ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

An Approach for Secure Mobile Ad Hoc Networks: Key Management and Routing

Hridya V Devaraj[1], Jinu Mohan[2]

Final Year M. Tech Student, Dept. of CSE., Sree Narayana Gurukulam College of Engineering, Kerala, India[1]

Assistant Professor, Dept. of CSE., Sree Narayana Gurukulam College of Engineering, Kerala, India[2]

ABSTRACT: ThePopularity of MANET is increasing at a very fast pace. Reason for this increased attention is the wide range of multimedia applications running in the infrastructure less environment. Because of this infrastructure less environment, limited power and dynamic topology, it becomes very difficult to provide a secure environment in MANET. Security protocols for MANET's can be categorized in two major categories: Prevention: This mechanism involves protocols which prohibits the attacking node to initiate any action. This approach requires encryption techniques to authenticate the confidentiality, integrity, non-repudiation of routing packet information. Attacks such as Modification Attacks, Rushing Attacks, Impersonation Attacks, Denial of Service attack. Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network. Secure communication between two nodes in a network depends on reliable key management systems that generates and distributes keys between the communicating nodes and a secure routing protocol that establishes a route between them.

KEYWORDS: Communication networks, Packet, Routing, Topology

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes or terminals which communicate with each other by forming a multi-hop radio network and maintaining the connectivity in a decentralized manner. A multi-hop wireless networks are a collection of nodes that communicate with each other wirelessly by using radio signals. The nodes establish a connection between the source node (which forms the connection point, a redistribution point, or a communication end point) to the destination node dynamically. Nodes can act as sources, sinks and relays for packet. In a communication network, nodes can interact with each other, collaborate or even influence with each other in establishing a connection. Since the wireless ad hoc network is a collection of nodes with no infrastructure fixed, mobile nodes searches for a route to a destination. Thus the dynamic and distributed environment is exploited, which requires a collaboration among the nodes.

The solution based on identifying or isolating the misbehaving / malicious nodes requires high computational power and hence is an overhead to the system. The proposed energy efficient technique is built to prevent the malicious node from becoming a member of the cluster, thus leading to a secure Network.A node in an ad hoc network has direct connection with the set of nodes, called neighboring nodes, which are in its communication range. The number of nodes in the network is not fixed. New nodes may join or leave the network while existing ones may be compromised or become un-functional.The routing protocol should be such a way that it can cope up with the changes in the network topology. So, by dividing the network into clusters, the paths are recorded between clusters instead of between nodes and this increases the routes lifetime, and hence it decreases the amount of routing control overhead. Clustering also increases the network capacity and reduces the routing overhead which brings more efficient routing in MANET. Clustering in MANET guarantees many advantages when compared with traditional networks. But due to the unstable nature of MANET clustering in MANET is a difficult task. Cluster based routing protocols are used in clustering approach, but still there exists limitations besides the functionality of the Routing protocols. Clustering focuses on dividing the networks into clusters and to choose a particular node as a Cluster Head. Each cluster group will have a specific node elected as cluster head (CH). Secure communication between two nodes in a network depends on reliable key management systems that generate and distribute keys between communicating nodes and a secure routing protocol that establishes a route between them. But due to lack of central server and infrastructure in Mobile Ad hoc Networks (MANETs), this is major problem to manage the keys in the network. Secure communication is very important in computer networks and authentication is one of the most eminent preconditions. However, common authentication schemes are not applicable in any ad hoc networks because public key infrastructures with a centralized certification authority are hard to deploy there. Hence a preventive security concept based on cluster with key management and routing scheme is proposed.

