Detection and Prevention of Packet Dropping using Secured Encryption AODV (SEAODV) with the performance comparison of SAODV,SDSR,SDSDV in MANET using Network Simulator

Abubucker Samsudeen Shaffi* & Capt. Dr. S. Santhosh Baboo**
*Research Scholar,, P.G and Research Department of Computer Science, D. G. Vaishnav College, Arumbakkam, Chennai, Tamil Nadu – 600106, India.
**Associate Professor, P.G and Research Department of Computer Science, D. G. Vaishnav College, Arumbakkam, Chennai, Tamil Nadu – 600106, India.

Received: June 09, 2018 Accepted: July 27, 2018

ABSTRACT *Mobility and portable nature of Mobile Ad Hoc Networks (MANET) has redoubled its quality by two fold.MANETs became a common network used for numerous applications. Quality and the transportable nature of MANETs may result in link failure throughout packet forwarded valuable packets could also be created by malicious nodes gifted within the network. In MANETs, Malicious packet dropping and link error are the two main causes of packet losses. A node will perform malicious and will hurt the packet causing method. Ad Hoc on demand distance vector (AODV) may be a good routing protocol, however it is defined to well-known packet drop attack. This paper proposes the routing protocol security by using a hybrid of security mechanism.Securing routing packets, detection and preventing of malicious nodes,which destroying the network is the major consideration of this security mechanism. These basic security mechanisms which the protocol uses the hash function, route discovery request, Certificates andtime synchronization.In this work an attempt has been made to check the performance comparisonthree routing protocols are Secured Encryption AODV(SEAODV),Secure Destination-Sequenced Distance-Vector routing protocol (SDSDV), Secure Ad hoc On-demand Distance Vector (SAODV) and Secure Dynamic Source Routing (SDSR) on the basis of various performance metrics such as Packet Delivery Fraction (PDF),Packet Delivery Ratio (PDR),Delay,Throughput,Packet Drop and Energy Consumption has been obtainableby using the NS-2 simulator. Based on the compared stimulated results concluded that SEAODV routing protocol is comparatively better in performance of all metrics than the SAODV, SDSDV and SDSR routing protocols.*

Keywords: *AODV, Secure,Packet Dropping, Malicious Node,Encryption, MANET, SEAODV, SAODV, SDSR, SDSDV.*

1. Introduction

MANETs are the wireless networks of computing, mobile devices without any support of a fixed infrastructure. MANET has mobile nodes which are self-organizing together within some arbitrary manner. A MANET is an independent collection of mobile consumers and by the use ofrelative bandwidth constrained in wireless links which will be communicated, while the nodes are mobility in nature, the network topology mightchange unpredictably and rapidlyover time. By using multi hop routing, nodes can able to communicate each other, when they are not within the radio range.The multi hop communication between the nodes where supported by MANETs,while performing such process is considered for the information which can't be created by misbehaved links or malicious nodes. It's still a complicated in security concern [1][2].

MANETs are built,maintained and operated by its components wireless nodes. These nodes basically have a definite transmission range and forwarding packets,each node pursues the support of its neighboring nodes [3]. The routing protocol of configured which is engaged in term to create the routes between nodes, that are farther than a single hop. Insteadof dynamic topology, the ability to trace the route is the unique feature of these protocols. Security in MANET is a twofold problem. One is securing the routing protocols which enable to communicate the nodes with oneanother and the second is the security of the data whichpass over the network on routes established by the routing protocols [4].

The combination of DSR andDSDV properties are available in AODV. To manage with on-demand route basis, AODV is aidedfor a route discovery process, whereas routing tables are provided for route information maintenance. It is a reactive protocol, so non communicated nodes route are not maintained in this routing protocol.In this protocol,Route Request (RREQ) messages are used for broadcasted to neighbor nodes and managing route discovery process.Until the node realize the fresh route or desired destination is reached, the message will floodthrough the network and to assurance the loop freedom sequence numbers were used[5][6].The allocated entries of the route table for reverse route were caused bypassed nodes in RREQ message. The Route Reply (RREP) form destination node will up-cast back to the source node. The

transmitting node from RREP message generatesentries of the routing table for forward route.Figure-1illustrate the RREQ and RREP message in the AODV routing protocol.

