Nirbhay Kumar Chaubey, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 204-212 ISSN: 2321-8363
Impact Factor: 5.515

SECURITY ENHANCEMENT AND MINIMIZED DELAY OF NEIGHBOUR DEFENCE TECHNIQUE FOR AODV (NDTAODV) ROUTING PROTOCOL BY VARYING NETWORK SIZE IN MANETS

Nirbhay Kumar Chaubey
Associate Professor of Computer Science,
S.S.Agrawal Institute of Computer Science, Affliated to Gujarat Technological University,
Navsari, Gujarat, India-396445
E-mail: nirbhay@ieee.org

Abstract:

Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that can be established instantly without any help of fixed infrastructure and centralized monitoring. In this scenario, designing an efficient and secure routing protocol has been a major challenge over the last many years. In this paper, we study impact of RREQ flood attack of our proposed Neighbour Defence Technique for AODV (NDTAODV) with the existing Secure Ad Hoc On-demand Distance Vector (SAODV) and Ad Hoc On-demand Distance Vector (AODV) routing protocol by varying network size in MANETs with respect to four major performance metrics i.e. Packet Delivery Fraction (PDF), Average Throughput (AT), End-to-End Delay (AED) and Normalized Routing Load (NRL). Simulation results show that the NDTAODV gives better security and outperform the AODV in all performance metrics and also found nearly same result as that of SAODV with minimised AED and improved NRL without using any complex cryptography processing on the mobile node in MANETs.

Keywords - Ad Hoc Network, MANETs, on-demand Routing Protocol, AODV, NDTAODV, SAODV, RREQ Flood Attacks, Security, Performance Analysis, Route Request (RREO), Packet Delivery Fraction (PDF), Average Throughput (AT), End-to-End Delay (AED) and Normalized Routing Load (NRL).

1. Introduction

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any support of the existing infrastructure and centralized administration. This network has no fix routers, in fact all nodes work as a router and as a host[1]-[3]. Various routing protocols in MANETs have been proposed, these protocols can be divided into two categories: table-driven (proactive schemes) and on-demand routing (reactive scheme), researchers done several experiments with objective to find best protocol out of the available protocols. Almost all experiments lead to the most used and reliable protocol namely Ad hoc On-demand Distance Vector (AODV) [4]- [6]. AODV routing protocol has no security measures in-built in it[7] and it is vulnerable to many types of attacks. Interestingly, designing adequate security schemes for MANETs is a very challenging. Several researchers proposed modifications in AODV to provide secure route discovery and prevention of attacks using cryptography based encryption algorithm, nevertheless each one has its own limitations and constraints. 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 and the certificate authority (CA). Cryptography and key management are too expensive for MANETs [7]-[8]. In this paper, we study extended work of our proposed Neighbour Defence Technique for AODV (NDTAODV) to Mitigate RREQ Flood Attacks in MANETs. The proposed technique has been designed to isolate the malicious nodes from the network to make AODV routing protocol more robust. Our paper is divided into several sections as follows: Section 2 describes the theoretical analysis of AODV, SAODV and NDTAODV routing protocols. In section 3, a description of the RREQ Flood Attack is given. Section 4 explains the related work in this area. Section 5 and Section 6 provide the simulation set up and result analysis respectively. Finally, the section 7 concluded the paper followed by the references and author biography.

2. Theoratical analysis of AODV, SAODV AND NDTAODV

2.1 Ad hoc On Demand Distance Vector (AODV)

Ad-hoc On-Demand Distance Vector (AODV) is an on demand routing protocol which is used to find a route between the source and destination node as needed. AODV does not maintain up-to-date information about the network topology as it is done by the proactive routing protocols [9]-[10]. AODV protocol performs Route Discovery using control messages Route Request (RREQ) and Route Reply (RREP) as shown in figure 1. In AODV, routes are set up by flooding the network with RREQ packets which, however, do not collect the list of the traversed hops. Rather, as 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. When source node receives the RERR, it can reinitiate route discovery if the route is still needed. Neighbourhood information is obtained by periodically broadcasting Hello packets [11]. For the maintenance of the routes, two methods can be used: a) ACK messages in MAC level or b) HELLO messages in network layer. The fundamental route discovery process of AODV is depicted in Figure 1.

