Secure Routing Scheme in MANETs using Secret Key Sharing

A. Amuthan
Associate Professor
Department of Computer Science & Engineering
Pondicherry Engineering College
Puducherry-605014

B.Aravind Baradwaj
PG Scholar
Department of Computer Science & Engineering,
Pondicherry Engineering College,
Puducherry-605014

ABSTRACT
A Mobile Ad-hoc NETwork (MANETs) follows a dynamic topology with distributed architecture. MANETs has no basic infrastructure also has no fixed access point or routers, where in the nodes moves in an undefined manner in a specified area of work. Basically, the distributed dynamic architecture is vulnerable to various kinds of attacks like blackhole, wormhole flooding, etc. Providing a security measure that would enhance the role of security services during a data transmission is a critical task. In this paper, we propose a new solution for the secure routing of all tree based multicast routing protocols such as MAODV, ADMR, etc, against attacks like flooding, wormhole, blackhole attack etc,. In this scheme, keys are generated by source and transmitted to the client nodes in the network. Interpolation concept under the finite field provides a promising outcome for securing the network. The proposed scheme is based on Shamir secret sharing scheme with encrypted transmission of keys. As the transmission of keys to the participant nodes is done using RSA public key encryption algorithm, it is not vulnerable to attacks like replay attacks, and other spoofing

General Terms
MANETs, Multicast Secure Routing

Keywords
Multicast, Secure Routing, Tree based protocols, Shamir secret sharing scheme, RSA, Mobile Ad-hoc NETworks.

1. INTRODUCTION
Providing security services to MANETs, has been a challenging task for many years, and has been under research. Solution for various kinds of attacks in MANETs has been a buzzword amongst researchers because MANETs applications have been extended for the use in military applications, emergency rescue operations, in confidential video conferencing, etc. A MANET is an automated network which is fully dynamic and distributed in nature. The functionalities of every node are alike where in identification of an attacker or malicious nodes amongst the network is a challenging task. Maintaining the security for multicast routing in MANETs is equally important. There are many security protocols under the functionality of multicast [1] has been designed. But these protocols are vulnerable to various kinds of attacks on MANETs [2] like flooding, blackhole, wormhole, etc. There has been many works published in the literature regarding their attacks and the solution for the attacks.

MANETs despite their dynamic environment they are suitable for many applications where the centralized environment cannot be used. Dynamism is caused by the movement of nodes in a specific region there by creating and modifying the existing links and their data transfer. MANETs works on the basis of specific protocols where in the entire functionality of the network lies. The protocols are grouped based on their functionality. The three broad classifications of the protocols are Tree based [3], Mesh Based [3] and Hybrid [4]. Tree Based protocols uses a tree based structure for their operation of the protocols and also for the maintenance of the member of the groups. There is various tree based structure that are formed during protocols operations. They are source based tree and shared tree structure. Source based tree structure is formed when the source gets in interests and sends the route requests to many other nodes in the network, thereby each and every other members in the networks gets in and grabs the route requests and sends a reply back to the source. As by the protocol operations, there will be many trees in an area wherein MANETs are used for operations. Shared Tree uses a single tree for all its protocol operations. A single tree is formed where the tree connects to each and every node in a network and any operation is done using the single tree that is interconnected. Examples of tree based protocols are MAODV [5], ADMR [6][7]. Another genre of the classification is the mesh based protocols. Using mesh based protocols; the functionality extends to a higher level of support than tree based protocols by creating cluster of links between each and every node, thereby creating the ease of data transfer between the nodes in the networks. Ease of data transfer is guaranteed on the usage of mesh based protocols because of multiple links between source and destination and also the interim data transfer. It provides high packet delivery ratios and also multipath functionality at the times of nodes lost from the group on usage of specific links from source to destination. Some of the mesh based protocols are ODMRP [8], CAMP [9]. Third classification is Hybrid protocols where it uses the functionality of both tree and mesh based protocols. Example of hybrid protocols is ZRP [10], TORA [11].

