A Novel Approach to Increase Security in AODV Using RSA Asymmetric Cryptography and Hash Function

Utkarsh Mendevell[#1]

Student, Wireless Communication and Networks, Gautam Buddha University (GBU)
Greater Noida, Gautam Buddha Nagar, Uttar Pradesh, India
utkarshmendevell@gmail.com

***Abstract* – A Mobile Ad-Hoc Network (MANET) is one of the practical applications oriented emerging research area. They are infrastructure less network i.e. a network that works without an access point and is used for communication between two or more number of nodes in a wireless network. Attacks are classified in two categories:Routing attacks, and Data Forwarding attacks. Data forwarding attack is basically comprised of modification or dropping of data packets which does not affect routing protocol. In this paper, I propose a secure version of ad hoc on-demand distance vector routing protocol (AODV). The proposed protocol in the paper provides security for routing packets and is able to prevent attacks for example, black hole attacks, routing information modification and impersonation efficiently. The projected method uses hash messages, authentication/ security code function, that provides quicker message verification and sender in addition to intermediate nodes authentication. Results have demonstratedthat the proposed method has minimized the Delay and NRL, increased the throughput PDR involved in computation and verification of fields during route discovery process and has performed better than the AODV protocol in the presence of malicious nodes during a black hole attack.**

Keyword – Mobile ad hoc network, Routing Protocol attacks, AODV, Black hole, Impersonation, Hash Function, Authentication, RSA Cryptography,

I. INTRODUCTION

AODV is a self-starting, loop free routing protocol that establishes routes from sender to receiver on demand made by source node. It uses unique sequence numbers to tell how old routes were created to sort old routes from new ones and refresh old routes when they get obsolete. AODV protocol is based on assumption that all the nodes present in the network are uncompromised and cooperative in nature, making it one of the most affected networks in the case of an external/internal attack such as presence of a malicious node or as such in a scenario of black hole attack. A Black-Hole attack can be described as a denial of service attack wherein a malicious node seeks to be selected as potential next hop forwarder to attract as many data packets as possible.Then instead of forwarding it as it just discards all these received data packets and notify others falsely that the packet has been transmitted countering the problem of retransmission by others.

RSA algorithm which is inspired from the surnames of Ron Rivest (an MIT professor), Adi Shamir (a cryptographer), and Leonard Adleman (a computer scientist) –theydescribed it first in 1977. It is currently being used in a variety of platforms to provide a means of secure communication among different products and industries around the whole world. RSA is a vital part of all the key protocols used for secure network communication and is incorporated into them. It provides security form unauthorized user access. RSA is one of the most high-quality algorithms that are employed in majority of the encryptions and cryptography conception, which is being used in transmission of information in network systems.

Hash function attaches an additional layer of security through its hashing algorithm that helps to verify data integrity checking of data packet.Fewof the key points and aspects covered in this paper are:

- First, working of AODV Protocol is studied in presence of malicious and compromised nodes in the network.
- Second,Effect of a customized black hole attack is studied on AODV protocol when malicious nodes try to attract as many packets and then drop these packets to decrease network performance
- Third a customized version of AODV protocol is introduced which uses RSA for encryption and a hash function for data integrity check of data packets

II. Related Works

My work is mainly focused on introducing a customized black hole attack scenario to study effect of malicious and compromised node on AODV protocol therefore some of the main protocols studied for consideration are mentioned in this section

A. Ad-Hoc On-Demand Distance Vector Routing (AODV) Protocol

AODV[1] is a routing protocol designed for MANET's and wireless networks. It establishes routes from sender to destination on demand. Such routes are built only when requested by source nodes. Therefore, AODV is considered as an on-demand algorithm, which creates no extra traffic for communication to take place among nodes. The routes built are created only as long as requested by source nodes. Source nodes also forms trees to connect to multicast group nodes. AODV uses unique sequence numbers to ensure proper route freshness, recycle obsolete routes. They are self-starting, and loop free even though scaling to huge number of mobile nodes. In AODV, network is silent until all the connections are formed. Network node that needs to connect broadcasts a request for connection. The remaining nodes forwards this message keeping record of the node which has made request for connection creating a series of temporary routes tracing back to the requesting node. A node holding the route to the desired node when receives such message, transmits a backward message through the temporary routes formed to the route requesting node. The node which made the request uses the route with minimum number of hops through other nodes to communicate to destination. The entries that are not used recently in the routing table are recycled and refreshed after some time. If a link fails, the routing error message is dispatched back to the transmitting node and whole process is repeated. Sequence numbers are maintained properly to keep AODV loop free. A routing table is maintained for all routes even the short ones. Protocol was developed to with an assumption that all nodes in network trust each other and are cooperative such as in OR protocols.