II. Related work

In the year 2008, Zhaowen Xing, Le Gruenwald and K.K. Phang proposed a paper titled “A Robust Clustering Algorithm for Mobile Ad Hoc Networks” [2] which provides a promising way that can solve the routing scalability problem. Which divides a MANET into clusters first, and then develop a routing protocol on top of the clustered MANET. A clustered MANET consists of cluster heads and cluster members, where a cluster head (like a mobile support station in a cellular mobile network) manages its clusters, coordinates intra/inter-cluster communication and so on. A cluster member is a node that belongs to a cluster and is not a cluster head. Several weighted clustering algorithms have been proposed:

Mobility-only-based: Mobility of nodes triggers re-clustering and makes networks unstable, thus, it becomes the key attribute in the weight computation in the mobility-only-based clustering algorithms.

Power-only-based: A node with a higher remaining power level is, of course, a better candidate for the cluster head; so battery power is the only system parameter applied to calculate the weight of each node in power-only-based clustering algorithms.

Combination-based: Each node is assigned with a weight, which is calculated by considering more than one system parameters like node degree, remaining power, roaming speed, and so on.

Later on AbdelhakBentaleb, AbdelhakBoubetra, SaadHarous introduced a paper named “Survey of Clustering Schemes in Mobile Ad hoc Networks” [3] which surveys various clustering schemes. The process that divides the network into interconnected substructures, called clusters. A cluster is there-fore composed of a cluster head, gateways and members node.

Cluster Head (CH): it is the coordinator of the cluster.

Gateway: is a common node between two or more clusters.

Member Node (Ordinary nodes): is a node that is neither a CH nor gateway node. Each node belongs exclusively to a cluster independently of its neighbors that might reside in a different cluster.

Algorithms for Cluster Heads Election in MANETs

There are several algorithms in the literature for cluster heads election in mobile ad hoc networks: Lowest-ID, Highest-Degree, Distributed Clustering Algorithm, Weighted Clustering Algorithm (WCA) and Distributed Weighted Clustering Algorithm (DWCA).

Clustering Schemes in Mobile Ad hoc Network:

Identifier Neighbor Based Clustering: In identifier neighbor based clustering, a unique ID is assigned to each node. Each node in the network knows the ID of its neighbors. The cluster head is selected based on criteria involving these IDs such as the lowest ID, highest ID...etc.

Topology Based Clustering: In the topology based clustering, the cluster head is chosen based on a metric computed from the network topology like node connectivity.

Mobility Based Clustering: Lowest Relative Mobility Clustering Algorithm (MOBIC) is based on the LCA algorithm but involves the relative mobility of nodes as a criterion in the cluster head selection.The idea is to choose nodes with low mobility as cluster heads because they provide more stability. MOBIC uses a similar clusters maintenance procedure as LCC with an additional rule to minimize the cost of clusters maintenance.

Energy based Clustering: The battery power of node is a constraint that affects directly the lifetime of the network, hence the energy limitation poses a severe challenge for network performance. CH performs special tasks such as routing causing excessive energy consumption.

Weight based Clustering: Weight based clustering techniques use a combination of weighted metrics such as: transmission power, node degree, distance difference, mobility and battery power of mobile nodes… etc. The weighting factors for each metric may be adjusted for different scenarios.

“Clustering & Cluster Head Selection Techniques in Mobile Ad hoc Networks” proposed by V.Preetha, Dr.K.Chitra [4] proposes that the cluster head plays the role of a coordinator within its substructure. Each CH acts as a temporary base station within its cluster and communicates with other CHs. Cluster head (CH) election is the process to select a particular node within the cluster as a head node. The responsibility of the CH is to manage the nodes of its own cluster and to communicate with other Clusters. It can communicate with other clusters directly through the respective CH or through gateways. It can communicate by sending and receiving the data, compressing the data and transmitting the data to the other Cluster Heads. Electing a specific node as a head node is not an easiest task. Depending on different factors such as geographical location of the node, stability, mobility of the node, energy, capacity and throughput of the node, trusted nodes etc the selection criteria may vary. But Cluster Head node may be a special mobile node with extra functions. The following figure represents the structure of a Cluster with Cluster head as the Special node and the cluster members (ordinary node) with white circles and the gateway nodes communicating between clusters.

