ISSN:0975-9646

Hybrid Security Using Digital Signature & RSA Encryption for AODV in MANET

Shelbala Solanki, Anand Gadwal

Department of Computer Science & Engineering
Truba College of Engineering and Technology Indore(M.P), India

Abstract -Mobile ad-hoc network offers an effective way of short range communication with infrastructure less environment. In this wireless network the routing is performed by node itself without any centralized administrative controls. It also supports dynamic topologies which causes heavy movement of nodes within a specific range. In such environment, verifying the nodes authenticity and achieving data confidentiality is a challenging task. Unlike the wired medium, infrastructure less networks has not accumulated with proper security controls. It causes high attack rates such as DoS, impersonation, fabrication, blackhole, spoofing etc attacks associated with data drops and performance reductions. Apart from these MANET suffers from various security vulnerabilities. Such networks can only assure protection of data and control packets by identifying the nodes reliability with a robust authentication and signature mechanism. Also the protocol developed for MANET must be of light weight in nature which results fewer overhead and resource consumptions. This work proposes a hybrid security mechanism for MANET using digital signature and cryptosystem. Here the cryptosystem is developed using well known public key algorithm RSA and the digital signature is achieved using SHA-I. The work will protects both category of information is the packet i.e. data and control information such a shop count values. Here the work introduces with each node verification comes in the participating route for communications. The performances of this solution will be evaluated through the NS2 based simulation on different parameters. It will also allow us to check the correctness of the protocol and to estimate the control traffic generated under different operating conditions. Finally while developing this solution, its effectiveness and robustness was proving the fitness and workability of the approach.

Index Term: Ad-Hoc Network, MANET, Secure AODV, Confidentiality, RSA, Authentication, Digital Signature (SHA-I);

I. INTRODUCTION

Ad-hoc network is a network form by the group of nodes communicating with each other without any fixed infrastructural elements. The connection establishes only for the purpose of communication between the nodes in a specific range. Here each node will serve as a router which supports the communication protocols without any centralized controlling system and called as self organized also. Apart from the above characteristics the ad-hoc network is adaptive in nature. It can take different forms and has highly variable mobile characteristics such as power and transmission conditions, traffic distribution variations, and load balancing.

Ad-hoc network is having the wide range of protocols for supporting the motion based communication with dependencies of mobile devices. Thus the requirements must be satisfied in lightweight medium. Fundamentally the routing protocol delivers the messages from source to destination with enhanced performance in terms of delay and security. The functionality of routing protocol is to discover network topology along with the route formation for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes [1]. The routing protocol is mainly classified into three categories based on their functionality: Reactive (On Demand), Proactive (Table Driven) and Hybrid.

Security in Ad-Hoc Network

Mainly the ad-hoc network deals with the two types of packets: control packets and data packets. The nature of both the protocol is different so as their security needs. Data packets can be easily protected using some of traditional security primitives but serving same for control packets is quite complicated. The control packets or routing packets are sent to instant neighbors, processed, probably modified, and resent to the source. If there is some processing applied to the control packets then their routing information might get changed. In such communication network the intermediate nodes to be able to authenticate the information contained in the routing messages. Also the propagation or processing could not affect the actual networking control packets.

The routing packet usually contains the hop count information of the route they are requesting or providing. Therefore, in a routing message two types of information could be distinguished: mutable an non-mutable. It is desired that the mutable information in a routing message is secured in such a way that no trust in intermediate nodes is needed. Otherwise, securing the mutable information will be much more expensive in computation, plus the overall security of the system will greatly decrease.

Addressing in Ad-Hoc Network

While getting each node identified before participating in communication there must be some addressing schemes used. Some of the ad-hoc networks are assigned with dynamic IP addressing using netmask. Here the addressing schemes might get effectively used for assuring the security against the IP based communication. But dynamic IP configuration must require the server to authenticate them. Such a solution cannot be employed in ad-hoc network due to the unavailability of any centralized IP configuration server.

Some of the network based address configuration and security mechanism are applied by using IPv6 and IPSec. Although these mechanisms bring known benefits, they also open the door for new security threads, many of which have been identified during the design of security solutions for Mobile IP. The mobile ad-hoc network is having high vulnerability to both active and passive category of attacks due to their wireless links. Some of the losses involves are secret information compromise, interfering with the content, impersonation etc. Restricted communication with fixed bandwidth causes a space for the occurrence of denial of service attacks. Thus is could be easily concluded that the ad-hoc network lacks somewhere in integrity, access control and authentication. Thus, the security mechanism must be developed for serving the above requirements along with malicious source detection and preventing such attacks to occur.