B. Known Security Issues in Routing.

The routing attacks in Ad Hoc Wireless networks can be classified as – Active and Passive attacks[2]. In an active attack, the attacker is able to inject some false packets in the network compromising integrity of network. Whereas in passive attack, the attacker is only able to eavesdrop in the network to hear all or some part of the communication but unable to disturb operation of routing protocol. An active attack is harmful to AODV. Some of the examples of active attack are black hole attack, malicious node attack and denial of service attack.

A Wireless network needs to be Reliable, Robust and Secure at all times. Presence of malicious nodes and compromised nodes degrade network performance may bring entire network down. Cryptographic methods are considered as best solution in defence against the problem of malicious and compromised nodes as they guarantee safety and integrity of messages transferred between nodes. However, there are some special cases or attacks like a compromised node injecting false data in network compromising integrity of network.

Impersonation, Black Hole, Grey-Hole and Worm-Hole are some of the most harmful routing attacks done in a wireless network[3]. In Impersonation, a malicious node try to represent falsely as another node of the network to acquire information not meant for its real identity but can be attained by representing someone else's identity (Impersonating)[4]. In Black Hole attack the malicious node try to push false routing information in the network so that it gets selected by other nodes as potential next hop forwarders. In this way, it gets maximum number of data packets possible to pass through it but instead of forwarding these packets it discards them and sends false message in the network that packet was delivered to counter retransmission by other nodes. Hence, data packet gets lost completely and network performance is decreased. It is a type of denial by service attack. A Grey-Hole attack is a special case of Black-Hole attack in which malicious node drops fewof the intercepted packets whereas forwards others at random, i.e. it chooses to act maliciously at some time whereas acts like any other normal node other time.Therefore, it is very difficult to distinguish a grey-hole attack from a black-hole one.In a Worm-Hole attack two malicious nodes located geographically at two different regions of the network collide with each other[5]. When one of the malicious nodes receives a data packet it forwards it to other malicious node through a secret tunnel between the two instead of simply forwarding it to other potential next hop forwarders. The other node which receives the packet through first malicious node replays the packet in that region thereby compromising integrity of the network.

C. RSA algorithm

RSA algorithm can be used to provide security in AODV routing protocol as explained in[6]. RSA is one of the most commonexamples of asymmetric cryptographic algorithm. In RSA algorithm, one can easily find and multiply large to very large prime numbers together,howeverit is very difficult to factor their product. These prime numbers are used in Private and Public keys, which increases the complexity of the algorithm. The security being provided is evident in the following frame formats.

Encryption and Decryption using RSA Algorithm:

- Choose two large prime numbers R and S.
- Calculate N such that N=R*S.
- Select the public key Q such that Q is not a factor of (R-1) and (S-1).
- Select the private key P such that it follows equation (P*Q) mod (R-1) and (S-1) = 1
- For encryption calculate the cipher text CT from plain text PT such that CT = PTQ mod N
- Send CT as the cipher text to the receiver.
- For Decryption calculate the plain text PT from the cipher text CT such that PT = CTP

Thus, I can conclude that RSA algorithm can be used to provide security in AODV protocol. RSA uses both Public as well as Private Key.

D. *Hash Function*

A Hash Function gives output as hashed value when a string of plain text is provided as input. Hash value is attached to packet header for integrity checking. At the other end of communication process, after the decryption process has taken place the decrypted text will be hashed again to obtain new-hashed value. This new-hashed value thus obtained will be compared to the value attached within packet header. If bot the values are found to be equal, the data integrity is verified and decrypted text is accepted otherwise the packet is discarded. If the packet is discarded, an acknowledgement packet will be sent back to sender informing him about the status of the packet.

III. ALGORITHM

The proposed protocol is based on shared secret key technology. A mechanism is assumed to set up pair wise secret keys. Total number of n. (n-1)/2 pair wise secret keys will be maintained in the network. Source and Destination nodes both are not compromised. AODV assumes bidirectional links which means if a node A is able to receive packet transmitted directly by some node B then node B is also capable of receiving packet directly transmitted by node A. The notation used to describe cryptography operations is as follows. A and E are source and destination nodes respectively. KS denotes the secret key shared between nodes E and S. Each node holds the MAC (hash function based message authentication) algorithm. Hash function denotes the computation of the message authentication code of message M using secret key KS between nodes A and E[7][8].

