Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 1, January 2016, pg.327 – 333

Secured and Intelligent Multipath Routing Approach using AOMDV in Manet

Rashmi Gupta, Mr. Ramesh Chandra Sahoo, Maneesh Kumar
Department of Computer science and Engineering, NIET, Greater Noida, India
Assistant Professor CSE Department, NIET, Greater Noida, India
rashmigupta2904@gmail.com
rsahoo22@gmail.com
maneeshniet1987@gmail.com

Abstract— There are two type of communication network used for communication purpose first one is Traditional wireless network and second is mobile Ad hoc network . Mobile Ad hoc network is better option than Traditional Ad hoc network due to its independent nodes and no central administration required. In MANET, sensor nodes are battery operated because it is a limited resource therefore it requires attention to minimum consumption of energy in MANET.
In this paper, the main focus is on the energy of the sensor nodes and security of the sensor nodes. As AODV is traditional algorithm for mobile Ad hoc network, the concept of AODV is used in modified fashion to get the multiple paths in single route discovery phase for minimum energy consumption. And for security purpose we use the two well known cryptographic algorithms RSA and Diffie Hellman one by one find which gives best performance in terms of time taken.
Results show that the diffie hellman key exchange algorithm provide better results while compare with the RSA key generation algorithm in terms of time taken.

I. INTRODUCTION

IN MANET'S world, devices such as laptops, PCs, cellular phones, appliances with ad hoc communication capability link together on the fly to create a network. This technology is the key to solving today's most common communication problems such as having a fixed infrastructure, and centralized, organized connectivity, etc. MANET is a self configuring network of mobile routers and associated hosts connected by wireless links. The routers (mobile devices, nodes) are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. The network appears on-demand, automatically and instantly, and data hops from ad-hoc device to device till it reaches its destination, the network updates and reconfigures itself to keep nodes connected. The network topology changes when a node joins in or moves out. Packet forwarding, routing, and other network operations are carried out the by the individual nodes themselves [2].

In MANETs with each node acting as a router and dynamically changing topology the availability is not always guaranteed. It is also not guaranteed that the path between two nodes would be free of malicious nodes. The wireless links between nodes are highly susceptible to link attacks (passive eavesdropping, active interfering, etc). Stringent resource constrains in MANETs may also affect the quality of security when excessive computations is required to perform some encryption. These vulnerabilities and characteristic make a case to build a security solution, which provides security services like authentication, confidentiality, integrity, non-repudiation and availability. In order to achieve this goal we need a mechanism that provides security in each layer of the protocol. [1], [2]

© 2016, IJCSMC All Rights Reserved

Cryptography is the art and science of keeping messages secure. Basically, the point of cryptography is to allow any user to keep his data secure and not readable from not desired individuals. Distributed Cryptography is the method of key distribution or distribution of trust to among nodes. Distributed Cryptography ensure the availability of nodes, even if some of the information is lost still the actual message reaches the intended receiver without compromising the security. Distributed Cryptography can be implemented using RSA, Elliptic Curve Cryptography (ECC) and Digital signature. Distributed cryptography involves sharing of a key by multiple individuals called shareholders engaged in encryption or decryption [3].

II. OBJECTIVES

In MANET environment, communication node usually attempt to find other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes.

In our proposed system we have two objectives first is to find the multiple routes in single route discovery phase and the second objective is to make these routes network attacks free. For achieving first objective we modified AODV routing protocol and for achieving second objective we use two well known cryptographic algorithms called RSA and Diffie Hellman. We apply this algorithm one by one on the modified AODV and find which algorithm gives the better results in term of time taken. Communication over the network using Cryptography Mechanism for providing security. Our main aim is to compare the performance of these two algorithm on our proposed system and find which one give better performance.