II. BACKGROUND

Ad-hoc network can be categorized in various sub networks with different operating frequency ranges and characteristics. Some of these networks are MANET, WSN, Radio Network, Cognitive network, VANET, Bluetooth, and ZigBee etc. This paper focuses specifically on serving the security requirements with address configuration and identity authentications for MANET (Mobile Ad-hoc Network). The research on MANET address Auto-Configuration security is still in its early stage. Currently, the secure MANET can be developed with the help of applying some of the traditional network security primitives such as authentication, cryptography, access control, integrity etc. This work focuses its intension towards exploring AODV (Ad-Hoc on Demand Distance Vector) for security based routing. It is a reactive unicast routing protocol for mobile ad hoc networks. It is a kind of reactive protocol which only maintains the routing process information for the current active paths and connection configurations.

The AODV protocol provides dynamic multihop routing with a quick route formation using route request and route reply packets.

It will also allow mobile nodes to respond to link breakages and changes in network topology in a timely manner [2]. In AODV, routing information is maintained in routing tables at nodes. Every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route. A routing table entry expires if it has not been used or reactivated for a pre-specified expiration time. The formal routing protocols in MANET are failed to provide protection against attackers due to lack of cryptographic and other security controls. Some of the later versions of protocols include such controls.

Before developing a robust solution the types of attacks must have to be clearly elaborated. It makes the solution more effective and applicable. The attacks falls in various categories but the work restricted itself to the security against address attacks and data confidentiality. Some of those attacks are given here as [3]:

- **Address Spoofing Attack:** Without an authentication mechanism, a malicious node can freely choose any configured node as a victim, spoof its IP address, and hijack its traffic.
- **False Address Conflict Attack:** An attack may purposely transmit a false address conflict message to a targeted victim. Since the victim cannot verify the authenticity of the purposed address conflict, it may have to give up its current address and seek a new one.
- **Denial of service Attack:** An attacker could maliciously claim as many IP addresses as possible. If all valid IP addresses are exhausted by the attacker, a newly arrived node will not be able to get an IP address.
- **Negative Reply Attack:** In some previous work, the assignment of a new address requires an approval of all configured nodes. An attacker therefore may continuously send negative replies to prevent a newly arrived node from getting an address.

Secure AODV (SAODV) and Trust based AODV (TAODV) is two of them used to provide cryptographic and trust based security mechanism [4]. They usually deal with the tradeoffs of DoS attacks and their variants. For the purpose of deeply exploring the concepts secure AODV is taken as base protocol. Secure AODV is an expansion of the formal AODV routing protocol with some additional security controls such as authentication, confidentiality, non repudiation and integrity. It assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem [5]. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme. SAODV works on in two forms; fist which provides digital signature and second is hash chains for securing the hop count information from the attacker.

This paper aims to provide a deep study along with a problem based solution for improving the traditional SAODV to effectively serve the auto security and address configurations for MANET. In a way to achieve its goal there are some related works are given with the next section.

III. LITERATURE SURVEY

After the brief study about the various strategy proposed by researcher during the last few years, it is quite clear that security in MANET is a very tedious task. If the security controls affects the routing information then the connection will terminates immediately and the data will never reach to its destinations. In a way to achieve its goal the article related with our work is given below.

The paper [6] addresses the issues related to the network configuration for ad-hoc network. Here with the ad-hoc network the centralized configuration system had not existed. For authenticating the nodes in the network it must be assigned the IPS from the specific ranges. For making such network secure against the various network vulnerabilities there must be some security mechanism available with them. The paper suggested a novel security mechanism for the VASM protocol based on zero

knowledge approach. A hash function has very low running time. So this so this scheme is very light-weight. The VASM protocol uses coordinate value of point in main address sheet for generating addresses. The implemented solution had four components allocator, initiator, requester and normal. It works towards achieving the IP configuration in highly vulnerable and heterogeneous environment. The approach uses the combination of the hash and SHA-I approach.