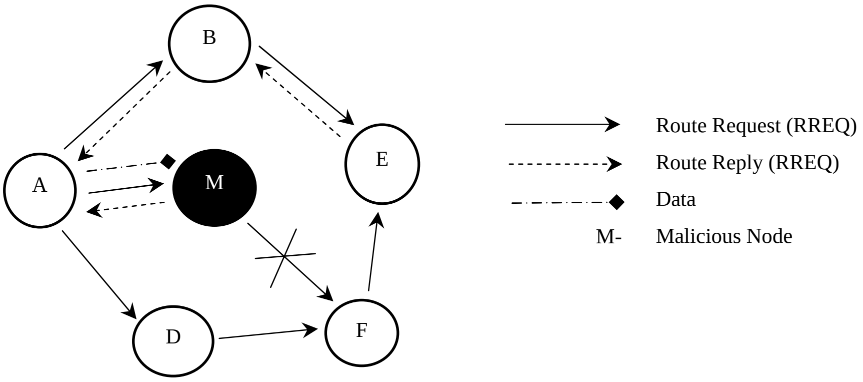


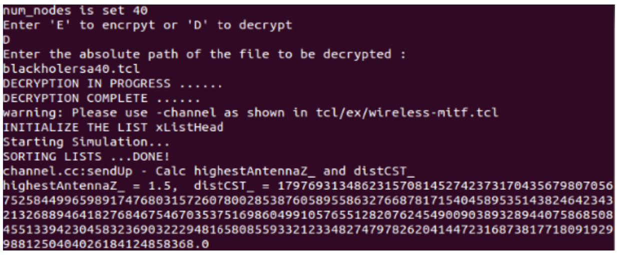
Fig. 1. Attacks of malicious node

A new methodology for generation of id key for the authentication of node has been proposed. This method is based on cycle chain mechanism. In this mechanism, any previous record of data is automatically destroyed. In other words, the process of key generation is maintained independent of next value. The naming convention used for my algorithm is as follows

- {M1, N1, M2} set of notations represent the value of source point, intermediate node and sink node.
- nk = Session key.
- (ki)s = Secrete key.
- Ne = Session in one Node to another Node.
- Cid = Communication and its identity
- WT = Represent value of communication, it equals H {W1, W2, W3}
- Token = a generated token
- (Y) =message

- H(Y) = hashed message

Key Generation Technique used here discuss the dynamic key generation, which is a novel approach and one of the main contributions proposed. The type of information shared between the two nodes is confidential. This method requires two set of keys to be generated at both sender's and receiver's side which are secondary key (Ki)s and session key (SK)s. (Ki)s is required to generate V values which is used to enhance security to generate session keys. The node M1 will issue the intermediate node (N1) and a communication authentication once authenticated.



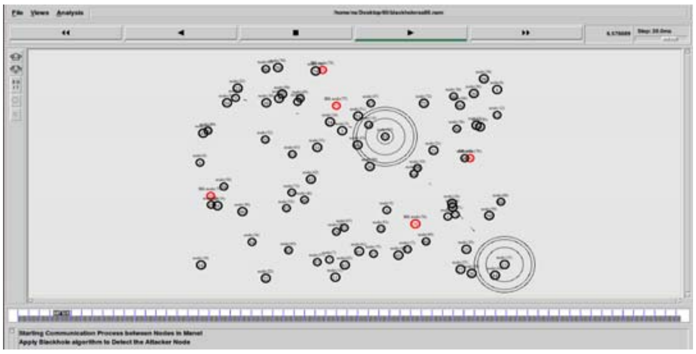
```
num_nodes is set 40
Enter 'E' to encrpyt or 'D' to decrypt
D
Enter the absolute path of the file to be decrypted :
blackholersa40.tcl
DECRYPTION IN PROGRESS ......
DECRYPTION COMPLETE ......
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 17976931348623157081452742373170435679807056
75258449965989174768031572607800285387605895586327668781715404589535143824642343
21326889464182768467546703537516986049910576551282076245490090389328944075868508
45513394230458323690322294816580855933212334827479782620414472316873817718091929
9881250404026184124858368.0
```