III. RELATED WORK

Ye et al. [4] have proposed an alternative protocol called AODVM that extends AODV to find node disjoint paths. In addition, they study the impact of node density on number of node-disjoint paths and the utility of placing special reliable nodes to improve overall network reliability. Compared to AOMDV, AODVM may incur higher overhead as it precludes RREP generation by intermediate nodes; moreover, it cannot find link disjoint paths like AOMDV. There are other related alternate path routing protocols which do not consider path disjointness [5,6]. AODV-BR [5] is an enhancement to AODV for utilizing routes maintained at neighboring nodes (via overhearing) as backup routes when the primary route fails, thereby reduce loss of data packets in flight. Specifically, AODV-BR does a local broadcast of the data packet when the primary route fails requesting other nodes in the neighborhood to salvage the data packet. Note that this is somewhat similar to the alternate routing mechanism mentioned in Reference [7]. Also note that AODV-BR is not a true multipath protocol as every node still has at most one route per destination like in AODV. Recently, a similar but more sophisticated protocol called CHAMP [6] was proposed. In contrast to AODV-BR, CHAMP maintains multiple shortest loop-free paths at each node, and the node upstream of the node that has all paths invalidated salvages the data packets using an alternate path. Other on-demand hop-by-hop protocols [8,9] rely on inter-nodal coordination to determine multiple loop free paths as opposed to our approach to use destination sequence numbers. In addition, these protocols do not take path disjointness into account. TORA [8] is an on-demand, multipath protocol which combines the source-initiated route creation in LMR [10] with the link reversal technique from Reference [11] for localized recovery from route failures. The class of 'link reversal' algorithms [11] seek to maintain a destination-oriented directed acyclic graph (DAG). In these algorithms, whenever a link failure at a node disorients the DAG (i.e., the node has no downstream links to reach the destination), a series of link reversals starting at that node can revert the DAG to a destination oriented state.

Wan An Xiong, et, al [12] [2011] discusses about Elliptic curve Cryptography, Identity based Cryptography and Shamirs (t,n) threshold cryptography. Nonlinear pair computation is applied to realize secure key management and communication. Shamirs (t,n) threshold cryptography is used to build three level security in ad hoc network. This scheme can be applied to dynamic topology and different sizes of ad hoc network. This scheme does not require any certificate management. It can get a high security with few traffic and computation. It does not give any simulation proofs. Also the three level topology can be replaced by SRT that uses simple topology with reduced overhead.

Maria Celestin Vigila S, et, al [13] [2009] discusses the implementation of text based Elliptic Curve Cryptosystem. Each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an a fine point on the EC, by using a starting point called Pm. Transformation of the plaintext ASCII value by using an affine point is one of the contributions of this work. The purpose of this transformation is two folds. Firstly a single digit ASCII integer of the character is converted into a set of co-ordinates to fit the EC. Secondly the transformation introduces non-linearity in the character thereby completely camouflaging its identity. This transformed character of the message is encrypted by the ECC technique. Decryption of ECC encrypted message is itself quite a formidable task, unless we have knowledge about the private key 'nB' ,the secret integer 'k' and the affine point Pm. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are constrained. Such applications include chip cards,

© 2016, IJCSMC All Rights Reserved

electronic commerce, web servers and cellular telephones. One of the applications that the ECC can be used for is encryption of large image files. The selection of the primes and the faster multiplication and doubling algorithms are the focus of research, the image encryption using ECC is completely a new domain and has tremendous scope of research.

Durgesh Wadbude, et al, [14] [2012] proposes an approach that uses improved security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and the Protocol Enforcement Mechanism. The performances of these two protocols (SAODV and ARAN) were tested in simulation and their communication costs were measured using the NS-2 simulator, which is suitable for the present purpose. The evaluation metrics used are overhead and end to end delay. In proposed scheme along with digital signature and hash chain ECC points are used for generation of secret key.

Prakash Kuppuswamy, et al, [15] [2012] proposes method of Digital Signature Scheme based on the linear block cipher or Hill cipher. It is basically symmetric key algorithm. Digital Signatures can provide added assurances of the evidence to identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. But this method is a conventional method

Bin Sun et al, (2009) [16] analyses three layered key management architectures to Mobile Ad hoc networks (MANET) with three-layered virtual infrastructure. Two kinds of three layered key management architectures are introduced. The communication efficiency of them has been
analyzed. It also shows that the communication cost of the three-layered key management schemes is always smaller than that of the two layered ones. These two conditions can be used to optimize the MANET virtual infrastructure protocol. It also shows that the communication cost of the three layered key management schemes is always smaller than that of the two-layered ones.