The paper [7] provides a test bed implementation for mobile computing based communications. It work without any specific infrastructural requirements and serve the goal of high security. The paper addresses the issues of the MANET with lack of central administrations. For implementing the desired test bed the WMN test bed is used here for enabling the secure routing. As the primary aim of the security control is to serve the authentication, confidentiality and integrity, thus the work mainly emphasizes on the confidentiality construct. The work focuses on serving the goals for the OLSR protocol using secure hash algorithms (SHA-1) and AES respectively. At the evaluation point of the view the approach seems to provide the reduced computation time with lower complexities of the system. It also gives a light weighted solution.

The paper [8] covers some of the security objectives for the OLSR and STAR routing protocols for pretending the data dropping and malicious node detections. The paper deals with the IPSec mechanism for the MANET. The performance is decrease if malicious node is not present in the network, because overhead of IPSec protocol is present in proposed approach. In this paper we have proposed one approach to minimize the packet dropping by malicious nodes in the network by applying IPSec in OLSR and STAR routing protocols and compared the results with existing without IPSec protocols. While comparing the results of the approaches the STAR and the OLSR seems to provide effective results for the MANET.

There are some other approaches suggested with the literature which works on improvising the traditional security control of MANET using IPSec. One of such approach is IPSec-LANMAR given with [9]. It works with the propagation model using two basic characteristics path loss and shadowing is presented. The IPSec-LANMAR gives a strong impact on the performance of a protocol because the propagation model determines the number of nodes within one collision domain, an important input for contention and interference. This, in turn, has a straight effect on a node's ability to transmit a packet to another node and it offer security services for both routing information and data message at network layer. The simulation result shows that free space propagation model with IPSec-LANMAR routing protocol outperforms compared to two ray propagation model and Shadowing model in emergency area environment and the experiments are carried out using the simulator.

The paper [10] suggested a solution as an extension to AODV called Secure AODV (SAODV). Mainly the security in MANET is served here using IPSec which was discussed earlier. The work assures that the IPSec implementation can use as a selector the TCP and UDP port numbers. Network communication contains two types of packets data and control. Thus the security mechanism must allow the control packet directly without change and the data packet is verified using cryptographic primitives. The SADOV uses: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. The information relative to the hash chains and the signatures is transmitted with the AODV message as an extension message that will be refereed as Signature Extension.

Carrying forward the above work for providing the security to MANET the paper [11] gives a protocol named as SNAuth-SPMAODV (Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with IPSec. It provides a robust way of defense against Denial of Service (DoS) attacks. It protects both routing information and data message at network layer in MANET. Also the protocol works towards multipath discovery between the sender and receiver without any additional packets for authentication. It combines the IPSec and SNAuth. It implements the basic functionality of IPSec for MANTE such as ESP and AH. While evaluating the approach it gives higher results in term of processing efficiency, routing load and simulation time. The experiments are carried out using the simulator Qualnet version 4.5. This suggests that IPSec would be a better choice for MANET due to the reason that it can provide security protection for both routing information and data message simultaneously.

The paper [12] works towards improving the above authentication for MANET specifically for multicast packets security. Most of the times multicast allows transmission of a single packet to many users, possesses a potential danger of malicious activities which consumes the resources and affects the normal working. Suggested AuthMAN is a scalable and lightweight mechanism to address the problems of authentication in multicast mobile ad hoc networks. AuthMAN uses symmetric cryptography, and time-delayed key disclosure to achieve authenticated broadcast. AuthMAN uses time as an asymmetry property and it requires sender and receiver need to be time-synchronized. The evaluation results show the effectiveness and efficiency of the proposed solution.

The paper [13] presents a IP based auto configuration mechanism for MANET. It focuses on developing a security solution with dynamically changing topologies and lack of infrastructures. Thus, security is also a main issue in address allocation. To develop a framework for Auto and secure Assignment of IP address to new node entered in mobile ad-hoc network using Public key cryptography. Expected output of the framework offer security in address auto configuration in the absence of any static configuration or central sever. This approach uses public key cryptography "Rabin algorithm" to provide security in auto configuration.