Fig. 2. Terminal Output generated numbers of RSA

Fig. 3 after decrypting data

Fig. 4 after encrypting data

IV. SIMULATION



Starting Communication Process between Nodes in Manet
Apply Blackhole algorithm to Detect the Attacker Node

○ Normal Working Node

○ Malicious Node

Fig. 5 NAM simulation window in NS 2.35

TABLE I. Simulation Parameters

Simulation Tool	NS-2.35
Operating System	Ubuntu 12.04
No. of Nodes	20,40,60,80,100
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	50 packets
Data payload	512 bytes
Pause time	10 seconds
Channel bandwidth (data)	11Mbps
Transmission range	250m
Examined protocol	AODV,Hybridized AODV with RSA algorithm using Hash Function
Interface QueueType	Queue/Drop Tail/PriQueue
Mobility model	Random way point
Simulation area	1100M*1100M
Link Layer Type	LL

V. RESULTS

TABLE I. AODV Protocol

AODV	**Throughput (kbps)**	**PDR (%)**	**Delay (sec)**	**Energy Consumption (Joule)**	**Dropped Data**
20 Nodes	123.90	96.26	400.36	74.6	234
40 Nodes	263.86	96.77	355.86	74.6	362
60 Nodes	342.91	97.15	322.91	134.6	367
80 Nodes	456.89	97.45	297.43	184.7	433
100 Nodes	478.90	97.70	277.73	194.3	498

TABLE II. Hybridized AODV with RSA algorithm and Hash function

Proposed Algorithm	**Throughput (kbps)**	**PDR (%)**	**Delay (sec)**	**Energy Consumption (Joule)**	**Dropped Data**
20 Nodes	946.21	99.90	141.6	10.9	193
40 Nodes	1011.28	98.71	212.82	61.86	276
60 Nodes	1740.67	98.90	244.73	111.6	386
80 Nodes	473.11	99.03	288.32	176.6	393
100 Nodes	498.18	98.43	276.18	183.6	401