Fiat A et al, (1999) [17] proved the signature and identification scheme which enables the user to prove the identity and the authenticity of the message to other users without shared or public keys. This scheme is secure against any known or chosen message attack. It is very simple and secure and it is suited for microprocessor devices.
Menezes A et al, (1991) [18] analyses the reduction of the elliptic curve logarithm problem to the logarithm problem in the multiplicative group of an extension of the underlying finite field.

Haiyun Luo et al, (2004) [19] analyses ticket certification services through multiple node consensus and fully localized instantiation. It uses tickets to identify and grant network access to well behaving nodes. In URSA, no single node monopolizes the access decision or is completely trusted. Instead, multiple nodes jointly monitor a local node and certify its ticket. Experimental and simulation results are analyzed for various parameters.

Jin-Hua Hong et al, (2009) [20] implements Elliptic Curve Cryptography on GF (2163) using polynomial at the base. The encryption and decryption is implemented on the ECC chip, which needs fast operation and low hardware resources.

Gaga deep et al, (2012) [21] and Nishu Garg et al, (2009) focuses the various types of attacks on various layers under protocol stack. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs.
T. Kiran, T. P. Anish el .at.[24] Number of techniques has been used based on packet encryption to protect the data forwarding in MANETs, Still MANETs are attacked by hackers. To get over these attack a new technique called statistical traffic pattern discovery system can be used. It is an approach to discover entire raw traffic by using probability of traffic characteristics. It discover the relationships of source to destination communication. Maximum in wireless ad hoc network, it will always choose shortest path in prior. So attackers shall enter the network freely, because if the node monitors the packet forwarding mechanism it can easily identify the entire traffic pattern in the system. Based on the activity of hacker will enter the network effectively. It can be helpful for dropping or modifying data. But here we choose the second shortest path for data forwarding. In our scenario when we change to select the routing path hackers can't be capture the current routing path.
Neha B. Bhoyar, Prof. Poonam P. Borkar el.at.[25] Mobile Ad-hoc Network (MANET) consists of mobile nodes that are connected via very dynamic multihop channels. Routing in MANET is a challenging task. This is primarily due to their infrastructure less property of MANET. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. For instance, the presence and

© 2016, IJCSMC All Rights Reserved

collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. This work aims to identify the malicious nodes by using the novel approach called Acknowledge Based Route Discovery (ABRD), and also to provide alternative path using multipath routing algorithm, if such malicious node/nodes detected in routing path, during the route discovery. And also maintain blacklist of such malicious nodes so that all the nodes can be alerted not to use any route in which detected malicious node is participating.

Ms. Antima Jain, Dr. Suresh Jain , Mr. Abhishek Gaur, Ms. Manu Singh el.at.[26]
In the MANET (mobile ad-hoc network) important challenge in congestion control mechanism because how the sender know about network congestion and adjust the rate, so our objective is to work in the challenging field of congestion control for minimization waiting time as well as dropping of data packet and we design an congestion control with load balancing using multipath routing mechanism in mobile ad-hoc network, so that we eliminate congestion as well as we can minimize routing overhead of the network and also increase the packet delivery ratio of the network. For that purpose we will propose Congestion control with load balancing using AOMDV routing in MANET. Our protocol will ensure that there will be no dropping of packets in the network through the congestion and hence ensure that there will be successful data transfer with lowest overhead required.

Arminder Kaur, Dr. Tanu Preet Singh el.at.[27] Mobile ad hoc networks (MANETs) are highly vulnerable as there is no presence of trusted centralized authority and dynamic network topology. Due to such characteristics of MANET various kind of attacks are possible. Jellyfish (JF) is a new denial of service attack. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. In this paper we have proposed a secure technique in TORA protocol using selective node participation approach to diminish the impact of Jellyfish attack in MANET. The selective node participation approach identifies JF nodes during route creation and assigned it as an inactive and selects a subset of nodes to participate as part of the network.

