International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 6, November- December 2017 ISSN 2278-6856

# Security and Performance Analysis of NDTAODV, SAODV and AODV Routing Protocol under RREQ Flood Attack by Varying Malicious Nodes in MANET

**Nirbhay Kumar Chaubey**
Associate Professor of Computer Science, S.S.Agrawal Institute of Computer Science,
Affliated to Gujarat Technological University, Navsari, Gujarat, India-396445

**Abstract** - ***Mobile Ad-hoc Networks (MANETs) are always deployed in the situation, where there is no fixed infrastructure but networks are susceptible to compromise due to its fundamental characteristics as open media dynamic topology and lack of centralized monitoring. In such a scenario, designing an efficient and secure routing protocol has been a major challenge. This paper study impact of resource depletion RREQ flood attacks of our proposed Neighbour Defence Technique for AODV (NDTAODV) with that of Secure Ad Hoc On-demand Distance Vector (SAODV) and Ad Hoc On-demand Distance Vector (AODV) routing protocol by varying malicious nodes in MANETs with respect to four major performance metrics such as Packet Delivery Fraction (PDF), Average Throughput (AT), End-to-End Delay (AED) and Normalized Routing Load (NRL). Simulations results demonstrate that the NDTAODV gives better security and performance than the AODV and on a par with that of SAODV with improved AED and NRL without using any lengthy complex cryptography processing on the mobile node in MANETs unlike SAODV.***

**Keywords-** MANETs, AODV, NDTAODV, SAODV, Cryptography, Routing Protocol, Route Request (RREO), Route Reply(RREP), PDF, AT, NRL.

## 1. INTRODUCTION

Various routing protocols for Mobile Ad-hoc Networks (MANETs) have been proposed and these protocols can be classified into the three categories : Proactive, Reactive and Hybrid. Many researchers performed experiments analysis to find the best protocol out of the available protocols. Nearly, all experiments lead to the most used and reliable protocol namely Ad hoc On-demand Distance Vector (AODV) [1]- [9]. But the AODV protocol has no security measures in-built in it[10], thus, it is vulnerable to many types of attacks. Further, designing adequate security schemes for MANET is very challenging. Several researchers proposed their work to provide secure route discovery and detection and prevention of attacks and eEach one has its own limitations and constraints[10]-[11]. Many existing solutions address ways to provide security using cryptographic mechanism, further it is a very tedious process which involves consuming lot of nodes's time and energy. The cryptographic based secure routing protocol like Secure AODV (SAODV), Authenticated Routing for Ad Hoc Networks (ARAN), Security-aware Ad hoc Routing (SAR) etc. require a key management service to keep track of key and node binding and this needs a trusted entity called the Certificate Authority (CA) to issue public key certificate to every node[10]. Cryptography and Key Management are too expensive for MANETs[12]. In this paper, we study extended work of our proposed Neighbour Defence Technique for AODV (NDTAODV) to Mitigate RREQ Flood Attack by varying number of malicious nodes in MANETs. Paper structured as follows: Section 2 describes the theoretical analysis of AODV, SAODV and NDTAODV routing protocol. In section 3, a description of the RREQ Flood Attack is given. Section 4 describes the related work in this area. Section 5 and Section 6 provide the simulation set up and result analysis respectively. This paper concluded in section 7 followed by the references and author profile.

## 2. THEORATICAL ANALYSIS OF AODV and SAODV

### 2.1 Ad hoc On Demand Distance Vector (AODV)

AODV is an on demand routing protocol which is especially developed for MANETs and it does not maintain up-to-date information about the network topology unlike proactive routing protocols [8]-[9]. To discover route, AODV uses control messages Route Request (RREQ) and Route Reply (RREP), routes are set up by flooding the network with RREQ packets, RREQ traverses the network, the traversed mobile nodes store information about the source, the destination, and the mobile node from which they received the RREQ. The later information is used to set up the reverse path from destination to the source. When the RREQ reaches a mobile node, that knows a route to the destination or is the destination itself, the mobile node responds to the source with a RREP packet which is routed through the reverse path set up by the RREQ. This sets the forward route from the source to the destination. To avoid overburdening the mobiles with information about routes which are no longer (if ever) used, nodes discard this information after some time called timeout. Whenever either destination or intermediate node moves, a Route Error (RERR) is sent to the affected source nodes.