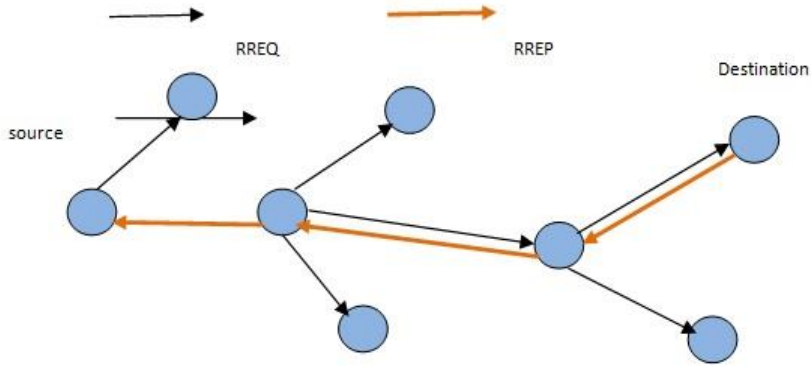

Figure.1 RREQ and RREP message in the AODV routing protocol

For route handling nodes send "GOOD MORNING" messages periodically to neighbor nodes. If a neighbor node failed to receive "GOOD MORNING" messages consecutively three times from a neighbor node, it concludes that message from the link to that specificnode is down.From the node detected broken link sends a Route Error (RERR) message to any upstream node. When a RERR message is received to the node, a new source discovery process will be indicated. Figure-2illustratesThe RERRmessage in the AODV routing protocol [7].

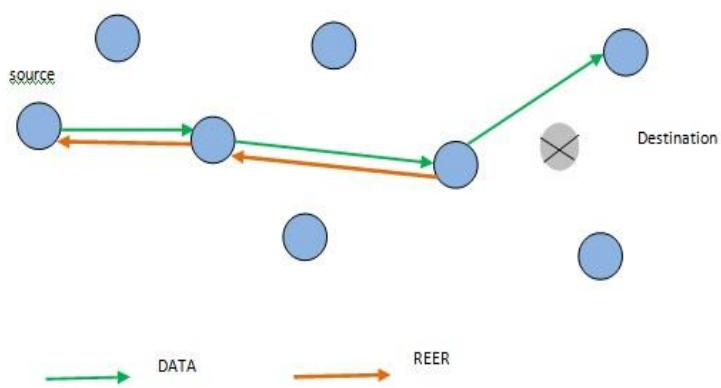

Figure.2 The RERR message in AODV routing protocol

In a packet drop attack, fake route information should be sent from malicious node, declared that it has an optimal route and through the malicious node the other good nodes were caused to route data packets. Thus make to choose the route from the source node which passes through the intruder. So the traffic will be routed by the intruder, therefore the traffic can be misused or discard.

Security Aware Ad Hoc (SAR) protocol conforms the node trust level and the route with security attributes to serve the incorporate the requested route with security metric. The vector used combination of available cryptographic techniques and security level is said to be Quality of Protection (QoP)[8]. By verifying transmitted packet with the digital signatures, attack like fabrication and modification can be stopped. During the path discovery each hop needs enormous encryption and decryption is the major demerit in using of SAR. To secure the routing protocol generally used mechanism iscryptographic mechanismswhich enforce the mutual trust relationships along with the wireless nodes [9].The proposed SEAODV routing protocol focuses are to secure the data transmission and also to construct a protected routing protocol.In this work an attempt has been made to check the performance comparison three routing protocols are Secured Encryption AODV(SEAODV),Secure Destination-Sequenced Distance-Vector routing protocol (SDSDV), Secure Ad hoc On-demand Distance Vector (SAODV) and Secure Dynamic Source Routing (SDSR) on the basis of various performance metrics such as Packet Delivery Fraction (PDF),Packet Delivery Ratio (PDR),Delay,Throughput,Packet Drop and Energy Consumption has been obtainable by using the NS-2 simulator. Based on the compared stimulated results concluded that SEAODV routing protocol is comparatively better in performance of all metrics than the SAODV, SDSDV and SDSR routing protocols.