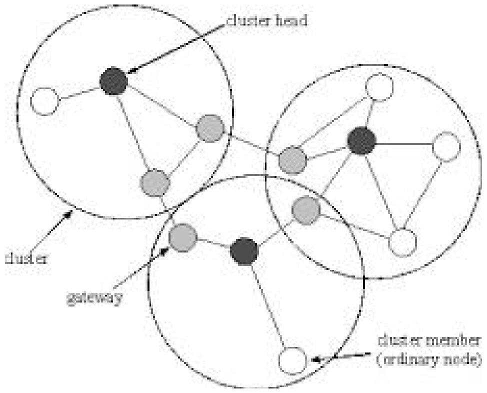


Fig 2.1 A Typical Cluster Model

“Energy and Mobility Based Group Key Management in Mobile Ad Hoc Networks” proposed by M.Ramya Priyadharshini1, S.Prasanna1, Dr.N.Balaji [5], provides a secure communication is a major research avenue in MANETs because of the dynamic topology due to mobility and energy constraint. To ensure security ID – based key management was introduced. Most of the existing systems have provided various key management schemes like ID – based multiple secret key with threshold cryptography, Hierarchical Identity Based Key management, Cluster Based Identity Management etc. Though these schemes are efficient in providing security, the energy consumption is high. This leads to the need of an energy proficient key management method. The proposed scheme EMBGK - Energy and Mobility based Group Key Management scheme concentrates in: 1) Cluster Formation 2) Link Stability 3) Mobility Prediction and 4) Group Key Management. The individual node properties are verified and the nodes are organized into clusters based on their transmission range. The mobility is predicted based on the previous positions of the node. Using all this, an optimized method is implemented for the cluster head election and cluster formation. The proposed scheme saves time and energy for frequent cluster updations and key updations.

“Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature “by Spinder Kaur1, Harpreet Kaur [6] proposes RSA security protocol (stands for the Rivest, Shamir and Adleman who are the creator of the RSA). RSA is an asymmetric-key security protocol as it uses two different keys for its encryption and decryption purpose. It is the most popular and proven asymmetric key cryptography algorithm. It generates two key private key and public key. Private Key is secrete to the user and public key is known to other who wants to communicate with the user. For this reason it is also known as public-key cryptography. It is the very first algorithm known to be suitable for signing as well as encryption, and was one of the first advances in public key cryptography.
CPU and Memory Utilization: An algorithm should utilize minimum CPU resources as well as minimum memory (RAM).
Energy Consumption: The Energy Consumed by RSA Cryptosystem is less as compared to RSA Digital Signature. RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring product of two large prime numbers, the factoring problem.

In the year 2008 Lin SHEN and Xiangquan SHI proposed a paper titled, “A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks” [7] Recent advancement in wireless communication and microelectronics has enabled the design and development of wireless sensor networks with low cost, low energy consumption and high utilization. Many cluster-based wireless sensor network routing protocols have been proposed. However, most of them take little consideration on communication protection, which is important to ensure the network security. In this paper, a lightweight key management approach is presented. Its analysis shows that this approach is an effective solution to the key management of hierarchical clustered wireless sensor networks.Wireless sensor networks (WSN) are wireless networks composed of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Each sensor node in a sensor network is typically equipped with a radio transceiver or other wireless communication device, a small microcontroller, and an energy source, usually a battery.