Routing mechanism is different for different types of protocols of no matter under what classification it lies in. The classification based on routing is divided into Table – Driven and On – demand. Even though the protocols has been classified based on their operations, their routing functionalities lies under any of these two hats. Table Driven protocols is also known as proactive, where the routes are pre-calculated and stored in a table. When the packets arrive at a node for routing, the packets are immediately routed using the pre-calculated table which is present in each node. The advantageous scenario for this type of routing is that the packets are routed immediately as

it is received in any node without further delay. Main drawbacks of this method are storage and routing overhead. Each and every specified interval the table has to be updated for the faster delivery of the information. Latter classification is on-demand, also known as reactive routing protocol. The routing characteristics of this mechanism are that, the routes are created or searched after a packet arrives to any of the nodes in the network. The route establishment of this method includes two phases: route request phase and route reply phase. On – Demand mechanism is relatively good for routing and the advantages are lesser network overhead and less storage space.

Enormous amount of publications has been made on secret sharing scheme [12]. As per the name, sharing of secret through communication channel is insecure as the way attacker sees it. In this paper, we introduce an easiest and yet powerful method for identification of malicious nodes in a network. We call it as Secure Key Sharing (SKS) scheme. In this scheme, the node which initiates the transaction is called source node and this node generates a polynomial randomly. On substitution of different values in the *'x'* value of the polynomial, we arrive to different D_i values where D_i's are the keys generated for corresponding nodes. This different D_i values are sent to the corresponding i^{th} node. During the authentication phase or route establishment phase, these D_i values are sent back to their source for verification. For to verify the node, then number sent back is substituted in the polynomial and is checked for arriving the master key. Using this scheme, the source node consistently distributes shares to its participating nodes.

2. PROBLEM DESCRIPTION

The main problems among MANETs are, it is prone to many kinds of attacks, especially routing attacks like flooding, wormhole, blackhole etc. As described earlier, providing the security features to MANETs has been a great task for the researchers. To overcome the attacks and to provide a solution, a secret key sharing scheme is governed. The scheme used for generation of different shares is Shamir secret sharing scheme [13][14]. The generated secret has to be safely transported or communicated to all their participating node is been a great deal of problem. For this key transmission, we use RSA scheme. However, this scheme is a general cryptographic scheme, but we have implemented this idea in MANETs. The key generated is encrypted using the node's public key and then transmitted to them. The original secret key can be reconstructed by applying private key for their corresponding public key encrypted data

3. RELATED WORKS

As MANETs are dynamic and has very distributed structure it is prone to many routing attacks. There are number of attacks present in the existing systems such as flooding, blackhole, wormhole attacks. Present system has been designed only by considering the work ability and to avoid overhead caused by the transactions of packets through the network. But these systems are more vulnerable to attacks during the routing of packets from one node to other (i.e.) source to destination.

Wide research has been conducted on MANETs for providing security solutions against attack on the basis of cryptographic scheme. Basic cryptographic schemes are public and private key cryptography. As MANETs are dynamic in nature, private key cryptography cannot be a reliable solution because the keys are to be sent through the channel for the receiver to decrypt the message. If even using Diffie – Hellman key exchange for the key it takes three messages to come to a mutual key which introduces lot of packets in the network that may lead to network congestion. On usage of public key cryptography, the efficient algorithm RSA comes under concern because it is reliable and secure when compared to other public key cryptographic systems. Earlier in the literature, these secret key sharing schemes has been used in multipath routing where the generated keys are divided into *'n'* shares and each shares takes a separate route to destination. Even if any of the *'n'* shares has been lost either due to network congestion or by any malicious activity by an attacker or intruder, with the help of *'n-1'* shares, we can generate the secret key at the destination. By using RSA based threshold cryptography [15] (RSA-TC), Lagrange's interpolation and the generation of polynomial is for generating partial keys. The sender transmits these partial keys into multiple routes to destination, along with the shared value. After receiving't' or more partial keys, the receiver selects *'t'* keys from the values received for the deciphering of the message. The receiver encrypts the shared value with the sender's public keys *'e'*, and transmits it to the sender along various paths. The sender then calculates the values using Lagrange's interpolation for the RSA's *'N'* parameter, where *'N'* is the product of very large prime number generated at random, is sent back to the receiver. Then the receiver apply the shared value to the partial keys and by collecting all results, he can decipher the secret message. The threshold cryptography based sharing also uses Elliptic Curve Cryptography (ECC) instead of RSA. Here the shared value may be split degree and after encryption. The message is split in *'n'* pieces. As by ECC, the point exponentiation takes maximum resources and time, while point addition takes the minimum. In ECC-TC [16], the key value is not shared because every value in ECC is in the form of points and for points Lagrange's interpolation is not possible. The function of key sharing may take two forms