2. Related works

There have been numerous kinds of attempts for securing the AODV routing protocols. In this subsection, some previous researches are mentioned and discussed. Some of the researchers have discussed about security issues and gave some results by analyzing the primary vulnerabilities in MANETs and discussed the criteria of security in the MANET. The major attack types against MANET were presented and for the attackable network the security solutions were provided [10, 11]. Others have desired to provide the routing protocol overview and the attacks against these protocols. Then, the antidotes to these attacks are suggested by researcher [12, 13]. In previous study many different methods have been initiated for the security of the AODV routing protocol. Most of the methods rely on cryptographic techniques. Some other researchers have presented an efficient, secured AODV routing protocol is said to be SAODV [14]. This protocol authenticated both mutable and non-mutable field information (hop count) of messages, by using of hash chain and digital signature, respectively their proposed routing algorithm proved that it has a better result in performance and security in terms of an end to end delay and the overhead. SAODV can secure data dropping attacks and tampering of control messages, but SAODV provide only the authenticity of the message and dependability of the route quality and route information will not be provided.

In some other articles the methods, including both cryptographic and trust base techniques together are presented. Liu has done research in this field [15], and in similar articles the comparison between protocols are given. Jared Cordasco and Susanne Wetzel have made a maximum quality of research for comparing Trust based Ad Hoc On Demand vector (TAODV) and Secure Ad Hoc On Demand vector (SAODV)which includes performance comparison on actual resource-limited hardware. This article addresses routing, security based on trust techniques and cryptography [16]. But his method is not efficient enough because it needs consecutive monitoringneighbors nodes also has a high cost to implement. Meka proposed trust-based solution (TAODV), which penalizing uncooperative nodes, isolating malicious nodes, and allowingto generate decisions for the destination best route by reviewing of both route trust and node trust metrics. In this paper, another trust based result will be obtained using a level of trust which can provide more suitable ideas along with implementation in comparison to presented previous works. Also in another paper, routing protocol with trust is suggested against problem with security and selfishness issues. It is said to be TAODV protocol, which is designed based on intrusion detection system andtrusted framework (secure protocol). In this model, trust information which gathered directly from monitoring nodes made to extend along routing table. Therefore the enormous decrease of routing procedure and overhead trustiness can be assured as the conclusion of this model [17]. Due to its few flaws points TAODV is still not an absolutely perfect protocol.By using TAODV routing protocol researcher has enhanced the performance of the MANETs [18]. The introduced method drastically and increases the network performance and also reduces the traffic on the network. Although this method is well performed, it could be more efficient and faster.

The SAODV protocol is an extension of the AODV protocol [19]. It provides the features of security such as integrity, non-repudiation and authentication are used to secure the mechanism route discovery of AODV. This protocol operates with AODV protocol by using the new extension messages. This certified public key allows intermediate nodes which it can authenticate to transit routing packet. The source of the routing control packet affixes its hash chain of the last element and RSA signature to the routing packets. These packets can traverse the network, intermediate nodes authenticate the hash value and signature cryptographically. The intermediate nodes develop the kth element of the hash chain, where k is the number of traversing hops in the packet. The intermediate or destination nodes having an active route are supplied to the needed destination.

3. Secured Encryption AODV (SEAODV)

In this security mechanism, Secured Encryption System (SES) algorithm is the primary Securing AODV routing packets, detection and preventing of malicious nodes, which destroys the network. This cryptography process is the basic idea for this SES algorithm.Secured Encryption system (SES) algorithms for cryptography,which use the same cryptographic keys for both encryption plaintext and decryption cipher text. This algorithm uses Symmetric-keys which are a class of the keys may be equal or there may be an easy conversion to do between the two keys. The keys represent a shared secret between two or more nodes, which can be used to support a private information link. The secret key can be accessed by both the nodes.In Secured EncryptionAd Hoc On Demand vector **(**SEAODV) is projected by adding further security measures to AODV protocol. In MANET the privacy for conserving truthful detection of packet drop attack is provided by SEAODV.The packet could also be born throughout forwarding of routing data or throughout knowledge forwarding. Droppings are often owing to presents of malicious nodes or owing to link error. The

SEAODV routing protocol will investigate the dropping in the route and may realize the malicious node or unsuccessful link behind this dropping.