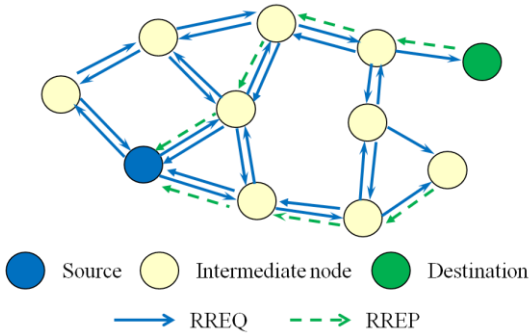

Figure 1: Fundamental Route Discovery Process of AODV[11]

AODV has no inherent security mechanisms and is full of security vulnerabilities making it trouble-free for attacker to perform attacks. The major vulnerabilities present in AODV routing protocol are due to (i) Possibility of attacker in impersonating as a source node S by forging a RREQ with its IP address as IP address of source node S (ii) Decreasing hop count in RREQ/RREP (iii) Increasing sequence number in RREQ/RREP (iv) Forging the RERR message and (v) Possibility of attacker impersonating as a destination node D by forging a RREP with its IP address as IP address of the destination node D.

2.2 Fundamental Working Of SAODV

Several researchers proposed modifications to the existing routing protocols such as AODV to make it secure and robust. Earlier in 2002-2004 M. G. Zapata and N. Asokan [12, 13] proposed a very first approach to 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 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. Whereas, the 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. 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 which leads for end to end delay. Furthermore, 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)[14]. The objective of carried out research work is to mitigate RREQ flood attacks to secure AODV routing protocol by varying number of connections 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[14].

**********/. 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 2: Proposed algorithm-NDTAODV

3. Description Of RREQ Flood Attack

AODV routing protocol is particularly vulnerable to RREQ Flood attacks wherein Intruder node broadcasts bulk RREQ packets to exhaust the communication bandwidth and resources of nodes so that the valid communication between nodes cannot be sustained. The injected packets are fake packets; attacker node puts its own defined value in RREQ packet in order to make this attack more dangerous. Flooding RREQ packets in the whole network will consume a lot of resources of the network. AODV protocol reduces congestions by limiting the number of messages originating from a node to RREQ_RATELIMIT per second.

After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value [14].

4. Related Work

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

In 2015, Su and Yang [15] proposed a routing algorithm based on the AODV and called RAODV (Resilient AODV). In the route discovery phase, RAODV differed from AODV. RAODV protocol established as many routes as possible unlike AODV which established only one routing path from a source node to the destination node. Thus, when the primary route broke, the node could immediately adopt an alternative route without further route search. If there was no possible alternative route, the node would transmit the route break information backward to instruct the previous node on the reverse route to select an alternative one until an alternative route was found. The RAODV could reduce the number of route rediscovery procedures and thus improve packet loss rate by 72.61% compared to traditional AODV especially in sparse MANET.

In 2015, Chaubey et al. [16] proposed Trust Based Secure On Demand Routing Protocol(TSDRP), studied the impact of Black hole attack with that of AODV routing protocol for making it secure. TSDRP protocol is able to deliver packets to the destinations node even in the presence of malicious node while increasing network size. In case of black hole attack TSDRP demonstrate better performance in almost all parameters: Packet Delivery Fraction (PDF), the Average End-to-End Delay (AED), the Average Throughput (AT), and the Normalized Routing Load (NRL), as compared to AODV.

In 2015, Chaubey et al.[17] proposed extended work of Trust-Based Secure on Demand Routing Protocol (TSDRP), analyzed the impact of blackhole attack and DoS attack of TSDRP and AODV by varying pause time in MANET, simulation results show that the TSDRP outperforms AODV with respect to performance metrics PDF,AED, AT, and NRL.

In 2014, A. Aggarwal, S. Gandhi, N. Chaubey et. al. in [11] proposed TSDRP protocol and evaluated result by varying number of malicious node and traffic connection. TSDRP confirm 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 [14] proposed NDTAODV a simple and effective technique to secure AODV routing protocol against flood attacks with different pause times by way of different number of malicious nodes 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. Packet Delivery Fraction (PDF) of NDTAODV improve and Average Throughput (AT) which is the most important aspect of protocol is maintained while AODV performance drops significantly under the presence of flood attack.