“Key Management Scheme in Mobile Ad Hoc Networks “proposed by Abu TahaZamani, Syed Zubair[8] proposes some solutions for key management in mobile ad hoc networks. The major problem in providing security services in such infrastructure, how to manage the cryptographic keys that are needed. In order to design practical and sufficient key management systems it is necessary to understand the characteristics of ad hoc networks and why traditional key management systems cannot be used. The aim of key management is to provide secure methods for handling cryptographic keying algorithm. The tasks of key management includes keys for generation, distribution and maintenance. Key maintenance includes the procedures for key storage, key update, key revocation, etc. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node’s available resources and the dynamic nature of network topology. A number of key management schemes have been proposed for MANETs. The ad hoc networks generally presents the following characteristics:
Dynamic network topology, Limited bandwidth, Energy constrained nodes, Limited physical security

“Efficient Cluster Based Multicast Tree for Secure Multicast Communication for Mobile Ad Hoc Networks” proposed by D.Suganya Devi and Dr.G.Padmavathi [9] proposes A Secure multicast communication in mobile ad hoc networks. The challenging characteristics of infrastructure-less architecture with lack of central authority, limited resources such as bandwidth, time and power. Hence key management is the fundamental challenge in achieving secure communication using multicast key distribution in mobile ad hoc networks. In many multicast interactions, due to its frequent node mobility, new member can join and current members can leave at a time due to node failure which causes delay in multicast transmission. This paper proposes a new efficient cluster based multicast tree (CBMT) algorithm for secure multicast Communication, in which source node uses Multicast version of Destination Sequenced Distance Vector(MDSDV) routing protocol to collects its 1 hop neighbors to form cluster and each node which have child node is elected as the Local controllers of the created clusters. The proposed approach is to achieve secure multicast communication for mobile adhoc networks. This approach uses Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using MDSDV tends to have multicast connectivity between the nodes. The approach of Efficient CBMT with mobility aware MDSDV is described in five phases with specific notations.
Phase 1: Authentication: For each node, assign certificate key to verify its node identity.
Phase 2: Cluster Head Election
Phase 3: Cluster Formation
Phase 4: Secure Multicast Communication
Phase 5: Node mobility

III. PROPOSED ALGORITHM

A. NETWORK MODEL

The basic idea of the multicast group clustering approach is realized by dividing the multicast group dynamically into several sub groups called clusters. A node in an ad hoc network has direct connection with a set of nodes, called neighboring nodes, which are in its communication range. The number of nodes in the network is not necessarily fixed.

New nodes may join the network while existing ones may be compromised or become un-functional. So, by dividing the network into clusters, now the paths are recorded between clusters instead of between nodes and this increases the routes lifetime, so it decreases the amount of routing control overhead. Clustering also increases the network capacity and reduces the routing overhead which brings more efficient and effective routing in MANET. Every clustering algorithm consists of two mechanisms, cluster formation and cluster maintenance. In cluster formation, cluster heads are selected among the nodes to form the hierarchical network. And cluster maintenance deals with the membership changes caused by the dynamic nature of mobile nodes. Clustering is a process that divides the network into interconnected substructures, called clusters. In a clustering scheme, all the mobile nodes in a MANET are grouped into different geographically distributed groups. Clustering in MANET guarantees many advantages when compared with traditional networks. But due to the unstable nature of MANET clustering in MANET is a difficult task. Cluster based routing protocols are used in clustering approach, but still there exists limitations besides the functionality of the Routing protocols. Clustering focuses on dividing the networks into clusters and to choose a particular node as a Cluster Head. Each cluster group will have a specific node elected as cluster head (CH).A definite cluster that could not be included in any another cluster termed as Exclusive Clustering algorithm is used. The Distance measure between the data points helps in the clustering algorithm to define a definite exclusive cluster. Each cluster is headed by a cluster head. The cluster head generates a group key and distributes it to its members through the secure channel. Whenever membership changes occur, the cluster head regenerates the group key and distributes through this secure channel. Lowest Relative Mobility Clustering Algorithm (MOBIC) is based on the LCA (Linked Cluster Algorithm) algorithm but involves the relative mobility of nodes as a criterion in the cluster head selection. The idea is to choose nodes with “low mobility” as cluster heads because they provide more “stability”.