1) Encrypt the message into a point and split the co-ordinates

2) Split the message, encrypt it with co-ordinates.

Many schemes have come into existence with secret sharing scheme in the field of MANETs. But to the best of my knowledge, it is not used in the identification of malicious nodes.

4. CONSTRAINTS

All nodes in the MANETs have unique identification address. We assume that if a node in MANET broadcast or multicast any data to other nodes in a network, each node reads the same value. Hence adversary cannot send two different values for other nodes in the network. As ADMR protocol is a source based initiated protocol, we assume that any request made to the source node to join the group is assumed to be genuine node and cannot turn adversary. Assumption also made that every node's public key known to every nodes that are inside the MANET.

5. SECURE SHARING SCHEME

In this paper, we propose the usage of Shamir secret sharing scheme for the process of identification of malicious nodes among MANET nodes. The motivation for the use of secret key sharing scheme is that, it gives confidence to the source node or the owner about the genuinely participating nodes in the network. Here a key is transmitted or shared among the multiple individuals in the network that are under the process of

encryption and decryption. The objective is to maintain the genuineness of the nodes that are present in the network. Here the keys are randomly generated by substituting any number to the polynomial generated by the source and then it is shared to their corresponding nodes for which it is generated. Maintaining the integrity of the data during transmission to the other nodes adds difficulties to the security services provided to the MANETs. To overcome this problem we use the public key encryption system called RSA. These secret key sharing schemes has been used under various scenarios where the secret is transmitted from source to destination in multiple paths by splitting the key *'k'* into *'n'* pieces, which takes *'n'* different paths to destination. At the destination, by considering *'n-1'* or more keys than *'n-1'*, the original secret is generated.

The solution for the attacks is designed by using Shamir secret sharing algorithm and the encrypted key exchange scheme. The Shamir secret sharing algorithm show that how to divided the key *'k'* in *'n'* pieces in such a way that *'k'* is reproduced from *'p'* pieces but even a complete knowledge of *'p-1'* pieces gives absolutely no information about the key *'k'*. This secret sharing scheme basically works by the concept of Lagrange's interpolation. The concept of Lagrange's interpolation is finding out missing data with all other data present.

5.1. Lagrange's Interpolation

If $x_1, x_2, \ldots, x_k$ are distinct real numbers and $y_1, y_2, \ldots, y_k$ are real numbers, there is one and only polynomial $q(x)$ of degree at most $k-1$, such that $q(x_i) = y_i$ for i=1,2,3…, k. The polynomial $q(x)$ is given by

$$q(x) = \sum_{r=1}^{k} y_r \prod_{\substack{i=1 \\ i \neq r}}^{k} \frac{(x - x_i)}{(x_r - x_i)}$$

This interpolation is used differently in the filed of modulo arithmetic. For a prime *'p'*, let $Z_p = \{0,1,2,\ldots\ldots, p-1\}$, Z_p is a field under addtion and multiplication modulo p.If $x \in Z_p$ and $x \neq 0$ then $\frac{1}{x} = y$ if and only if $xy \equiv 1 (mod\ p)$. On proving the example Z_5. Here p = 5, Z_5 = {0,1,2,3,4}, $\frac{1}{2} = 3$ since 2.3 = 6 ≡ 1(mod 5). Similarly $\frac{1}{4} = 4$.