The parameters are used for performance analyzes which are namely the packet delivery ratio, end to end delay and the normalized routing load. In this paper, we have analyzed some of the popular routing protocols namely SAODV, SDSR and SRAAA. The performances of the routing protocols have been investigated by using NS2 simulator. The simulation metrics used to analyze the performance of different routing protocols are SEAODV, SAODV, SDSDV and SDSR routing protocols.

4.Simulation Analysis and Performance of Routing Protocol

Simulation study shows that performance of routing protocol in terms of Throughput, Packet Delivery Ratio (PDR),Delay,Packet Delivery Fraction (PDF),Energy Consumption and Packet Drop strongly depends upon network conditions such as mobility and no. of nodes by using the NS-2 simulator.

4.1 Throughput

The below Figure.3 show the graph of SEAODV with SAODV, SDSR and SDSDV protocols. Number of nodes varied 30, 40, 50. It is calculated at destination node during entire SEAODV shows higher throughput than the SAODV, SDSR and SDSDV. The SEAODV has much more routing protocols than SDSR. SAODV is better routing protocols. SDSDV have lower throughput than other three protocols.

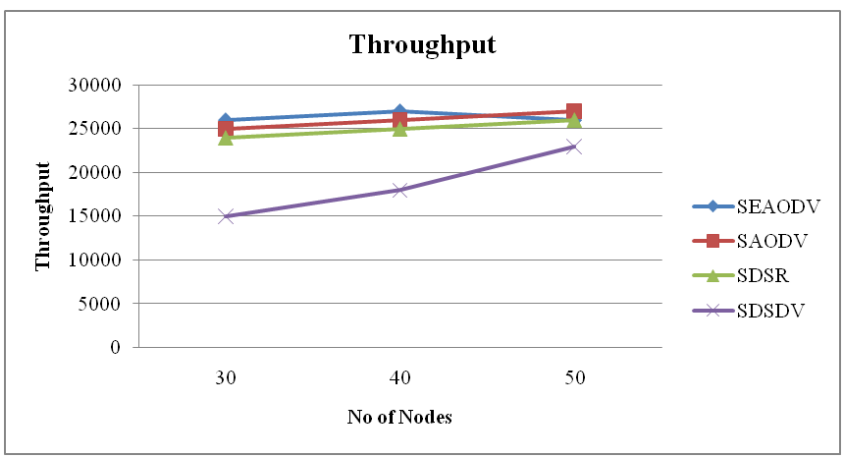

Figure.3 No of Nodes Vs Throughput

4.2 Packet Delivery Ratio(PDR)

The below Figure.4 show the graph of SEAODV with SAODV, SDSR and SDSDV protocols. SEAODV has slight higher packet delivery ratio than SDSR, SAODV and Table driven routing protocol(SDSDV) lower packet delivery ratio than reactive protocols(SAODV, SDSR).Among these three protocols SEAODV and SDSR is better packet delivery ratio than SAODV and SDSDV.