B. KEY MANAGEMENT

Key management is a basic part of any secure communication. Group key management protocols based on the decentralized approach can be best suited in mobile ad hoc network. However, group key management for large and dynamic groups in MANETs is a difficult problem because of the requirement of scalability and security.Thus this phase proposes a reliable dynamic clustering approach by reducing the packet drop ratio and increasing the key delivery ratio. In many multicast interactions, due to its frequent node mobility, new member can join and current members can leave at any time. The moving behavior of each members in the MANET should be realistic. The pattern of movement of members is classified Proposed Methodology into different mobility models and each one has its own distinct features. It is a crucial part in the performance of MANET. Once the clusters are created within the multicast group, the new CH becomes responsible for the local key management and distribution to their local members, and also for the maintenance of the strongly correlated cluster property. An efficient Cluster Based Multicast Tree (CBMT) using mobility aware Multicast version DSDV for secure multicast key distribution. MDSDV have multicast connectivity between nodes. It sends acknowledgement for each transmission in order to reduce the retransmission. The CHs are elected easily with periodic updates of node join and leave information using multicast tree. This overcomes the issues of end to end delay in multicast transmission and also tolerates the fault that occurs due to node failure. The proposed approach is to achieve secure multicast communication for mobile adhoc networks. This approach uses Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using MDSDV tends to have multicast connectivity between the nodes.

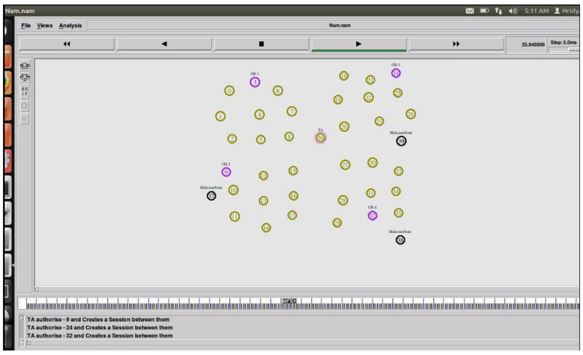
C. ROUTING

In the proposed methodology mobile nodes come closer to each other to form a temporary network. Any node can join or leave the network any time. RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring product of two large prime numbers, the factoring problem. Choose two distinct prime numbers p and q. For security purposes, the integer’s p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test. In the Next Phase, Path is computed via the CH to TA and vice versa. Source starts finding out shortest paths to CH. In case of route failure the immediate node will select the other shortest path to destination CH via the TA. And finally, text encryption RSA cryptosystem. RSA is a cryptosystem, which is

known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret.
In RSA, Encryption is as follow: Given a message M, 0 < M < n
use***public*** key (e, n) Compute, C = Me mod n
Whereas the decryption: Given a ciphertext C, use ***private*** key (d)
Compute,
Cd mod n = (Me mod n)d mod n = Med mod n = M

IV. IMPLEMENTATION

This research work is implemented using NS2.35. Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley.
Phase 1:
A Mobile ad hoc network (MANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure. Initially the topology creation is performed. Which mainly deals with the deployment of wireless nodes along with Trusted Authority, which may contain several malicious node. At this stage the distance between each neighboring node is determined. About 40 nodes are simulated. Fig 4.1 shows the simulated 40 mobile nodes.
Phase 2:
The distance metric mechanism in Exclusive Clustering is employed for cluster formation and cluster head selection. The Information Index send by each nodes contains the node details. The Mobility of the nodes are analyzed by the TA to choose the Cluster Head among each cluster. The Cluster Heads Election is done with respect to *Mobility Based Clustering* which deals with Lowest Relative Mobility Clustering Algorithm (MOBIC) algorithm that involves the relative mobility of nodes as a criterion in the cluster head selection. The idea is to choose nodes with low mobility as cluster heads because they provide more stability. MOBIC uses a similar clusters maintenance procedure as LCC with an additional rule to minimize the cost of clusters maintenance.
Phase 3:
Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using MDSDV tends to have multicast connectivity between the nodes.
Phase 4:
The source to destination routing via TA and CH leads to better and secure routing alongside encryption using RSA. Membership changes in cluster leads the CH to revoke the member from that cluster and the next respective cluster head reports the membership changes to TA. TA authorizes the cluster head. Later on the key management for the cluster member is authorized by the TA to the CH.



```
TA authorise - 9 and Creates a Session between them
TA authorise - 24 and Creates a Session between them
TA authorise - 32 and Creates a Session between them
```