IV. PROBLEM STATEMENT

MANET is an ad-hoc network with dynamic changes in topologies which involves continuous movement of nodes within the specific range. The controls made for MANET is made in such a way which consumes less resources and can be easily compatible with mobile devices. Thus some of the controls are missing like security primitives such as confidentiality and authentication. Lack of such control enables the malicious nodes to perfume destructing activities inside the networks causes data loss and performance degradations. A malicious node can silently drop some or all of the data packets sent to it for further forwarding even when no congestion occurs. If malicious packet dropping attack is used along with other attacking techniques, such as shorter distance fraud, it can create more powerful attacks called Black hole attack, which may completed disrupt network communication. Moreover A malicious node will drop all the data packets that it receives. In addition, it will not acknowledge to the sender that it has dropped a data packet.

This work will investigate how effectively the security controls can be embedded into the MANETS light weight protocol AODV. Traditionally the AODV is not present with any of the security control. Also the security mechanism provided by the digital signature and the RSA is applied to the network with supporting infrastructure presents. Applying them to MANET is again a challenging task. The specific problem to be addressed is how to use secure neighbor authentication of nodes in a multipath routing algorithm in MANET protected from Denial of service attack and provide network layer security. Also to apply security as the requirement of user and is based on the type of information available with the packets.

Thus the outlined objectives of the work are given as:

(i) To develop a robust security control for AODV in MANET
(ii) To provide higher order of security in fewer resource consumptions
(iii) To Reduces the delays involves with communication for the security mechanism
(iv) To provide each nodes authentication for multicast and unicast approaches

Thus, by considering the above objectives in mind and the problem associated with the all related approaches, the work had suggested a new hybrid approach to serve the purposes. Its details are covered in next section.

V. PROPOSED SOLUTION

The proposed work will give a novel approach which enables the trusted communication in a secure manner over the non trusted nodes zones of ad-hoc networks. In MANET the nodes and their topologies are dynamically changing, thus to verify their authenticity and malicious behaviour is not possible most of the time. But there is away by which the communication and transmission process can be made more secure than it was previously developed. This work will give a robust solution embedded with AODV which makes a guaranteed secure communication using digital signature (SHA-I) and RSA cryptosystem. It serves the complete requirements of the MANET as it was lightweight, consumes fewer resources and is effective. The process starts with the initiations of route discovery. The suggested scheme give a generic way of communication is a secure manner with lower range radio signals. The nodes participating in such a communication is not aware about the intermediate operations of the encryption and cryptosystem.

The work had also make the security schemes clear and starts evaluating them in a default mode. The approach is able to perform both authentication using digital signature and serve confidentiality using RSA cryptosystem.

The source S sends the RREQ message to its neighbour with a destination id. The neighbour node checks weather the id belongs to its own, or its subgroup or someone else known by him. If all the matching are not found then it is further forwarded to next intermediate nodes. Once the destination is found in this way then the destination node separates the type of data packets and control packets available with the request.

It is segregate into two categories: Mutable information and non mutable information.

The non mutable information something related with the source and its data and the mutable information is that which could be read out by the intermediate nodes and destination such as hop counts. This non mutable information is digitally signed with the destinations signature and embedded with the non mutable information in a RREP packet. Now, each intermediate node receiving this RREP packet will verifies the destinations signature from its neighbour table. If the signature is matched then only the packet is transmitted to next node from where it reaches to source S. If the signature is not matched at the intermediate node then it was dropped by them. Finally the reply reaches the source where it first matches the signature of its neighbour then the later ones are matched and if the first ID is not matched then it was dropped by source itself.

Now, the source knows the complete path and signed information for each intermediate nodes. The source selects the key for its respective intermediate nodes for transmitting the data to destination D. The key is gathered either from its neighbour table or calculated from its signature. The sender source encrypts the data containing in the packet by RSA cryptosystem which perform encryption using the public key of source S. The destination receives this and decrypts the data using its private key. Once the data decryption is successfully performed by the receiver or destination after verifying the data and all its information's integrity the success acknowledge message is revert back to the sender source S. Source verifies and confirms the data transmission only after getting this success ack message. If this message is not received then the next time repeat transmission will be performed from the different routes. Thus the work applies an enhancement to AODV that allows using shorter routes, which will result in lower end-to-end delays, and longer battery life better than existence works.