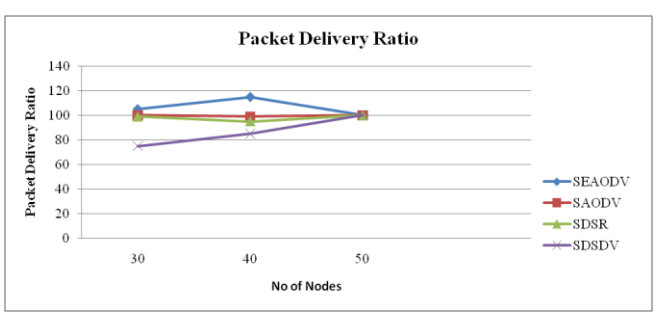

Figure.4 No of Nodes Vs Packet Delivery Ratio

4.3PacketDeliveryFraction(PDF) Overall performance of SEAODV is best. Figure 5 depicts that SEAODV has highest PDF as compared to SDSR and SDSDV. By analyzing the graph it is observed that PDF of SAODV is high for varying number of connections and nodes. But PDF of SDSR is good for low traffic and its performance degrades as the traffic load and number of connections grows. Performance of SDSDV is very poor in all cases. Finally best performance is shown by SEAODV routing protocol.

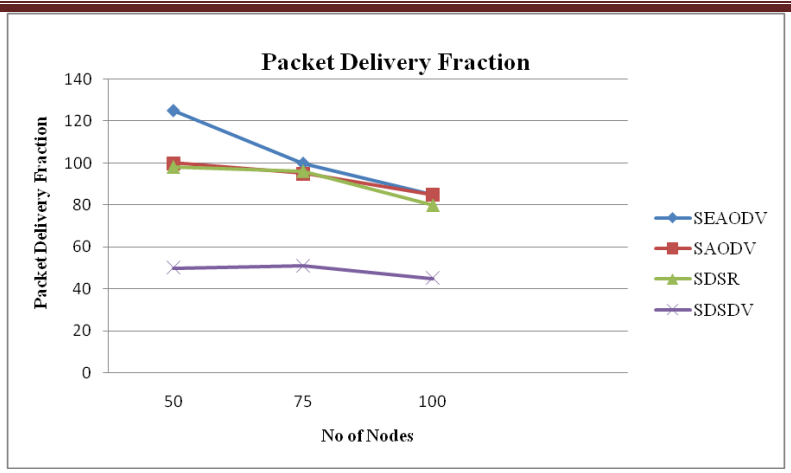

Figure.5 No of Nodes Vs Packet Delivery Fraction

4.4 End to End Delay

The below Figure.6 shows that Delay for SDSDV is least and almost constant for varying number of nodes. SDSR has much more delay as compared to SEAODV, SAODV and SDSDV.

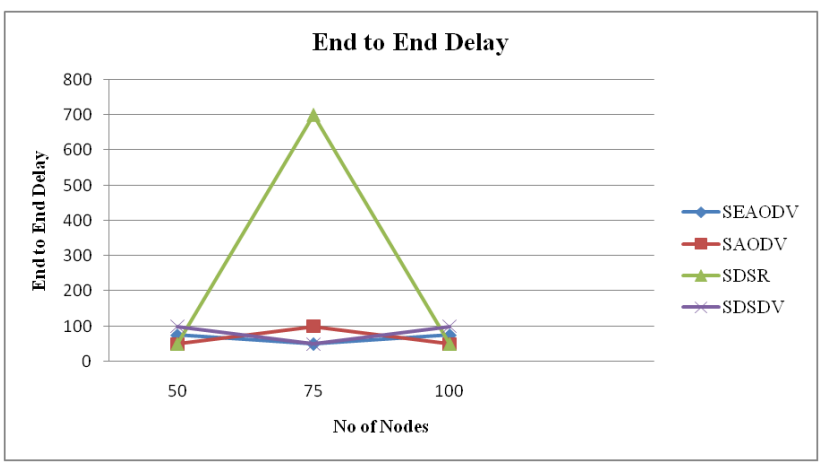

Figure.6 No of Nodes Vs End to End Delay

4.5 Energy Consumption

The above Figure.7 shows that as compared to other routing protocols, SEAODV used almost 100% less amount of energy for transmitting data among other nodes.