Neighbourhood information is obtained by periodically broadcasting Hello packets [10] - [11].

### 2.2 Fundamental Working Of SAODV

Earlier in 2002-2004 M. G. Zapata and N. Asokan [13, 14] proposed a secure AODV routing protocol called Secure AODV (SAODV). SAODV incorporates two schemes (i) nodes signing (using digital signature) the control messages and (ii) protecting the mutable information such as the hop-count using Hash Chain. The first scheme in SAODV using Digital Signatures provides authenticity of the non mutable information in the routing messages.

Originators of routing messages (e.g. RREQ, RREP) digitally sign each message (excluding the hop-count field in the AODV message and the hash field in the SAODV extension), which ensures that nodes do not impersonate other nodes. Second scheme in SAODV using Hash Chains for SAODV protects the mutable information such as the hop-count field in the RREQ and RREP messages. The SAODV is based on asymmetric key cryptographic operation therefore the nodes in MANET are unable to verify the digital signatures quickly enough as they have limited battery life as well as processing power. Moreover if a malicious node floods messages with invalid signatures then verification can be very expensive.

### 2.3 Fundamental Working Of NDTAODV

This section describes extension of our proposed Neighbour Defence Technique for AODV (NDTAODV)[13]. The objective of carried out research work is to mitigate RREQ flood attacks to secure AODV routing protocol by varying number of malicious nodes in MANET without using any complex cryptography. AODV routing protocol has been modified to implement NDTAODV algorithm to isolate the flood attacker with the use of timers, peak value and Hello Alarm Technique (HAT). Proposed NDTAODV has (i) Broody list table and (ii) RREQ_count table which are maintained by every node in the network. Broody list table keeps the record of malicious nodes, RREQ_count table keeps track of the number of requests received from each neighbour and expiry value as timestamp in the particular interval. Flood timer is used to generate dummy packet by the attackers whereas cache timer is used to trigger the event for flushing the RREQ_count to check if number of request exceed the peak_value. Table 1 and 2 show Broody List and RREQ count table respectively.

**Table 1:** Broody List

| Malicious node 1 id |
|---|
| Malicious node 2 id |
| Malicious node 3 id |

**Table 2:** RREQ_count

| RREQ_ID | RREQentry | TimeStamp |
|---|---|---|
| Requester1 Id | 5 | 0.34566 |
| Requester2 Id | 1 | 0.55346 |

NDTAODV uses FloodTimer and CacheTimer, FloodTimer which continuously sends the request packet as the value 0.009 second. Every 0.009 second attacker broadcast the request packet in the network and CacheTimer is used to observe request table entry for the expire time and request count entry for the requester to check whether it exceeds peak (Threshold) or not. Hello Alarm Technique (HAT) is used for Global Notification to notify other nodes about existence of the malicious node in the network[15].

**********
**/. Proposed algorithm-NDTAODV to flush RREQ_Count table entry/.
**********
**

```
If(CacheTimertrigger)
Then
   Flush RREQ_Count table entry
If(check all entry for the RREQentry exceed the peak value in RREQ_Count table)
Then
      Put the RREQester in broodyList
If(RREQester is in broodyList)
Then
      Drop the packet
If((RREQester is Neighbour)&&(there is no entry in RREQ_Counttable))
Then
      Add the RREQentry for this RREQ in RREQ_Count table
If(RREQentry>PeackValue)
Then
   Put the RREQester in BroodyList
```

**Figure 1** Algorithm-NDTAODV

## 3. DESCRIPTION OF RREQ FLOOD ATTACK

MANETs are particularly vulnerable to resource depletion RREQ flood attack. Intruder node broadcasts mass RREQ packets to exhaust the communication bandwidth and resources of nodes so that valid communication between nodes cannot be sustained. The injected packet is a forged packet. Flooding RREQ packets in the whole network will consume a lot of resources of the network[15].