Thus, the proof that the lagranges interpolation holds good in the finite field Z_p. That is if $x_1, x_2, \ldots, x_k$ are distinct elements of Z_p and $y_1, y_2, \ldots, y_k \in Z_p$, then there exists one and only polynomial of $q(x)$ of degree at most $k-1$ such that $q(x_i) = y_i$, where i= 1,2 3,…k.

5.2. Shamir Secret Sharing (K, N) Threshold Schemes

Shamir secret sharing (k, n) scheme [17] is based on polynomial interpolation where the information is considered theoretically secure. In general on assumption, the dealer divides the secret and distributes shares to these shareholders without making any flaws. Any share that has been sent to shareholder must unconditionally trust the received share as a valid one. In Shamir secret sharing based on Lagrange's interpolating polynomial, there are *'n'* shareholders $P = \{P_1 \ldots P_n\}$ and a mutually trusted dealer D. By using *(k, n)* threshold scheme [17] with $n=2k-1$, we can recover the original key even when $[n/2] = k-1$ of the *'n'* pieces are destroyed, but the other members cannot reconstruct the key even when keys are expose to $[n/2] = k-1$ of the remaining 'k' pieces. This scheme basically consists of two algorithms

1) Share generation algorithm and

2) Secret reconstruction algorithm

1) Share generation algorithm: The dealer D first selects a random polynomial $f(x)$of degree $t-1$: $f(x) = a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$in which $s = a_0$ and all the coefficients $a_0, a_1 \ldots a_{t-1}$ is in the finite field $F_p = GF(P)$ with *'p'* elements. D computes n shares $(s_1, s_2 \ldots s_n)$ as

$$s_1 = f(1), s_2 = f(2) \ldots\ldots s_n = f(n).$$

The dealer distributes each share s_i to shareholder P_i secretly.

2) Secret reconstruction algorithm: For any t shares $(s_{i1}, \ldots\ldots, s_{ik})$ where $(i_1, \ldots\ldots, i_t) \subset \{1,2, \ldots\ldots, n\}$, the secret s can be reconstructed.

Thus the basic requirement of the secret sharing scheme is

1) With the knowledge of any t or more than t shares, shareholders can reconstruct the secret

2) With the knowledge of any t-1 or fewer than t-1 shares, shareholders cannot reconstruct the secret S.

5.3. Detailed Working Of The Secure Key Sharing (Sks) Scheme

The Lagrange's interpolation and the Shamir secret sharing scheme have been handled differently in our solution. The source generates a polynomial $q(x)$ and assumes the value of p and D. Here, the constant value in the polynomial is considered as 'D' and this value is the super key. After the polynomial generation by source, then the source substitutes random values into the polynomial and gets number of corresponding outputs and sends to the each node connected to it. These values are encrypted using the public key of the nodes which has been generated using RSA [18][19] algorithm. The receiver decrypts the encrypted message with its private key. Then for verification the connected nodes are asked to send the values that they have received it from the source. These values when sent back to source, is been encrypted using public key of the source. After receiving the values, the source node decrypts it and substitutes it in the polynomial and check whether it arrives to the super key or not. If the source arrives to the super key then all the nodes that have sent the values are genuine nodes. If the super key is not arrived, then any of the nodes is considered to be malicious nodes. Thus with the help of this theorem we can identify the malicious nodes that are present in the network.

This scheme is based on polynomial interpolation. Given k points in the 2-dimensional plane $(x_i, y_i) \ldots\ldots\ldots, (x_k, y_k)$, with distinct x_i's, there is one and only polynomial $q(x)$ of degree $k-1$ such that $q(x_i) = y_i$ for all i. Without loss of generality, we can assume that the data D is number and can be divided into pieces D_i, then pick random $k-1$ degree polynomial $q(x) = a_0 + a_1x + \ldots\ldots + a_{k-1}x^{k-1}$in which $a_0 = D$, and evaluate

$$D_1 = q(1) \ldots \ldots \ldots D_i = q(i) \ldots \ldots \ldots D_n = q(n).$$

Given any subset of k of these D_i values (together with identifying indices), we can find the coefficient of $q(x)$ by interpolation, and then evaluate $D = q(0)$.Knowledge if those $k-1$ values does not suffice in order to calculate the value D.

