an authentication token from the cluster head. Trusted Authority (or TTP) generates a secret key for each node and for each cluster head and transmits the same, through a secure channel. In this protocol, secret key of a sender is generated based on the identity of the receiver, timestamp and certificate for each node. Nodes, which are within one-hop distance in a cluster, can communicate directly with each other using identities of the opposite entities. Only the intended receiver can validate the request received from the valid sender and generates the unique session key, to be used between them in order to make the communication more secure.

Hosseini et al.²³ have employed the cross layering technique to achieve a secure service discovery in MANETs. In their work, they introduced a new mechanism to secure network (Data and Communication) through a new Certificate Authority Mechanism with employing RSA mechanism with minimum energy consumption in comparison to other models. They have shown how cluster based networks integrates routing and security to achieve a secure and trusted way of deploying services in MANETS. Also they offered a secure solution with an authenticated routing protocol based on CBRP.

Renuka and Shet²² proposed a decentralized cluster based group key management scheme that uses a symmetric group key for communication within the cluster. This group key is generated by the cluster head and communicated to other members through a secure channel that uses public key cryptography. The nodes within the cluster communicate using symmetric key cryptography with the group key shared by all the nodes. Asymmetric key cryptography is used to encrypt the group keys generated, whenever membership changes occur. The authentication is done using hash trees or authentication trees. The computation cost of authentication and communication costs of re-keying messages is minimized here for change of membership.

6. Conclusion

In this survey paper, we have inspected the security issues in the Mobile ad-hoc networks. The security needs in the Mobile ad-hoc networks are much higher than those in the traditional wired or other wireless networks such as cellular networks. Initially we introduced the basic characteristics of the Mobile ad-hoc networks. Then some typical vulnerabilities, most of which are caused by the characteristics of the Mobile ad-hoc networks were discussed. Finally we have represented an evaluation of the available cluster based security solutions under different categories for the MANETs. Starting with the discussion on the security criteria in mobile ad hoc networks, we have seen the main attack types that threaten the operation of mobile ad-hoc networks. Finally we have discussed several cluster based security techniques that can help protect the mobile ad-hoc networks from external and internal security threats. There are mechanisms like cluster based intrusion detection techniques, cluster based authentication models, and cluster based secure routing protocols, which we have covered in this survey. We hope that this survey may be a helpful resource for researchers in the corresponding fields. Also the survey explores some points that can be further explored in the future.

References

1. K. Ammayappan, V. N. Sastry and A. Negi, Authentication and Dynamic Key Management Protocol based on certified tokens for MANETs, *Proc. of 2008 World Wireless Congress*, (2008) 30 – 35.
2. K. Ammayappan, V. N. Sastry and Atul Negi, Cluster based Multi-hop Security Protocol in MANETs using ECC, *Proc. of ACM MOBICOM*, (2001).
3. M. Bechler, H. Hof, D. Kraft, F. Piihlke and L. Wolf, A Cluster-Based Security Architecture for Ad-hoc Networks, *Proc. of INFOCOM 2004 - The 23rd Conference of the IEEE Computer and Communications Society*, **4** (2004) 2393-2403.
4. J. Chandra and L. L. Singh, A Cluster Based Security Model for Mobile Ad Hoc Networks, *Proc. of ICPWC 2005 - IEEE International conference on Personal Wireless Communications*, (2005) 413-416.
5. Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
6. H. Deng, W. Li, and D. P. Agrawal, Routing security in wireless ad hoc networks, *IEEE Communications Magazine*, **40** (10) (2002) 70-75.
7. Z. J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos and S. Sajama, *Wireless Ad Hoc Networks*, Wiley Encyclopedia of Telecommunications, 2003.
8. Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, *Proceedings of IEEE INFOCOM'03*, (2003).
9. Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, *Proceedings of ACM MobiCom Workshop - WiSe'03*, (2003).
10. Yi Huang and W. Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, *Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia*, (2003) 135 – 147.
11. J. Hubaux, L. Buttyan, and S. Capkun, The quest for security in mobile ad hoc networks, *Proc. of ACM symposium on Mobile Ad Hoc Networking and Computing (MobiHOC'01)*, (2001) 146-155.
12. Intrusion-detection system, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Intrusion-detection_system.
13. N. Komninos, D. Vergados and C. Douligeris, Authentication in a layered security approach for mobile ad hoc networks, *Elsevier Computers and Security*, **26**(5) (2007) 373- 380.
14. J. Kong and X. Hong, ANODR - ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, *Proc. of MOBIHOC'03 – 4th ACM international symposium on mobile ad-hoc networking and computing*, (2003) 291-302.

15. P. Krishna, N. Vaidya, M. Chatterjee and D. K. Pradhan, A Cluster-based Approach for Routing in Dynamic Networks, *ACM SIGCOMM Computer Communication Review*, **27** (2) (1997) 49–64.
16. J. Lee and C. Chang, Secure Communications for cluster – based ad hoc networks using node identities, *Elsevier Journal of Network and Computer Applications*, **30** (4) (2007) 1377-1396.
17. A. Mishra and K. M. Nadkarni, *Security in Wireless Ad Hoc Networks*, The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press, 2003.
18. A. S. Nargunam and M. P. Sebastian, Cluster Based Security Scheme for Mobile Ad Hoc Networks, *Proc. of IEEE WiMob'2006 - International conference on wireless and mobile computing, networking and communications*, (2006) 391-396.
19. T. Pedersen, A threshold cryptosystem without a trusted party, *Proc. of EUROCRYPT'91- 10th International conference on theory and applications of cryptographic techniques*, (1991) 522-526.
20. Charles Perkins, *Ad Hoc Networking*, Addison Wesley Longman Co. Boston, MA, 2001.
21. L. Qian, N. Song and X. Li, Secure Anonymous Routing in Clustered Multihop Wireless Ad Hoc Networks, *Proc. of 40th Annual Information Sciences and Systems Conference*, (2006) 1629- 1634.
22. A. Renuka and K. C. Shet, Cluster Based Group Key Management in Mobile Ad hoc Networks, *International Journal of Computer Science and Network Security*, **9** (4) (2009) 42-49.
23. S. A. Seno, T. Wan, and R. Budiarto, A Secure mobile ad-hoc network based on distributed certificate authority, *Springer-link Arabian Journal for science and engineering*, **36** (2) (2008) 245-257.
24. V. Varadharajan, R. Shankaran and M. Hitchens, Security for cluster based ad hoc networks, *Computer Commun*, **27** (2004) 488–501.
25. Y. Zhang, Li Xu, *An Efficient Secure On-Demand Routing in Clustered Wireless Ad Hoc Networks*, IEEE, 2008
26. Y. Zhang and W. Lee, *Security in Mobile Ad-Hoc Networks*, Ad-hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
27. Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad Hoc Networks, *6th Int'l Conf. Mobile Comm. and Net.*, (2000) 275 – 83.
28. L. Zhou and Z. J. Haas, Securing ad hoc networks, *IEEE Network*, **13** (1999) 24-30.
29. L. Zhou, F. B. Schaeider and R. Renesse, COCA: A secure distributed on-line certification authority, *ACM Trans. Computer Systems*, **20** (4) (2002) 329-368.
30. B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao and R. Deng, Anonymous secure routing in mobile ad hoc networks, *Proc. of 29th Annual IEEE International Conference on Local Computer Networks*, (2004) 102 -108.