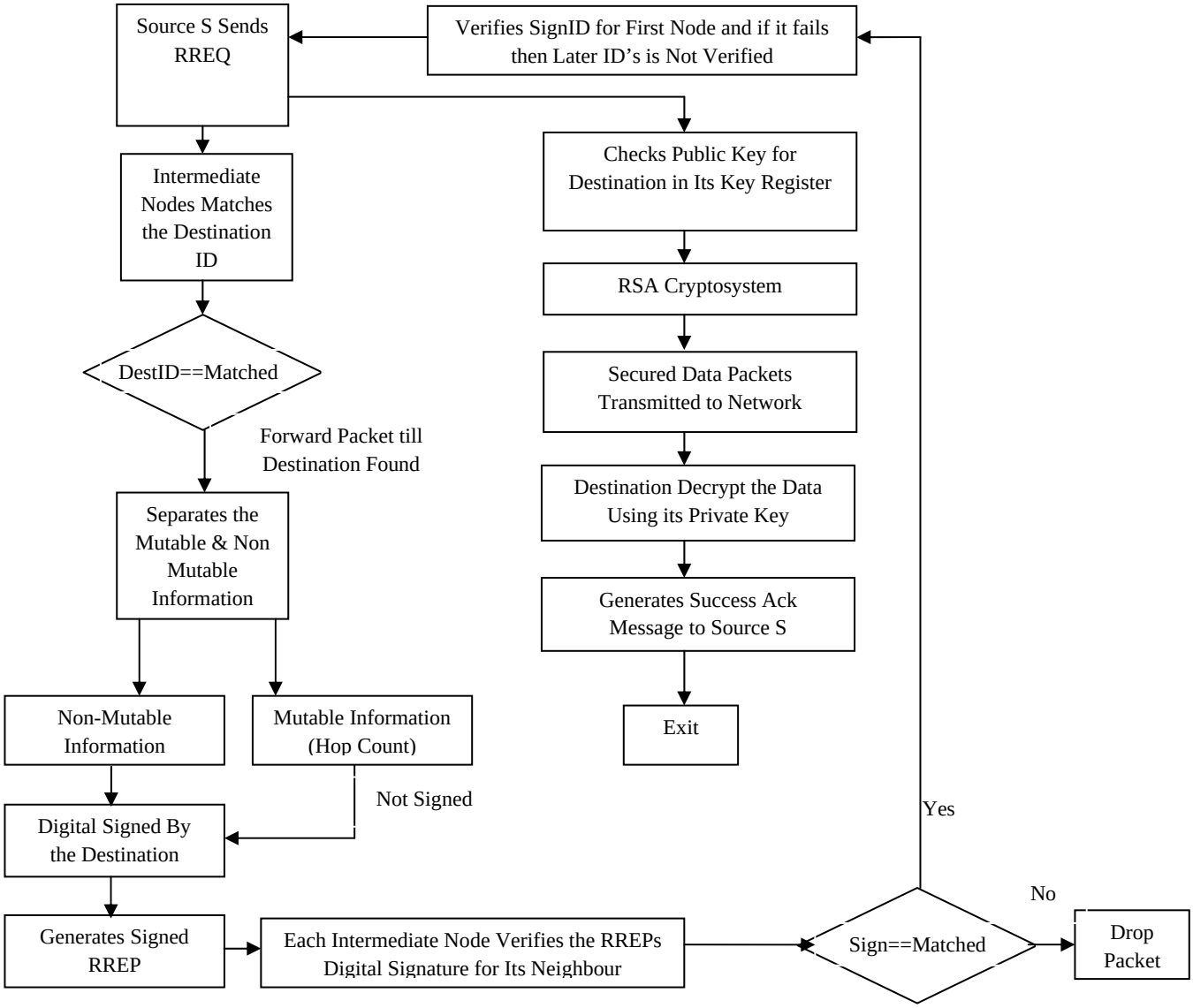

FIGURE 1: HYBRID SECURITY USING SHA- DIGITAL SIGNATURE AND RSA CRYPTOSYSTEM FOR ADOV IN MANET

Expected Benefits

(i) It provides security against modification, fabrication, replay, and impersonation attacks on MANET.
(ii) It gives low security overhead which considerably extends the network lifetime
(iii) It reduces the route setup delay and communication overheads.
(iv) It is cooperative for accomplishing high-level security with the aid of mutual collaboration/cooperation amidst nodes along with other protocols.
(v) Public Key Cryptosystem will assure tight security in an light weight version of protocol.
(vi) Can be used for Multicasting or Unicasting scenarios
(vii) It is flexible enough to trade security for energy consumption.
(viii) It is compatible with the security methodologies and services in existence.
(ix) It is scalable to the rapidly growing network size.