Fig 4.1 Network Deployment

DOI: 10.15680/IJIRCCE.2016. 0407007

V. SIMULATION RESULTS

The performance of proposed methodology for secure MANET is evaluated in terms of QoS metrics.

A. PERFORMANCE METRICS

The QoS metrics are end to end delay in key distribution, energy consumption, Key delivery ratio and packet drop ratio of multicast key distribution.

Energy Consumption is defined as the sum of energy units required to the key transmission throughout the duration of multicast data transmission. Energy consumption of multicast key distribution Energy consumption is calculated by adding the maximum energy and minimum energy among the nodes.

Key Delivery Ratio is defined as the number of received keys divided by number of sent keys. This metric allows evaluating the reliability of the protocol in terms of key delivery ratio in key transmission from the source to the group members as in eqn.

$$\text{KDR} = \frac{\text{Number of received keys}}{\text{Number of sent keys}}$$

Packet Drop Ratio: is the ratio between the number of packets received at the destination and the number of packets sent to the destination. This metric allows in evaluating the reliability of the protocol in terms of packet drop ratio in key transmission from the source to the group members as in eqn.

$$\text{PDR} = \frac{\text{No. of packets received at the destination}}{\text{No. of packets sent to the destination}}$$

End to End Delay: It indicates the average latency or end to end delay of key transmission from the source to the destination. This metric allows evaluating the average delay to forward a key from a TA to its cluster members. Transmission delay is calculated as in eqn.

$$\text{TD (N)} = ts + tk + \Sigma i{+}1n\ ((\ 1\text{-}pi\ )\ Ni\ )$$

N--> No. of packets from source to destination Ni-->.No. of packets transmitted to path
pi--> packet drop ratio TD--> Transfer delay ts--> setup time tk-->key transmitting time.

The Proposed Methodology is ideally tested in the simulation environment and the performance metrics are efficient under the varying network conditions. As in Fig 5.1 Energy Consumption of a node is decreasing.

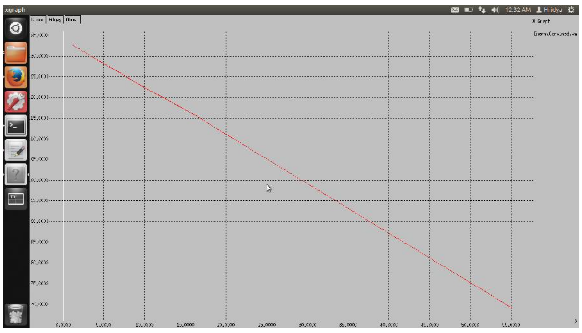


Fig 5.1 Energy Consumption of a node.

VI. CONCLUSION AND FUTURE WORK

The proposed approach is tested and the entire experiments are conducted in a simulation environment using network simulator NS2 which accurately predict the performance of proposed scheme in terms of QoS metrics under varying network conditions. The solution based on identifying or isolating the misbehaving nodes requires high computational power and hence is an overhead to the system. The proposed energy efficient technique is built to prevent the compromised node from becoming a member of the cluster, thus leading to a secure Network. A node in an ad hoc network has direct connection with a set of nodes, called neighboring nodes, which are in its communication range. The number of nodes in the network is not necessarily fixed. New nodes may join the network while existing ones may be compromised or become un-functional. The routing protocol should be such that it can cope up with the changes in the network topology. So, by dividing the network into clusters, now the paths are recorded between clusters instead of between nodes and this increases the routes lifetime, so it decreases the amount of routing control overhead. Clustering also increases the network capacity and reduces the routing overhead which brings more efficient and effective routing in MANET.