Let *p* be prime number exceeding *k* and *n*. Let $D < p$. Choose a random k-1 degree polynomial

$$q(x) = a[0] + a[1]x + a[2]x^2 + ... + a[k-1]x^{k-1}$$

with a*[0] = D* and the co-efficients $a[i] \in Z_p$ for $i = 1,2,3, ..., k-1$.Defining

$$D_i = q(i) \ (mod\ p)$$

For $i=1,2,...n.$ Then n D_i pieces will be distributed to all nodes .We can construct the number D from any of the k D_i pieces with their node ID's. Consider a subset of k of these D_i pieces, say D_{i1}, $D_{i2..}, ...$ D_{ik}. By Lagrange's interpolation we can find unique polynomial *f(x)* of degree at most *k-1* such that $f(i_j) = D_{ij}$ for $j=1, 2... k.$ such that polynomial *f(x)* is given by

$$f(x) = \sum_{r=1}^{k} Di_{\,r} \prod_{\substack{j=1 \\ j \neq r}}^{k} \frac{(x - i_j)}{(i_r - i_j)}$$

Since *q(x)* and *f(x)* satisfy the same hypothesis, by uniqueness of Lagrange's interpolation $f(x) = q(x)$ for all $x \in Z_p$. In particular *q[0] = f[0]*. Hence

$$D = q[0] = \sum_{r=1}^{k} Di_{\,r} \prod_{\substack{j=1 \\ j \neq r}}^{k} \frac{(i_j)}{(i_j - i_r)}$$

with this the value of D can be reconstructed.

6. ANALYSIS OF SECURE KEY SHARING (SKS) SCHEME

As by the proposed solution, the source node generates a polynomial of its own and just substitutes the random values for different participating nodes. An attacker cannot impersonate the source because the process of guessing the polynomial is very complicated and very tedious work. After generation of keys for all participating nodes, it then transmits it to the concern node through the communication channel. An attacker tries to capture the packets that transmit to the channel and look for information. If the data is sent as raw data, it is vulnerable and is easier for an attacker node to impersonate the intercepted node on the future. Here in our scheme, we use encrypted transmission using RSA, a public key encryption system. As the source node uses RSA for encryption, the data should be encrypted using the receiver's public key and only the receiver's private key alone can decrypt the value. When the attacker intercepts or interrupts the communication channel, it can receive only the encrypted packet and cannot decrypt because attacker does not possess the corresponding private key. This method, not only provide security to the data using encryption but also it provides security against various attacks. Consider the scenario, where the attacker captures the packets from the communication channel and it tries to reply the same packet to the source or any other node in the network ends up in a failure, because the packet that is sent is encrypted using the corresponding public key of the nodes and cannot impersonate other nodes in the network.

The idea of secret sharing is to generate a secret and send it to the participating nodes in the network. But the basic security nature of this scheme lies in the polynomial that is generated by the source node and the consideration of the prime number by the source node. For identification of the malicious nodes in the network, it requires n-1 node values as an input. But the main advantage of this scheme is that, it does not increase the network congestion by repeatedly transmitting values in the network, rather the computation complexity of the source node alone increases, which thereby does not the affect the entire network.

7. SIMULATION AND RESULTS

We conducted our experiments using Glomosim version 2.03.Our simulated network consists of 14 mobile nodes placed randomly within a 1000 m x 1000 m area. Each node has a transmission range of 250 m and moves at a speed of 1 m/s. The total sending rate of all the senders of the multicast group, i.e., the traffic load, is 1 packet/s. We use a low traffic load value to highlight the effects of the attacks on packet loss rate, as opposed to packet loss due to congestion and collisions resulting from a high traffic load. The mobility model chosen for a mobile node was the random way-point model. A mobile node begins by staying in one location for a pause time of 30 seconds. Once this time expires, the mobile node chooses a random destination in the simulation area and then travels toward the newly chosen destination. Upon arrival, the mobile pauses for 30 seconds before starting the process again. The attackers were positioned around the center of the multicast mesh in all experiments; the duration of each experiment was 300 seconds in simulated time. Every experiment was repeated 10 times using 10 different randomly generated seed numbers, and the recorded data was averaged over those runs.