Attacker selects many IP addresses which are not in the network, if the attacker knows the scope of IP address in

the network. Because none of the nodes can answer RREP packets for these RREQ, the reverse route in the route table of node will be conserved longer. The attacker can select random IP addresses if it does not know the scope of IP addresses. Figure 2 shows an example of resource depletion RREQ flooding attack. Here, node 8 is an attacker and floods mass RREQ packets over the networks so that other nodes cannot build route path in the network.

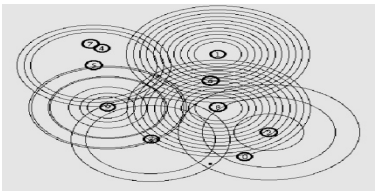

**Figure 2** Resource Depletion RREQ Flood Attack

## 4. RELATED WORK

In this section, some of the proposed solutions based on cryptographic or trust mechanisms to enhance security, improve performances of AODV routing protocols are discussed.

In 2015, Hanji and Shettar introduced an Improved AODV (I-AODV) protocol [16]. In the I-AODV protocol, the location and energy level of the nodes were considered, and the route discovery area was restricted based on the source and destination location. The nodes lying in this region were taken into account as route nodes. One hop communication took place when the two nodes were located in the communicating range of each other. If the communicating nodes were far away each other, then according to the distance between the selected intermediate node and destination node, the energy for the intermediate nodes was greater than the threshold energy, and the intermediate nodes were re-selected. This scheme could increase the lifetime of the path.

In 2015, Chaubey et al. [17] have proposed Trust Based Secure On Demand Routing Protocol(TSDRP) and studied the impact of Black hole attack with that of AODV routing protocol for making it secure. TSDRP protocol is capable of delivering packets to the destinations node even in the presence of malicious node while increasing network size. The performance of TSDRP and AODV routing protocol was tested with respect to different performance metrics, they concluded that in case of black hole attack TSDRP demonstrate better performance in almost all parameters: PDF, AED, AT and NRL as compared to AODV.

In 2015, Chaubey et al.[18] proposed a Trust-Based Secure on Demand Routing Protocol (TSDRP), considered the Packet Delivery Fraction (PDF), the Average End-to-End Delay (AED), the Average Throughput (AT), and the Normalized Routing Load (NRL), and analyzed the impact of the pause time of TSDRP and AODV under the blackhole attack and the DoS attack in MANET.

In 2015, Choudhurya et al. [19] proposed a scheme to modify the AODV routing protocol with the aim of mitigating the blackhole attack in MANETs. This scheme mainly created a Wait Time and Request Reply Tab table. Further, authors demonstrated a timer-based detection approach for identifying a blackhole node, modified the code of the AODV protocol according to the blackhole attack procedure, and proposed a timer-based method to overhear the next node action in the network layer, by using this approach, a blackhole node is completely removed from the MANET.

In 2014, A. Aggarwal, S. Gandhi, N. Chaubey et. al. in [12] proposed TSDRP protocol and evaluated result by varying number of malicious node and traffic connection. TSDRP assures that the packets are not handed over to malicious nodes and simulation result proved that the packet delivery ratio is higher, end to end delay is less, throughput is maintained compared to AODV.

In 2014, A. Aggarwal, S. Gandhi, N. Chaubey et. al. in [15] proposed NDTAODV a simple and effective technique to secure AODV routing protocol against RREQ flood attacks with different pause times in a small network with 20 node. Simulation results demonstrate that the attacks have a great effect on the network performance and NDTAODV efficiently detects and isolate the malicious nodes from the active route to make the network available. PDF of NDTAODV improve and AT which is the most important aspect of protocol is maintained while AODV performance drops significantly.