REFERENCES

1. Rohit S Jigalur,Suresha, C.BhushanThIcccnt "Designing A Secure Architecture Against Wormhole Attacks In Wireless Sensor Networks" July 4 - 6, 2013
2. Zhaowen Xing, Le Gruenwald And K.K. Phang "A Robust Clustering Algorithm For Mobile Ad Hoc Networks Handbook Of Research On Next Generation Networks And Ubiquitous Computing; A Book Edited By Prof. Samuel Pierre December 2008
3. AbdelhakBentaleb, AbdelhakBoubetra, SaadHarous "Survey Of Clustering Schemes In Mobile Ad Hoc Networks" ; Communications And Network, 5, 8-14 Doi:10.4236/Cn.2013.52b002 Published Online May 2013
4. V.Preetha, Dr.K.Chitra ; "Clustering & Cluster Head Selection Techniques In Mobile Ad Hoc Networks" International Journal Of Innovative Research In Computer And Communication Engineering (An Iso 3297: 2007 Certified Organization) Vol. 2, Issue 7, July 2014
5. M.RamyaPriyadharshini, S.Prasanna, Dr.N.Balaji "Energy And Mobility Based Group Key Management In Mobile Ad Hoc Networks" Vol. 1, Issue 7, July 2014
6. Spinder Kaur, Harpreet Kaur; D. Suganya Devi Et. Al. "Implementing Rsa Algorithm In Manet And Comparison With Rsa Digital Signature "International Journal Of Engineering Science And Technology Vol. 2(5), 2010, 1304-1310
7. Lin Shen And Xiangquan Shi "A Dynamic Cluster-Based Key Management Protocol In Wireless Sensor Networks"; International Journal Of Intelligent Control And SystemsVol. 13, No. 2, June 2008, 146-15
8. Abu TahaZamani, Syed Zubair "Key Management Scheme In Mobile Ad Hoc Networks "Journal Of Network And Computer Applications; International Journal Of Emerging Research In Management &Technology Issn: 2278-9359 (Volume-3, Issue-4)
9. D.Suganya Devi And Dr. G.Padmavathi "Efficient Cluster Based Multicast Tree For Secure Multicast Communication For Mobile Ad Hoc Networks" International Journal Of Engineering Science And Technology Vol. 2(5), 2010, 1304-1310.
10. Praveen Joshi; Procedia"Security Issues In Routing Protocols In Manets At Network Layer" Computer Science 3 (2011) 954–960
11. Kamal Kumar Chauhan And Amit Kumar Singh Sanger"Securing Mobile Ad Hoc Networks: Key Management And Routing" International Journal On Adhoc Networking Systems (Ijans) Vol. 2, No. 2, April 2012/Ijans.2012.2207 65
12. M.Ramya Priyadharshini1, S.Prasanna1, Dr.N.Balaji "Energy And Mobility Based Group Key Management In Mobile Ad Hoc Networks" 2014 International Conference On Recent Trends In Information Technology 978-1-4799-4989-2/14/$31.00 © 2014 Ieee

BIOGRAPHY

Ms.Hridya V Devarajreceived herB.Tech degree in Computer Science & Engineering from Kerala University, India. And is currently pursuing M.Tech Degree in Computer Science & Engineering in SreeNarayanaGurukulam college of Engineering, Kerala, India and is affiliated to Mahatma Gandhi University, India. Her area of research includes Computer Networks.

Mrs.Jinu Mohan has been working as Assistant Professor Computer Science & Engineering,SreeNarayanaGurukulam college of Engineering, Kerala, India and is affiliated to Mahatma Gandhi University, India. She obtained B.Tech,M.Tech and is currently pursuing Ph.D. She has 6 Years of Teaching Experience. Her areas of research include Computer Networks and Image Processing.