The simulation has been done with three types of attack solutions and the corresponding results are documented and the graphs are drawn comparatively. The three attack solutions are Statistical Analysis, Trust based system and my proposed system secure key sharing. One of the network characteristics namely network overhead is considered as a parameter for drawing the first graph. The parameter considered is the number of nodes in the network and the overhead that each node creates in the network thereby it becomes the network overhead. On the comparative based study that have been taken, the graph is drawn which shows that the proposed solution, the secure key sharing is better than the existing solution

On calculating the network overhead, the statistical analysis solution has more overhead when compared to other two solutions because it continuously monitors other nodes for malicious activity and updates it to the other nodes present in the network by transferring the update packet at specified time interval, so the network overhead is constantly increasing when then number of nodes present in the network increases. Trust based solution also has more network overhead that secure key sharing scheme because the transmission of trust table periodically between network nodes in order to update the trust value for each node causes more packets to be transmitted in the network. During the secret key sharing scheme, the network overhead does not increase because only the transmission of one key request packet and key response packet from source to destination occurs which make the network overhead nearly a negligible quantity.

When the node overhead is taken into account, the statistical analysis and trust based solution has more node overhead because all the nodes in the network performs the operation of gathering the data corresponding to the current network status and updates it to the other nodes by transmitting update packets. But in the proposed system, only the source node has more

computation than any other nodes because there are no operations done during the network operation for finding the malicious nodes.

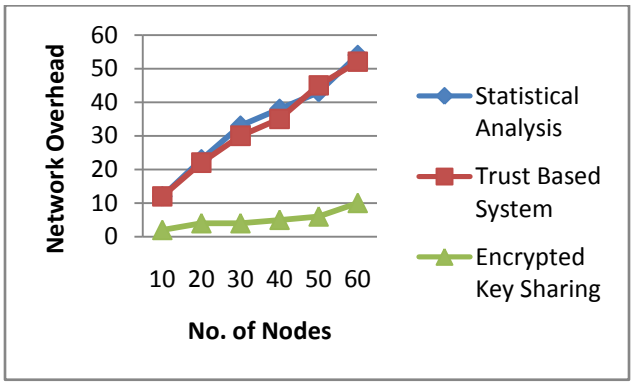

Figure 1: Network overhead

By using the trust based solution the attack identification percentage is less than statistical analysis and secure key sharing because if the node is mistrusted to be a trusted node. By using statistical analysis the number of attackers identified is less when compared to secure key sharing because the analysis is sent using the update packet and there occurs a threat if the update packet is lost during transmission. The proposed solution sharing identifies more number of attackers than statistical analysis and trust based solution because it uses key sharing scheme where the super key can be achieved using keys from minimum number of nodes. If the source node arrives at the super key then the nodes that have transmitted the keys are genuine nodes.