In 2013, R. Feng, S. Che, X. Wang and N. Yu in [20] proposed a novel trust mechanism named TDS-AODV. TDS-AODV can establish trusted route with minimum hops and maximum path trust based on trust mechanism denoted by TDS-AODV. Simulation results reveal that TDS-AODV can eliminate malicious nodes when building the route. The revised Dempster-Shafer (D-S) evidence theory is used to combine multiple recommended pieces of evidence and obtain the recommended trust value.

In 2011, Nabet, A., R. Khatoun, L. Khoukhi et al. in [21] proposed an Efficient Secure Routing Protocol (ASRP). To apply authentication, each node has to verify the identity of another node before communicate with it. Two new packets are added (Key Exchange and Authentication packets) for the purpose to obtain shared secret key between two neighbor nodes and authentication. In the Key Exchange packet, a Diffie-Hellman algorithm applies to collect a shared key required as a password in the authentication process. The packet authentication exploits the shared secret found in Key exchange to exchange parameters between two neighbors' nodes. ASRP algorithm limited the using of the trusted party in authentication stage, which is difficult to be established.

## 5. EXPERIMENTAL SETUP AND NETWORK SCENARIO

This section explains the complete evaluation methodology along with the simulation environment and network scenario in detail. Simulation was performed using Network Simulator (NS-2 Ver. 2.35) [21] to measure the

performance of proposed NDTAODV to be able to compare it with popular SAODV and basic AODV routing protocol. The simulation setup, network scenario and performance metrics are summarized in Table 3, Table 4 and Table 5 respectively.

**Table 3:** Summary of simulation setup

| Parameter | Value |
|---|---|
| Simulator | Ns-2(ver.2.35) |
| Simulation Time | 100 s |
| Number of Nodes | 70 |
| Routing Protocols | NDTAODV, SAODV, AODV |
| Traffic Model | CBR(UDP) |
| Number of Sources | 4 |
| Terrain Area | 1000m x 1000m |
| Mobility Model | Random Waypoint |
| Packet Size | 512 bytes |
| Packet Rate | 4pkt/s |
| MAC Protocol | IEEE 802.11 with RTS/CTS |
| Propagation Model | Two-Ray Ground Model |
| Antenna Type | Omni Antenna |
| Flood Interval | 0.009 sec |
| Cache Interval | 1 sec |
| Peack Value | 10 (no. of request) |
| Entry Expiry Time | CURRENT_TIME+1 |

**Table 4:** Summary of network scenarios

| Sr. No. | Network Scenario | Description |
|---|---|---|
| 1. | Malign environment (with attack) | Numbers of malicious nodes are varied from 1 to 7 |

**Table 5:** Summary of Performance Metrics

| Sr. No. | Performance Metrics | Description |
|---|---|---|
| 1. | Packet Delivery Fraction (PDF) | This is the ratio of the number of data packets successfully delivered to the destinations to those generated by sources. |
| 2. | Average End-to-End Delay (AED | This refers to the average delay in transmission of a packet across the network from source to destination. |
| 3. | Average Throughput (AT) | It is the rate of successfully transmitted data packets in a unit time in the network during the simulation. |
| 4. | Normalized Routing Load (NRL) | The number of routing packets transmitted per data packet delivered at the destination. |

## 6. RESULT AND PERFORMANCE ANALYSIS

The simulation results of compared protocols according to the network scenario described in Table 4 presented here and to test and compare the performance of NDTAODV against secure SAODV and basic AODV, we used NS-2.35 [21]. Also developed a set of tools viz. Traffic file, Mobility Files, TCL scripts [23] and AWK programs [24]-[25] to post-process the output trace files.