IV. PROPOSED SYSTEM

In proposed system we proposed multipath routing approach using AOMDV. AOMDV shares several characteristics with AODV. It is based on the distance vector concept and uses hop-by-hop routing approach. Moreover, AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. The core of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjoint, and in efficiently finding such paths using a flood-based route discovery. AOMDV route update rules, applied locally at each node, play a key role in maintaining loop-freedom and disjointness properties. Here we discuss the main ideas to achieve these two desired properties. AOMDV relies as much as possible on the routing information already available in the underlying AODV protocol, thereby limiting the overhead incurred in discovering multiple paths. In particular, it does not employ any special control packets. In fact, extra RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) constitute the only additional overhead in AOMDV relative to AODV

Now our next goal is to provide security using Diffie hell man and RSA algorithm separately and then compare their performance on the basis of timing. To achieve this, when the RREP route reply packet is unicast to the source from destination it checks each intermediate node with the help of encryption algorithm.

V. RSA ALGORITHM

Rivest-Shamir-Adleman (RSA). A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs, including Pretty Good Privacy (PGP). RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It is still widely used in electronic commerce protocols, and isR believed to be secure given sufficiently long keys. The RSA scheme is a block cipher. Each plaintext block is an integer between 0 and $n - 1$ for some n, which leads to a block size $\leq \log2 (n)$. The typical block size for RSA is 1024 bits [22].

1) World's most popular Asymmetric Key Encryption algorithm
2) Based on the theory of Prime Numbers
3) Algorithm is based on the fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.
4) The private and public keys in RSA are based on very large (100 or more digits) prime numbers.
5) Real challenge in the case of RSA is the selection and generation of public and private keys.

© 2016, IJCSMC All Rights Reserved

Steps of this algorithm are as:

1) Choose two large prime numbers P and Q.
2) Calculate N = P x Q.
3) Select the public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q -1).
4) Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1.
5) For encryption, calculate the cipher text CT from the plain text PT as follows: CT = PTE mod N
6) Then send CT as the cipher text to the receiver.
7) For decryption , calculate the plain text PT from the cipher text CT as follows: PT = CTD mod N

Limitations of RSA are as:

1) Every RSA initialization process requires the random selection of two very large prime numbers (p and q).
2) In the real world the encryption capabilities of RSA are rarely used for one simple reason: the length of plain text that can be encrypted is limited to the size of n=p*q.
3) RSA is much slower than DES and other symmetric cryptosystems.
4) If any one of p, q, e, d is known, then the other values can be calculated. So secrecy is important.
5) To protect the encryption, the minimum number of bits in n should be 1024

VI. DIFFIE HELLMAN ALGORITHM

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure Connectivity protocols on the Internet. In an era when the lifetime of "old" technology can sometimes be measured in months, this algorithm is now celebrating its 25th anniversary while it is still playing an active role in important Internet protocols.

DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. A shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec). These protocols will be discussed in terms of the technical use of the DH algorithm and the status of the protocol standards established or still being defined [23].

Steps of this algorithm are as:

1) Taking two numbers "P" and "G" "P" is a large prime number "G" is called the base or generator.
2) Picks a secret number "A" as first secret number = A, then picks another secret number "B" as second secret number = B.
3) Computes first public number X = G A mod P, and public number = X. Then computes second public number Y = GB mod P, and public number = Y.
4) Exchange their public numbers.
5) First knows P , G , A, X, Y, Second knows P, G, B, X, Y.
6) Computes First session key as KA = Y A mod P OR KA = (G B mod P) A mod P OR KA = (G B) A mod P OR KA = G BA mod P.
7) Computes second session key as KB = X B mod P OR KB = (G A mod P) B mod P OR KB = (G A) B mod P OR KB = G AB mod P. m

Limitations of Diffie Hellman key Exchange are as:

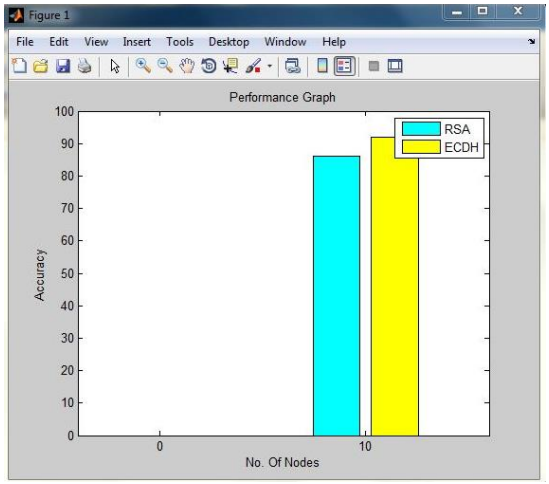
1) There is no identity of the parties involved in the exchange.
2) It is easily susceptible to man-in-the-middle attacks. A third party C, can exchange keys with both A and B, and can listen to the communication between A and B.
3) The algorithm is computationally intensive. Each multiplication varies as the square of n, which must be very large. The number of multiplications required by the exponentiation increases with increasing values of the exponent, x or y in this case.
4) The computational nature of the algorithm could be used in a denial-of-service attack very easily.
5) The algorithm cannot be used to encrypt messages.
6) There is also a lack of authentication.

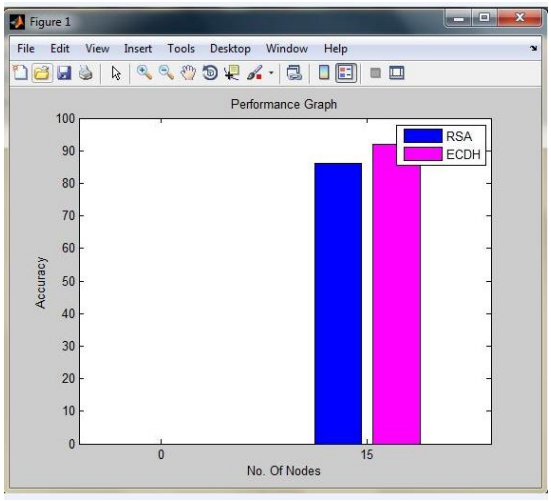
© 2016, IJCSMC All Rights Reserved

VII. AOMDV ALGORITHM

1: If($seq\_num^d_i < seq\_num^d_j$) then{/* enforces the sequnces number rule */}
2: $Seq\_num^d_i = seq\_num^d_j$;
3: advertised $hop\_count^d_i = \infty$;
4: $route\_list^d_i$ =NULL
5: If(j=d)then {/* neighbor is the destination */}
6: Insert (I,j,1) into route $list^d_i$;
7: else
8: Insert (j,$last_hop^d_{jk1}$advertised_hop_$count^d_j$+1) into $route\_list^d_i$;
9: end if
10: else if(($seq\_num^d_i = seq\_num^d_j$) and (advertised_hop_$countd_i$ > advertised_hop_$count^d_j$)) then {/* enforces the route acceptance rule */}
11: If(j=d) then {/*neighbor is the destination */}
12: If ((/ $^{\exists}k_1$: {$next\_hop^d_{ik1}$= j)} and (/$^{\exists}k_2$: ($last\_hop^d_{ik2}$= j))) then {/* establishes uniqueness of next and last hops */}
13: Insert {j,I,1} into $route\_list^d_i$;
14: else if
15: else if ((/$^{\exists}k_3$: ($next\_hop^d_{ik3}$=j)) and (/$^{\exists}k_4$: ($last\_hop^d_{ik4}$ = $last\_hop^d_{ik}$) then { /* establishes uniqueness of next and last hops */}
16: Insert (j, $last\_hopd_{jk}$ advertised_hop_$count^d_j$+ 1) into $route\_list^d_i$;
17: end if
18: end if

VIII. RESULT





© 2016, IJCSMC All Rights Reserved

IX. CONCLUSION

One of the main challenges in the design of routing protocols for WSNs is energy efficiency due to the scarce energy resources of sensors. The ultimate objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. The energy consumption of the sensors is dominated by data transmission and reception. Therefore, routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network lifetime.

In this paper, first we create our own multipath routing algorithm which is inspired from AODV algorithm. In our work first we apply RSA algorithm for security purpose and then we apply Diffie Helman for the security purpose and we find that the diffie hellman takes less time when it compared to RSA algorithm. So we conclude that Diffie helman takes less time in compare to RSA algorithm. So it is well fit for our multipath routing algorithm.

REFERENCES

[1] Y . Hao et al . , " Security In Mobile Ad Hoc Networks: Challenges and Solutions " , IEEE Wireless Communications, 2004.