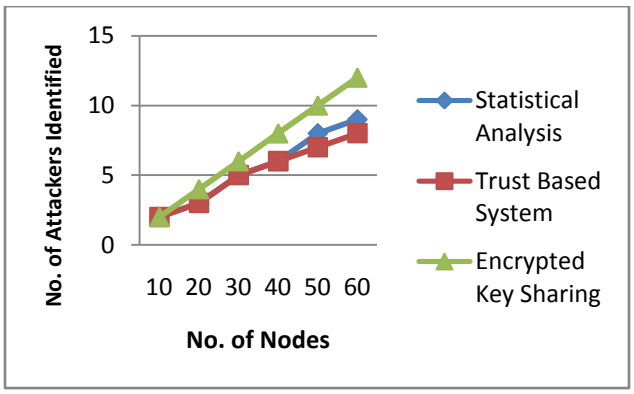

Figure 2: Identification of Attackers

8. CONCLUSION

Thus the solution that has been proposed for the security of MANETs against attacks like flooding, wormhole, blackhole etc, has been achieved. This provide a secure routing for all tree based multicast routing protocols such as ADMR, MAODV etc., With this scheme it is easier for the source node to identify the malicious nodes that enter the network without authorization. This solution is very much applicable in the situation where the attacker enters the network and tries to impersonate themselves as legitimate nodes in the network. This solution is designed only for the external attacker that claims to be as genuine nodes. The future enhancement for this scheme is to provide suitable solution for other type of attackers and also to extend the solution for the mesh based protocols also.

9. REFERENCES

[1] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, 78-91, First Quarter 2009.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, "Survey of routing attacks in Mobile Ad-Hoc Networks", IEEE wireless communication, pp. 85-91, October 2007.

[3] Kumar Viswanath, Katia Obraczka, Gene Tsudik, "Exploring Mesh and Tree-Based Multicast Routing Protocols for MANETs", IEEE Transactions on Mobile Computing, Vol. 5, NO.1, pp. 28-42, January 2005.

[4] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Ad-Hoc Networks 2, ELSEVIER, pg. 1-22, 2004.

[5] E. M. Royer, and C. E. Perkings, "Multicast Operations of the Ad-hoc On-Demand Distance Vector Routing Protocol", In Proceedings of ACM/MOBICOMM, August 1999.

[6] Jorjeta G. Jetcheva, David B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", International symposium on Mobile Ad Hoc Networking and Computing, 33-44, (MobiHOC) 2001.

[7] Jorjeta G. Jetcheva, "The Adaptive Demand-Driven Multicast Routing Protocol for Mobile Ad Hoc Networks (ADMR)", IETF Internet draft, draft-ietf-manet-admr-00.txt, July 2001.

[8] S.J. Lee, M. Gerla, and C. C. Chiang, "On Demand Multicast Routing Protocol", In Proceedings of IEEE WCNC'99, pp. 1298-1302, September 1999.

[9] J.J. Garcia-Luna-Aceves, and E. L. Madruga, "The Core-Assisted Mesh Protocol", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1380-94, August 1999.

[10] Yun Ge, Guojun Wang, Weijia Jia, Yongming Xie, "Node - Disjoint Multipath Routing with Zoning Method in MANETs", The 10th IEEE International Conference on High Performance Computing and Communications, pp. 456 - 462, August 2008.

[11] Sunil Taneja, Ashwani Kush, "A survey of routing protocols in Mobile Ad-Hoc NETworks", International Journal of Innovation, Managment and Technology, Vol 1. No. 3, August 2010.

[12] L. Ertaul and N. Chavan," Security of Ad Hoc Networks and Threshold Cryptography", International Conference on Wireless Networks, Communications and Mobile Computing, vol.1, pp.69- 74, 2005.

[13] A. Shamir, "How to share a secret?", Comm. ACM, vol. 22, no. 11, pp.612-613, 1979.

[14] Hugo Krawczyk, "Secret sharing made short", Springer - Verlag, 1988.

[15] Sarkar, B.Kishu, S.Mishra, M.S.Obaidat, "Chinese Remainder Theorem Based RSA - Threshold Cryptography in MANET Using Verifiable Secret Sharing Scheme", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 258-262, November 2009.

[16] L. Ertaul and N. Chavan, "Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs", International Journal of Computer Science and Network Security, vol.7, No.4, April 2007.

[17] Lein Harn, Changlu Lin, "Strong (n, t, n) verifiable secret sharing scheme", ELSEVIER, Information Sciences 180, 3059 - 3064, 2010.

[18] Tom. M. Apostol, "Introduction to Number Theory", Springer – verlag, New York, 1976.

[19] Neal Koblitz,"A Course in Number Theory and Cryptography", Springer, 1987.