### 6.1 Impact of number of malicious node (1-7 node) on the routing path in the Network

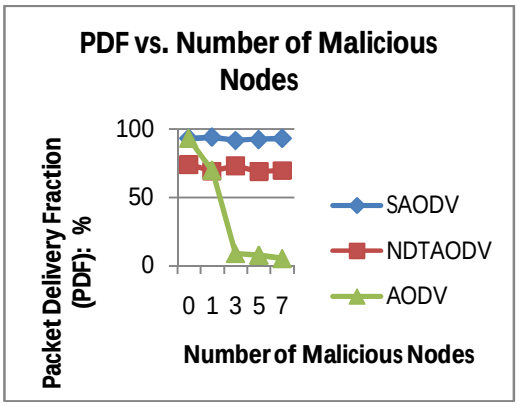


**Figure 3(a)** PDF vs Number of Malicious Nodes

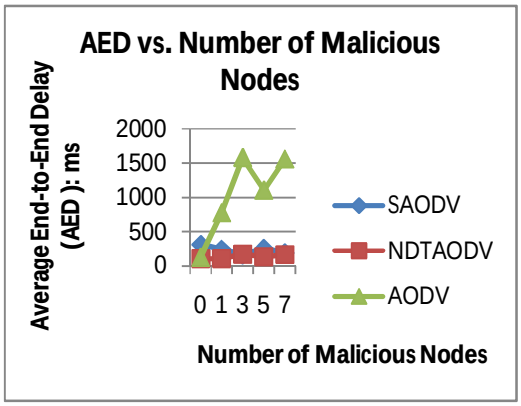


**Figure 3(b)** AED vs Number of Malicious Nodes

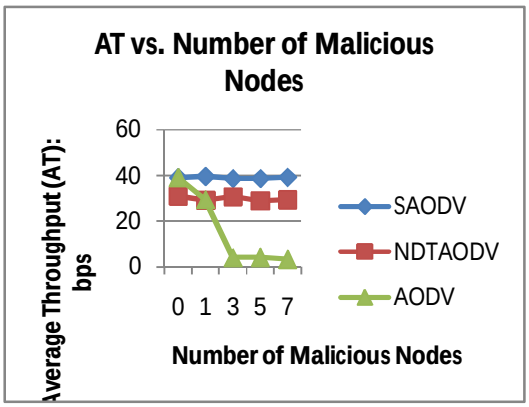


**Figure 3(c)** AT vs Number of Malicious Nodes

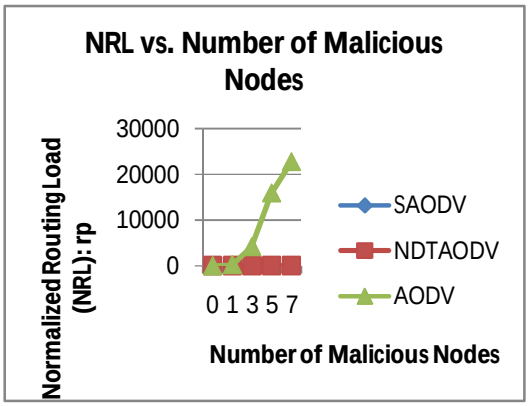


**Figure 3(d)** NRL vs Number of Malicious Nodes

Figures 3(a), 3(b), 3(c) and 3(d) represent the effect under Resource Depletion RREQ flood attack on PDF, AED, AT and NRL of our proposed NDTAODV and that of SAODV and AODV routing protocol while number of malicious nodes in the network is varied from 1 to 7 in the the malign network environment.

PDF of our proposed NDTAODV is consistently maintained between 70 to 75 % while that of AODV falls down to 5%.

AED of NDTAODV is consistent between 100 and 200 sec., lesser than the SAODV (192) and that of AODV is fluctuate vastly upto 1600 sec.

AT of our proposed NDTAODV is higher than that of the AODV (falls down drastically to below 5) and a little lower than the SAODV while NRL of NDTAODV is always less than that of SAODV and AODV (fluctuating 100 to 22,884). For the sake of brevity, Table 6 highlight the significance of the contributions of NDTAODV for 70 node network size under Resource Depletion RREQ flood attack for worst case only. Extended work of the proposed technique NDTAODV has been designed to mitigate attack and isolate the malicious node from the network.