A. *Average Throughput*

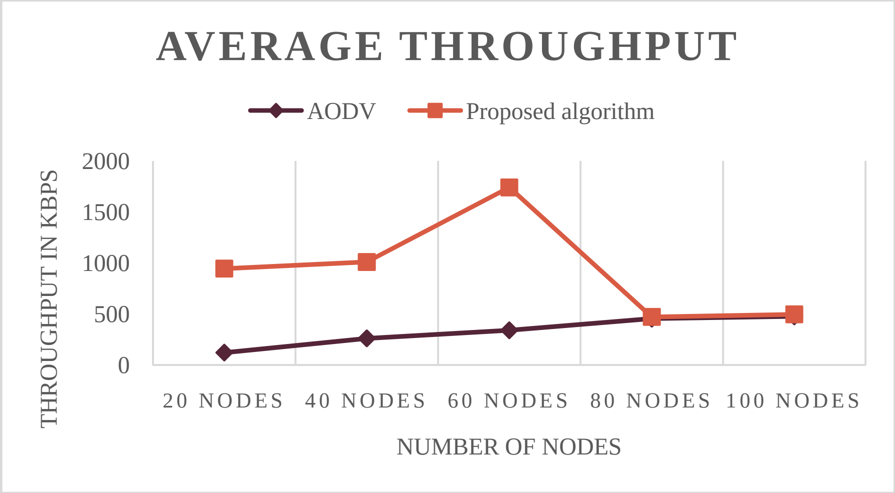


Fig. 6. Comparison of Throughput

B. *Packet Delivery Ratio (PDR)*

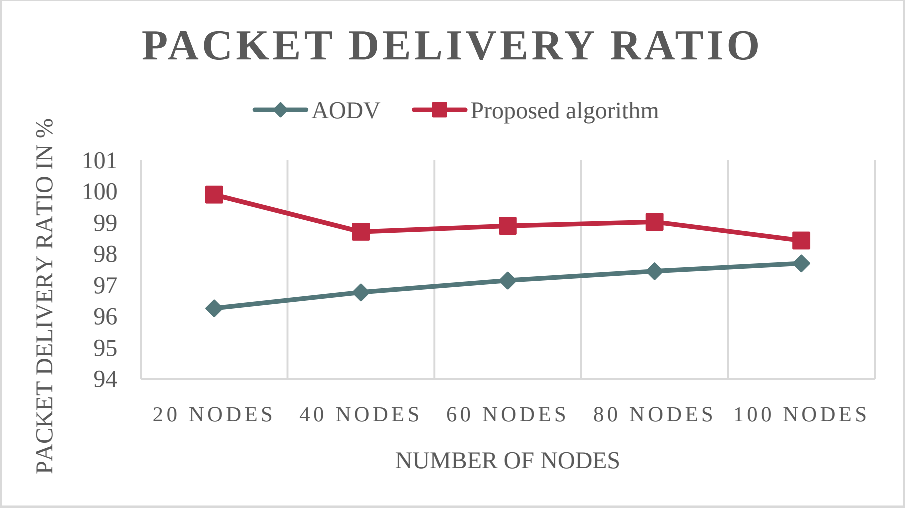


Fig. 7. Comparison of Packet Deliver Ratio (PDR)