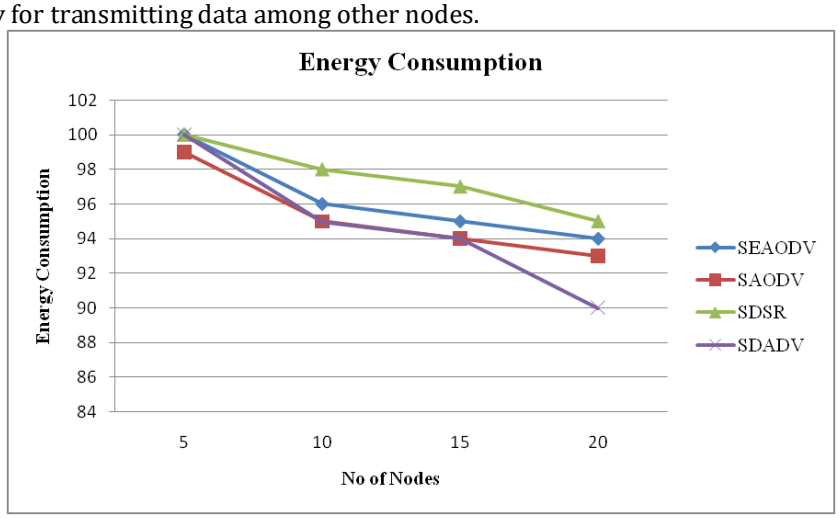

Figure.7 No of Nodes Vs Energy Consumption

4.6 Packet Drop

The number of data packets that are not successfully sent to the destination. Number of Packets Dropped is shown in figure 8.Number of Packets Dropped with SDSR is much higher than SEAODV,SAODV&SDSDV.

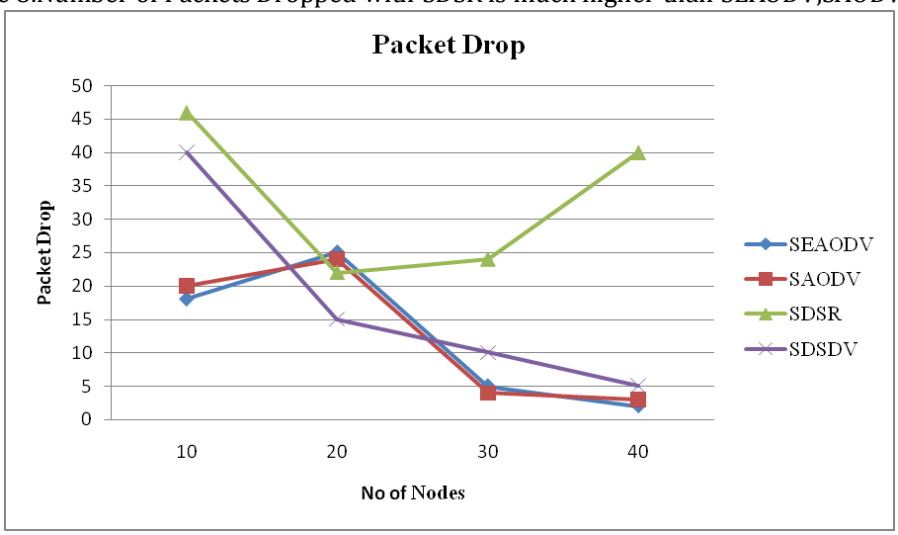

Figure.8 No of Nodes Vs Packet Drop

5. Conclusion

The proposed SEAODV routing protocol focuses are to secure the data transmission and also to construct a protected routing protocol. This is a hybrid of security mechanisms so that it gratify the primary security needs and assures the discovery of an accurate and secure route. In this paper performance comparison of SEAODV,SAODV, SDSR, andSDSDV routing protocols for Mobile Ad-hoc Networks is done as a function of number of nodes.Performance of these routing protocols is evaluated with respect to performance metrics such as Throughput, Packet Delivery Fraction, End to End Delay, Packets Drop& Packet Delivery Ratio. In our assumed scenario SEAODV shows best performance than SDSR &SDSDV in terms of Throughput, Packet Delivery Fraction, End to End Delay, Packet Delivery Ratio and Number of Packets Drop.This SEAODV routing protocol is more secure than the SAODV,SDSR,SDSDV.