**Table 6:** Performance Summary of NDTAODV , SAODV and AODV

| Worst Case Scenario | AODV | | | | SAODV | | | | NDTAODV | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PDF (%) | AED (sec.) | AT (bps) | NRL | PDF (%) | AED (sec.) | AT (bps) | NRL | PDF (%) | AED (sec.) | AT (bps) | NRL |
| Number of malicious nodes in the network : 7 | 5 | 1562 | 3 | 22884 | 93 | 192 | 39 | 18 | 69 | 164 | 29 | 4 |

## 7. CONCLUSION AND FUTURE SCOPE

Security and performance analysis of NDTAODV is compared with that of most popular SAODV and basic AODV protocol by varying number of malicious node in the MANETs and our findings is that, in case of resource depletion RREQ flood attack, NDTAODV demonstrate better performance in almost all performance metrics parameters: PDF, AED, AT and NRL as compared to AODV and nearly similar result with that of SAODV with improved AED and NRL. We can conclude that the NDTAODV is very efficient and able to prevent malicious nodes, isolates them from the active route and is capable of delivering packets to the destination in the MANETs without using any complex cryptographic mechanism which causes higher cost for route discovery unlike SAODV. The future scope of the paper is to more focus on implementation of Replay attack and Location Disclosure attack.

## References

[1] D. Kumar, A. Srivastava, and S. C. Gupta, “Routing in Ad Hoc Networks under Reference Point Group Mobility”, European Modelling Sysposium, IEEE Computer Society, pp. 595-598, 2013

[2] C. M. Cordeiro, D.P.Agrawal, “Ad Hoc & Sensor Networks”, Theory and Applications, World Scientific Publishing Ltd. 2006

[3] C Siva Rama, C. Murthy, B.S Manoj, Ad Hoc Wireless Networks Architectures and Protocols, Low price Edition, Pearson Education, 2007.

[4] D. P. Agrawal and Q.A. Zeng, “Introduction to Wireless and Mobile Systems”, Brooks/Cole Publishing, August 2002

[5] A. Agarwal, S. Gandhi and N. Chaubey, “Performance Analysis of AODV, DSDV and DSR in MANETs”, nternational Journal of Distributed and Parallel Systems (IJDPS), Vol. 2, No.6, November 2011, pp:167-177

[6] S. Gandhi, N. Chaubey, P. Shah, and M. Sadhwani, "Performance evaluation of DSR, OLSR and ZRP protocols in MANETs, " Computer Communication

and Informatics (ICCCI), 2012 International Conference on, pp. 1-5, 2012.

[7] S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Scenario based Performance Comparison of Reactive, Proactive and Hybrid Protocols in MANET", In Proceedings of the IEEE International Conference on Computer Communication and Infomatics(ICCCI), pp. 1-5. 2012.

[8] C. E. Perkins, "The Ad Hoc On-Demand Distance-Vector Protocol (AODV)" Ad Hoc Networking, Addison-Wesley, pp. 173–219, 2001

[9] C. Perkins, E Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing", RFC 3561, July 2003

[10] Farooq Anjum and Petros Mouchtaris, "Security for wireless ad hoc networks," John Wily, 2007.

[11] Akshai Aggarwal, Savita Gandhi and Nirbhay Chaubey "A Study of Secure Routing Protocol in Mobile Ad hoc Networks" in Proceedings of National Conferences on Advancement in Wireless Technology and Applications, SVNIT, Surat, India,Vol 8,pp. 18 -19,2008.

[12] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies(ACCT).

[13] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", Proceedings of ACM Workshop on Wireless Security (WiSe-2002), pp. 1–10, 2002

[14] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet Draft, http://ietfreport.isoc.org/idref/draft-guerrero-manet-saodv/

[15] Aggarwal A., S. Gandhi, N. Chaubey, et. al. , 2014. "Neighbor Defense Technique for Ad hoc On-demand Distance Vector (NDTAODV)". International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014 DOI: 10.5121/ijcnc.2014.6102

[16] Hanji, B.R.; Shettar, R. Improved AODV with Restricted Route Discovery Area. In Proceedings of the 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 8–10 January 2015.

