**Abstract:**

* An Ad hoc network is a type of temporary computer-to-computer connection.
* In ad hoc mode, you can set up a wireless connection directly to another computer.
* The opponents are trying to manipulate the data.
* The hostile use the situation of multi cast traffic.
* Authentication of source and message integrity is the basic requirement.
* Tiered Authentication is used in multicast protocol.
* Multicast traffic employs the MAC to authenticate the message source.
* Advanced Encryption Standard (AES) is used to cipher the file for the security purpose by the sender.
* Central Authority (CA) sends the ciphered file to the users in the Ad-Hoc network.
* And the users retrieves the file by the AES algorithm and confirms the integrity of the file by MAC.

**Existing :**

* Nodes communicated through the Ad-Hoc network.
* It is possible by the multi cast protocol.
* No trusted certificate is provided because keys are not provided to the nodes.
* Tired authentication is not possible.
* Data is transferred from source to destination with out key.

**Disadvantages:**

* Traffic in multi cast is used by the hostile.
* Security is not guaranteed.
* There is no authentication to trust the data.
* Whether the data may be changed by the opponent.
* Key without data increases the vulnerability.

**Proposed:**

* Multicast protocol is used in the proposed system.
* Tired authentication is possible because of multicast protocol.
* MAC is used for the authentication purpose of data and source integrity.
* key is shared by the nodes for getting the Message Authentication code.

**Advantages:**

* Prevent the transmission of data reading by the adversary.
* Manipulation of data by hostile is prevented.
* Trusted authentication is provided because of MAC .
* Original data from source is received by the destination.

**Software Requirements:**

* Os : Windows xp
* Coding language : Java
* IDE : Eclipse
* Database : mysql server

**Hardware Requirements:**

* Hard Disk  : 250 GB.
* Monitor   :   15 VGA Color.
* Mouse    :   Logitech.
* Ram    : 512 MB.

**No of modules:**

* MAC yielding.
* File ciphering using AES and transfer.
* CA deployment and data distribution.
* File retrieve using AES.
* Data integrity checking.

**Modules description:**

1. **MAC Yielding:**
   * Sender selects a file for transmission and creates a Message Authentication Code (MAC) for data integrity.
   * Fetch the Message Authentication Code with its appropriate key to the transmission file.
2. **File ciphering using AES and Transfer:**
   * File is ciphered for the purpose of security using AES algorithm by the user defined key.
   * And the file which is encrypted is transferred to the (CA) Central Authority.
3. **CA Deployment and Data Distribution:**

* The file from sender is received by the Central Authority.
* Central Authority sends the appropriate file to the destinations with out doing any change.

1. **File Retrieve using AES:**

* The encrypted file from the Central Authority is received by the receiver.
* Receiver retrieves the file by using the AES algorithm.
* Receiver must use the correct key for the decryption of the file.

1. **Data Integrity Checking:**
   * Receiver gets the key from the file which is used to generating the MAC.
   * And receiver creates the MAC and compared it to the MAC which is received from the file.
   * If there is no change in the two MAC means then the file is not changed and the integrity is proved.

**Literature Survey:**

1. A survey of key management in ad hoc networks:

Abstract:

The wireless and dynamic nature of mobile ad hoc networks (MANETs) leaves them more vulnerable to security attacks than their wired counterparts. The nodes act both as routers and as communication end points. This makes the network layer more prone to security attacks. A main challenge is to judge whether or not a routing message originates from a trustworthy node. The solution thus far is cryptographically signed messages. The general assumption is that nodes in possession of a valid secret key can be trusted. Consequently, a secure and efficient key-management scheme is crucial. Keys are also required for protection of application data. However, the focus here is on network-layer management information. Whereas key management schemes for the upper layers can assume an already running network service, schemes for the protection of the network layer cannot. Keys are a prerequisite to bootstrap a protected network service. This article surveys the state of the art within key management for ad hoc networks, and analyzes their applicability for network-layer security. The analysis puts some emphasis on their applicability in scenarios such as emergency and rescue operations, as this work was initiated by a study of security in MANETs for emergency and rescue operations.

1. Multi-receiver authentication codes: models, bounds, constructions, and extensions:

Abstract:

Multireceiver authentication codes allow one sender to construct an authenticated message for a group of receivers such that each receiver can verify authenticity of the received message. In this paper, we give a formal definition of multireceiver authentication codes, derive information theoretic and combinatorial lower bounds on their performance and give new efficient and flexible constructions for such codes. Finally we extend the basic model to the case that multiple messages are sent and the case that the sender can be any member of the group.

1. A survey of clustering schemes for mobile ad hoc networks:

Abstract:

Clustering has been found to be an effective means of resource management for MANETs regarding network performance, routing protocol design, Quality of Service (QoS) and network modeling though it has yet to be refined to satisfy all the issues that might be faced by choosing this approach. Scalability is of particular interest to ad hoc network designers and users and is an issue with critical influence on capability and capacity. Where topologies include large numbers of nodes, routing packets will demand a large percentage of the limited wireless bandwidth and this is exaggerated and exacerbated by the mobility feature often resulting in a high frequency of failure regarding wireless links. In this paper we present a comprehensive survey and classification of recently published clustering algorithm, which we classify based on their objectives. We survey different clustering algorithm for MANET's; highlighting the defining clustering, the design goals of clustering algorithms, advantages of clustering for ad hoc networks, challenges facing clustering including cost issues and classifying clustering algorithms as well as discussion on the objectives and features of various clustering schemes presented in a comprehensive survey of the related literature.

1. Trust management in mobile ad hoc networks using a scalable maturity- based model:

Abstract:

In this paper, we propose a human-based model which builds a trust relationship between nodes in an ad hoc network. The trust is based on previous individual experiences and on the recommendations of others. We present the Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbors. Our proposal does not require disseminating the trust information over the entire network. Instead, nodes only need to keep and exchange trust information about nodes within the radio range. Without the need for a global trust knowledge, our proposal scales well for large networks while still reducing the number of exchanged messages and therefore the energy consumption. In addition, we mitigate the effect of colluding attacks composed of liars in the network. A key concept we introduce is the relationship maturity, which allows nodes to improve the efficiency of the proposed model for mobile scenarios. We show the correctness of our model in a single-hop network through simulations. We also extend the analysis to mobile multihop networks, showing the benefits of the maturity relationship concept. We evaluate the impact of malicious nodes that send false recommendations to degrade the efficiency of the trust model. At last, we analyze the performance of the REP protocol and show its scalability. We show that our implementation of REP can significantly reduce the number messages.

1. A survey of multicast routing protocols for mobile ad-hoc networks:

Abstract:

Design of a suitable routing protocol is difficult for mobile ad hoc networks due to its inherent dynamism and frequent topology change. Multicasting is even more complex because it requires transmission of an information to various destinations at approximately same time, if possible. Active research work in this field has resulted in a variety of proposals based on tree or mesh structures. This paper presents a state-of-the-art overview of multicast routing protocols for ad hoc networks. We believe that this survey will be a great source of information for researchers in ad hoc networks.