[2] A . Mishra , and K . Nadkarni , " Security in MANETs", The handbook of wireless ad hoc networks, 2002.

[3] Elliptic Curve Cryptography Threshold Cryptography Levent Ertaul , IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April 200748.

[4] Ye Z , Krishnamurthy S V , Tripathi SK . A framework for reliable routing in mobile ad hoc networks. In Proceedings of IEEE Infocom, 2003.

[5] Lee S J , Gerla M . AODV – BR : backup routing in ad hoc networks. In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), 2000.

[6] Valera A, Seah WKG, Rao SV. Cooperative packet caching and Shortest multipath routing in mobile ad hoc networks . In Proceedings of IEEE Infocom, 2003.

[7] Jubin J , Tornow JD. The DARPA packet radio network protocols. Proceedings of IEEE 1987; 75(1): 21–32.

[8] Park VD , Corson MS. A highly adaptive distributed routin algorithm for mobile wireless networks. In Proceedings of IEEE Infocom, 1997.

[9] Raju J , Garcia-Luna-Aceves JJ. A new approach to on-demand loop-free multipath routing. In Proceedings of Int'l Conference on Computer Communications and Networks (IC3N), 1999

[10] Corson MS , Ephremides A . A distributed routing algorithm for mobile wireless networks. Wireless Networks 1995; 1(1): 61–81.

[11] Gafni E , Bertsekas D . Distributed algorithms for generating loop-free routes in networks with frequently changing topology. IEEE Transactions on Communications 1981; 29(1): 11–18.

[12] Wan An Xiong , Yao Huan Gong , " Secure and Highly Efficient Three Level Key Management Scheme for MANET", proceedings of WSEAS transactions on computers, Volume 10, 2011 pp. 6-15.

[13] Maria Celestin Vigila S, Muneeswaran K, "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", IEEE, Volume 9, 2009, pp. 82-85.

[14] Durgesh Wadbude , Vineet Richariya , " An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274 -279.

[15] Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher", IOSR Journal of Computer Engineering (IOSRJCE), Volume 7, Issue 1, 2012, pp. 47-52.

[16] Bin Sun and Bin Yu , " The Three – Layered Group Key Management Architecture for MANET", proceeding of 11th International Conference Volume 02, 2009, pp. 15-18.

[17] Fiat A and Shamir A , " How to Prove Yourself: Practical Solutions to Identification and Signature Problems" proceedings of the Springer-Veriag, 1999, pp. 306-314.

[18] Menezes A, Okamoto T and VanstoneL S, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", journal of information theory, IEEE transaction, Volume 39, 1991, pp. 1639-1646.

[19] Haiyun Luo , "URSA Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", IEEE/ACM transactions on networking, Volume 12, No. 6, 2004, pp. 1049-1063.

[20] Jin – Hua Hong , Wei - Chung Wu , " The Design of High Performance Elliptic Curve Cryptographic", IEEE, Volume 9, No.9, 2009, pp. 527-530.

[21] Gagandeep , Aashima , Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Volume 1, 2012, pp 269-275.

[22] Dynamic Authenticated Secure Group Communication R. Aparna, and B. B. Amberker World Academy of Science, Engineering and Technology 34 2007.

[23] Y. Desmedt and Y. Frankel, "Threshold cryptosystems", in Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara: Springer-Verlag,1990, pp. 307-315.

[24] T. Kiran, T. P. Anish," Secure Hidden Routing in Mobile Ad Hoc Networks", Volume 5, Issue 4, April 2015

[25] Neha B. Bhoyar, Prof. Poonam P. Borkar," Neha B. Bhoyar, Prof. Poonam P. Borkar", Vol. 3, Issue 4, April 2015

[26] Ms. Antima Jain, Dr. Suresh Jain , Mr. Abhishek Gaur, Ms. Manu Singh," A Study of Novel Congestion control with load balancing using AOMDV routing in MANET", International Journal of Emerging Technology and Innovative Engineering Volume I, Issue 4, April 2015

[27] Arminder Kaur, Dr. Tanu Preet Singh," Securing MANET from jellyfish attack using selective node participation approach", International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-4, April 2015

© 2016, IJCSMC All Rights Reserved