Performance Metrics

As per the requirements of the suggested work there are some performance metrics selected to compare the proposed Hybrid security based AODV protocol with the existing one. The following metrics were considered for the comparison were

- **Packet Delivery Ratio**: it is the ratio of the number of packets received and the number of packets sent.
- **Throughput:** This gives the fraction of the channel capacity used for data transmission.
- **Average Latency:** Gives the mean time (in seconds) taken by the packets to reach their respective destinations

VI. CONCLUSION

This paper proposes a novel hybrid mechanism for improving the security of MANET. Mainly the security here deals with the authentication and confidentiality of the data packets. The packets information here is encoded after separating them into categories or mutable information

contains in them. Authentication is performed using digital signature algorithm SHA-I. Normally the approach verifies the non mutable information with the unique signature associated with the packet. Encryption is performed with the RSA based public key cryptosystem. Thus the approach authenticates a sender and all the intermediate nodes in a multicast environment of mobile ad hoc network with a low computation overhead. The protocol assumes each node has pre-distributed secret key. In near future of implementation, extensive evaluation and experimental study will prove the results effectiveness of the suggested approach.

REFERENCES

[1] Sanket Nesargi and Ravi Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", IEEE Transaction, ISSN:0-7803-7476-2/02, 2002

[2] Majid Taghiloo, Jamshid Taghiloo and Mehdi Dehghan, "A Survey of Secure Address Auto-Configuration in MANET",IEEE Transaction, ISSN: 1-4244-0411-8/06, 2006

[3] El Hajjar, A.Lasebae and D.K.Saini, "Secure routing protocol for Mobile Ad Hoc Network using IPsec", Middlesex University, London, United Kingdom

[4] Jared Cordasco and Susanne Wetzel, "Cryptographic vs. Trust-based Methods for MANET Routing Security", Department of Computer Science Stevens Institute of Technology, Hoboken, STM, 2007

[5] Manel Guerrero Zapata, "Middlesex University, London, United Kingdom", in Mobile Computing and Communications Review, Volume 6, Number 3.

[6] Majid Tajamolian, Majid Taghiloo and Mahnaz Tajamolian, "Lightweight Secure IP Address Auto-Configuration Based On VASM", International Conference on Advanced Information Networking and Applications Workshops, IEEE Computer Society, ISSN: 978-0-7695-3639-2/09, 2009

[7] Emmanouil A. Panaousis, George Drew, Grant P. Millar, Tipu A. Ramrekha and Christos Politis, "A Test Bed Implementation for Securing OLSR in Mobile Ad-Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, 2010

[8] Harish Shakywar, Sanjeev Sharma and Santoh Sahu , "Securing OLSR and STAR Routing Protocols ", International Journal of Computer Applications, ISSN:(0975 – 8887, Volume 35, No.3, December 2011

[9] 1D.Devi Aruna and Dr.P.Subashini, "Analysis of Different Propagation Model for IPSec-LANMAR Routing Protocol to Secure Network Layer for MANET in Emergency Area Environment", IJCST, ISSN: 0976-8491(Online), Vol. 2, Iss ue 4, Oct . - Dec. 2011

[10] Anil Suryavanshi and Dr. Poonam Sinha, "Efficient Techniques for SAODV in Mobile Ad-Hoc Network", Journal of Global Research in Computer Science, Volume 2, No. 8, August 2011

[11] D.Devi Aruna and Dr.P.Subashini, "SNAuth-SPMAODV with IPSec to secure network layer for Mobile adhoc networks in Military Scenario", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 5, July - 2012

[12] Prasad Chaudhari and Ms. Deepali Gothawal, "AuthMAN: Authentication in Multicast Mobile AdHoc Networks using Time Asymmetry", International Journal of Computer Science and Information Technologies (IJCSIT), 5085-5088, Vol. 5 (4), 2014.

[13] Jagrati Nagdiya and Shweta Yadav, "Secure Autoconfiguration in Mobile Ad hoc Networks using Rabin cryptosystem", IJETAE, ISSN 2250-2459, Volume 4, Issue 4, April 2014