[17] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, "Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size" 2015 Fifth International Conference on Advanced Computing & Communication Technologies, pp. 320–324, February 21–22, 2015.

[18] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, " Effect of Pause Time on AODV and TSDRP Routing Protocols under Black Hole Attack and DoS Attacks in MANET". In Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 11–13 March 2015.

[19] Choudhary, N.; Tharani, L. Preventing Black Hole Attack in AODV Using Timer-Based Detection Scheme. In Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems (SPACES), Guntur, India, 2–3 January 2015.

[20] R. Feng, S. Che, X. Wang, and N. Yu et. al., "A Credible Routing Based on a Novel Trust Mechanism in Ad Hoc Networks", International Journal of Distributed Sensor Networks Volume 2013, Article ID 652051, 12 pages, 2013

[21] Nabet, A., R. Khatoun, L. Khoukhi, J. Dromard and D.Gaiti, 2011. Towards secure route discovery protocol in MANET. Proceedings of the Global Information Infrastructure Symposium (GIIS), Aug. 4-6, Da Nang, pp: 1-8. DOI: 10.1109/GIIS.2011.6026717

[22] "The Network Simulator-NS-2", Home page, [Online] http://www.isi.edu/nsnam/ns/ns-build.html

[23] Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns". http://www.isi.edu/nsnam/ns/tutorial/

[24] Network Simulator - 2 (NS-2) http://mohit.ueuo.com/NS-2.html

[25] Tcl Developer Xchange, Main Tcl developer site, [Online] http://www.tcl.tk/

[26] Manish M. Patel, Akshai Aggarwal, Nirbhay Chaubey "Wormhole Attacks and Countermeasures in Wireless Sensor Networks: A Survey". International Journal of Engineering and Technology (IJET), ISSN 0975- 4024 (Online), Vol.9, No.2, January 2014

[27] Manish M. Patel, Akshai Aggarwal, Nirbhay Chaubey, "Detection of Wormhole Attack in Static Wireless Sensor Networks" 2nd International Conference on Computer,Communication and Computational Sciences (IC4S- 2017), Phuket, Thailand , 11-12 October 2017, Springer series: book on Advances in Intelligent Systems and Computing.

[28] Manish M. Patel, Akshai Aggarwal, Nirbhay Chaubey, "Analysis of Wormhole Attack in Wireless Sensor Networks", 5th International Conference on Advanced Computing, Networking and Informatics[ICACNI- 2017], NIT, Goa,India, 01-03 June, 2017, Springer series: book Advances in Intelligent Systems and Computing.

[29] Nirbhay Chaubey, Dharati H. Patel, "Routing Protocols in Wireless Sensor Network: A Critical Survey and Comparison", International Journal in IT and Engineering(IJITE), ISSN: 2321-1776[Online], Vol.04 Issue-02, February, 2016, Page: 8-18

[30] Nirbhay K. Chaubey, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study", International Journal of Security and Its Applications (IJSIA) 2016, 10 (5) (2016), pp. 261-274

**AUTHOR**

**Nirbhay K. Chaubey,** Ph.D (Senior Member of IEEE, Senior Member of ACM, Life Member of CSI) working as an Associate Professor, S.S. Agrawal Institute of Computer Science, Gujarat Technological University, Gujarat, India and a Ph. D. supervisor (Computer Science and Engineering), Gujarat Technological University. His research interests lie in the areas of Computer Networking, Wireless Networks (Protocol Design, QoS, Routing, Mobility, and Security), Cloud Computing and Sensor Network etc. He has published several research papers in peered reviewed International Journals, International and National Conferences. He has been a member of editorial board, technical program committee, reviewer for various Transactions and Journal of Computers and Communications apart from numerous refereed international and national conferences and workshops.