C. *Average End-to-End Delay*

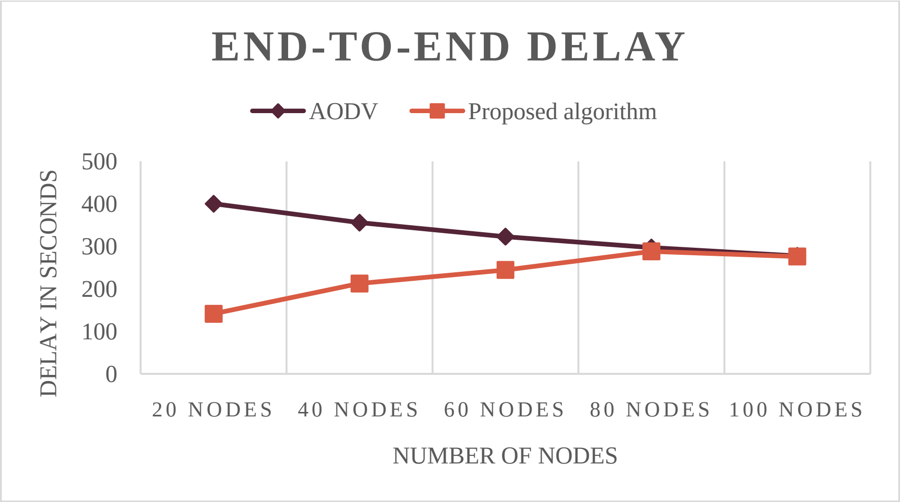


Fig. 8. Comparison of average end-to-end delay

D. *Energy Consumption*

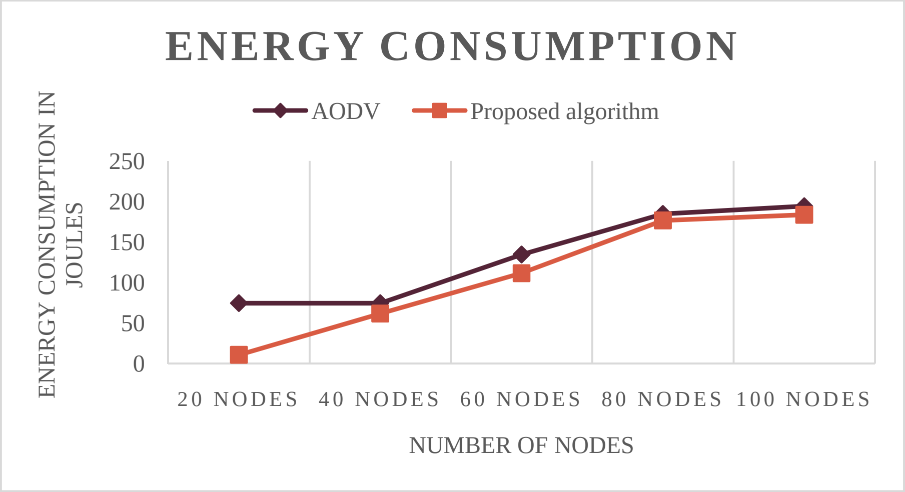


Fig. 9. Comparison of Energy Consumption

E. *Total Packet Dropped*

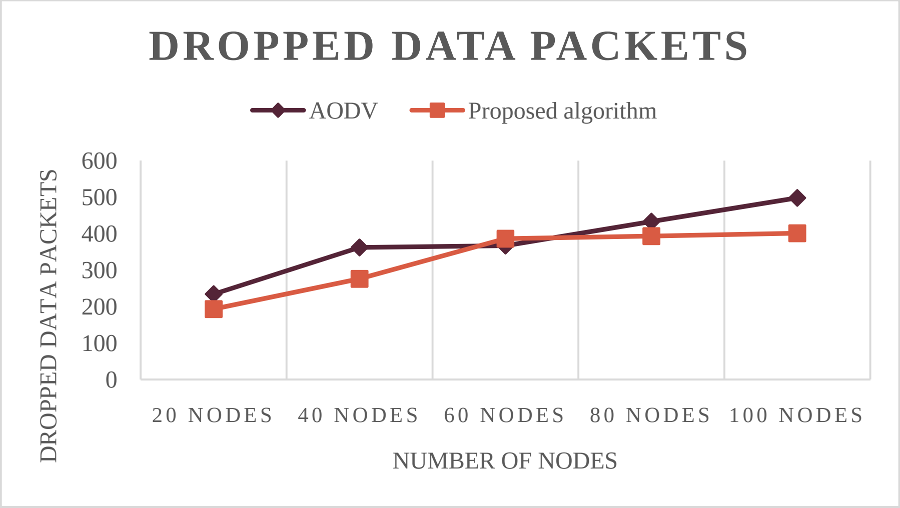


Fig. 10. Comparison of dropped data packets

VI. Conclusion

In this paper, I have suggested aninnovative security mechanism to the AODV protocol by using asymmetric cryptography i.e. RSA to provide reliable and efficient data transfer from source to destination. Here I have enhanced security to AODV by using RSA algorithm. The AODV routing protocol comes in picture at the time of sending data packets. To prevent the loss of data,I have implemented RSA algorithm to increase the security. The encryption/decryption of message and reception of keys (sent and received) is used to enhance security in AODV protocol. The AODV protocol uses the RSA algorithm to encrypt the message to be sent and decrypt the message received at the destination. Thus, we can make data secure with the use of RSA algorithm. Hence RSA can be used to achieve safe data transmission in AODV.

Acknowledgment

This research is partially supported by GBU for my M.Tech Dissertation. I want to thank Dr. Vidushi Sharma, my guide for giving me enough time to learn these technologies and conduct this research. I am thankful for her support during my entire research duration. Her knowledge, and talenthas greatly assisted this work.

I thank Miss Jyoti Gangwar for being extremely helpful in making me understand concepts and working of NS2 software. Without her help this research work was not possible.

I want to take this opportunity toalso thank Dr. Anil Kumar Gautam, Professor and Dean, School of ICT,GBU for motivating me to conduct my research and helping me publish a research paper.

References

[1] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing,” Proc. - WMCSA’99 2nd IEEE Work. Mob. Comput. Syst. Appl., pp. 90–100, 1999.

[2] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, Security in wireless sensor networks, in: Handbook of Information and Communication Security, Springer, 2010, pp. 513–552..

[3] A. Echchaachoui, A. Choukri, A. Habbani, and M. Elkoutbi, “Asymmetric and dynamic encryption for routing security in MANETs,” Int. Conf. Multimed. Comput. Syst. -Proceedings, vol. 0, no. 1, p. 7, 2014.

[4] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” Human-centric Comput. Inf. Sci., vol. 1, no. 1, pp. 1–16, 2011.

[5] S. Ji, T. Chen, and S. Zhong, “Wormhole attack detection algorithms in wireless network coding systems,” IEEE Trans. Mob. Comput., vol. 14, no. 3, pp. 660–674, 2015.

[6] Miss .Rashmi P. Shinde*, Mr. Sanjay S. Pawar. Security Provided to Mobile Ad-Hoc Network using RSA – Asymmetric Key Cryptography. International Journal of Engineering Sciences & Research Technology February, 2015] ISSN: 2277-9655.

[7] K. K. Waraich and B. Singh, “Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks,” vol. 82, pp. 63–70, 2015.

[8] Preeti Sachan and Pabitra Mohan Khilar, “Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism,” Int. J. Netw. Secur. Its Appl., vol. 3, no. 5, pp. 229–241, 2011.

AUTHOR PROFILE

Utkarsh Mendevell obtained his B.Tech degree in Information Technology from UPTU in 2014. He is currently, aM.Tech student at GBU, G. B. Nagar, India and studies Wireless Communication and Networks under the guidance of Assistant Professor Dr. Vidushi Sharma. His main area of research interest consists of Ad-Hoc Wireless Networks, AODV protocol and security in wireless networks.