REFERENCE

1. TaoShu and Marwan Krunz, Fellow, IEEE. “Privacy-Preserving and Truthful Detectionof Packet Dropping Attacks in WirelessAd Hoc Networks,” IEEE Transactions on MobileComputing, vol. 14, no. 4, April 2015.
2. Rahul Desai, Patil B P and Davinder Pal Sharma, “Routing Protocols for Mobile Ad Hoc Network: A Survey and Analysis”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 7, No. 3, September 2017, pp. 795 ~ 801.
3. Dilip Singh Sisodia, Riya Singhal, Vijay Khandal, “A Performance Review of Intra and Inter-Group MANET Routing Protocols under Varying Speed of Nodes”, International Journal of Electrical and Computer Engineering, Vol 7, No 5: October 2017.
4. Justin Sophia I, N. Rama, “Improving the Proactive Routing Protocol using Depth First Iterative Deepening Spanning Tree in Mobile Ad Hoc Network”, International Journal of Electrical and Computer Engineering, Vol 7, No 1: February 2017.
5. Youn-Sik Hong, “A Control Packet Minimized Routing Protocol for Ad-hoc Wireless Networks”, TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol.12, No.2, February 2014, pp. 966 ~ 975.
6. VivekSoi and Dr. B.S. Dhaliwal, “Performance comparison of DSR and AODV Routing Protocol in Mobile Ad hoc Networks”, International Journal of Computational Intelligence Research, Volume 13, Number 7 (2017), pp. 1605-1616.
7. Tamilarasan-Santhamurthy; “A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011, PP: 176-184.ISSN(online):1694-0814.
8. Asha and G. Mahadevan , “An Adaptive Cross-Layer Architecture to Optimize QOS Provisioning in MANET”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 6, No. 1, April 2017, pp. 16 ~ 25.
9. A. A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” Proceedings of the 27th Australasian Computer Science Conference (ACSC), vol. 26, no. 1, pp. 47–54, 2004.
10. Li, W., and Joshi, A., “Security Issues in Mobile Ad Hoc Networks,” Department of Computer Science and Electrical Engineering; University of Maryland, Baltimore County, 2007.

11. Narayanan, K.K.L., and Castro, A.F., "High Security for MANET Using Authentication and Intrusion Detection with Data Fusion," International Journal of Scientific & Engineering Research, Vol. 3, Issue 3, pp. 36-40, Mar. 2012.
12. Agrawal, S., Jain, S., and Sharma, S., "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," JOURNAL OF COMPUTING, Vol. 3, Issue 1, pp. 41- 48, Jan. 2011.
13. Wadbude, D., and Richariya, V., "An Efficient Secure AODV Routing Protocol in MANET," International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 4, pp. 274-279, Apr. 2012.
14. Goswami, J., &Dafda, A. (2012)."Security aspects with AODV in WMANETs". National Conference on "Power Systems, Embedded Systems, Power Electronics, Communication,Control and Instrumentation, Jan- 2012". Department of Electronics & Comm. Engg., L.D. Collage of Engg. Ahmedabad, Gujarat.
15. K. Meka, M. Virendra, and S. Upadhyaya. "Trust based routing decisions in mobile ad-hoc networks." Proceedings of the Workshop on Secure Knowledge Management (SKM 2006), 2006.
16. Cordasco, Jared, and Susanne Wetzel. "Cryptographic versus trust based methods for MANET routing security." Electronic Notes in Theoretical Computer Science 197.2 (2008): 131-140.
17. Sharma, Pankaj. "Trust based secure AODV in MANET." Journal of Global Research in Computer Science 3.6 (2012): 107-114.
18. Uddin, M., Rahman, A. A., Alarifi, A.,Talha, M., Shah, A.,Iftikhar, and M.,Zomaya, A., "Improving Performance of Mobile Ad Hoc Networks Using Efficient Tactical On Demand Distance Vector (TAODV) Routing Algorithm", International Journal of Innovative Computing, Information and Control, Vol. 8, No. 6, pp. 4375-4389, Jun. 2012.
19. M. G. Zapata, "Secure ad hoc on-demand distance vector (saodv) routing," IETF MANET, Internet Draft (work in progress), 2001.