In 2014, Kasiran Z. et. al. [18] proposed a new approach and evaluated the throughput performance in AODV under a wormhole attack and Sybil attack, and provides the conclusion that the impact on throughput generated by the Sybil attack was greater than the impact of the wormhole attack.

In 2013, Liu et al.[19] presents an optimized protocol: B-AODV protocol to solve the shortage of routing finding and routing repair in AODV protocol. Two steps in B-AODV are adopted, firstly, BRREQ (B-AODV RREQ) was used to replace of RREQ in order to reduce the time of route finding and Secondly, the two hops record in control messages and route table could improve the rate of routing repair and reduce the time of route finding, Simulations results show that B-AODV gives better result than that of AODV.

In 2012, Ehsan, H. et. al.,[20] proposed Malicious AODV: Implementation and Analysis of Routing Attacks in MANET. Author analyzed blackhole attack, the selfish node behavior, the RREQ flooding attack and the HELLO flood attack in AODV routing protocol with respect to performance metrics i.e. packet efficiency, routing overhead, and throughput as our performance metrics. Simulation study shows that flooding attacks like RREQ flood and hello flood drastically increase the routing overhead of the protocol. Route modification attacks such as sinkhole and blackhole are deadly and severely affect the packet performance and bring down the network throughput to unacceptable ranges.

In 2010, X. Li et al. [21] proposed "Trust-based on-demand multipath routing in mobile ad hoc networks" AOTDV routing protocol wherein, trust of a node is represented as a weighted sum of forwarding ratio and path trust is computed as a continued product of node trusts. Here, node is considered malicious based on its forwarding behaviour.

In 2004, X. Li, M. R. Lyu et. al. [22] proposed "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" . Trust is represented by opinion, if a node behaves in a normal manner, other nodes increase its opinion, otherwise decrease its opinion. The nodes authenticate each other by verifying the certificate, which is an added overhead. However, the protocol is unable to detect an internal attack.

In 2012, Hazra and Setua proposed a trust computation-based Sybil attack avoidance scheme in AODV [23]. The TOR (Trusted On-demand Routing) model involved three major modules: the Node Manager, the Trust Module, and the Decision Manager. The Decision Manager secured the routing path on the basis of the trust value, which was computed in the Trust Module. The Node Manager reacted accordingly to AODV in response. Simulation results show the effectiveness of TOR model against sybil attack.

From the above analysis, nearly all of the secure protocols in AODV have been proposed for efficiently detecting and militating against the attacks in many different scenarios. However, not a single standard protocol captures common security threats. Thus, there is still a scope for continuous improvements of existing routing protocol.

5. Experimental Setup and Network Scenario

This section describes the simulation set up and network scenario. Simulation was performed using Network Simulator (NS-2 Ver. 2.35) [24] to measure the performance of proposed NDTAODV to be able to compare it with SAODV and 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 Malicious Nodes	2
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)	Number of sources node communicating in network 1- 4

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 Analysis of NDTAODV, SAODV AND AODV Under RREQ Flood Attack

The simulation results of compared protocols according to the network scenario described in Table 4 are presented below:

To test and compare the performance of our proposed NDTAODV with that of SAODV and AODV in malign network environment, we used NS-2.35 [24] and also developed a set of tools viz. Traffic file, Mobility Files, TCL scripts [25] and AWK programs [26]-[27] to post-process the output trace files.

6.1 Impact of network size (varying number of nodes 10-70) with 2 malicious nodes in the Network

Below Figures 3(a), 3(b), 3(c) and 3(d) represent the effect of RREQ flood attacks on PDF, AED, AT and NRL of NDTAODV, SAODV and AODV while network is varied from 10 to 70. It is evident from the figure that the PDF of NDTAODV is consistently increasing (80%), which is slightly lower than the SAODV and that of AODV is continuously falls down till 5%. AED of NDTAODV is always lower and it is maintained not more than 200 ms while increasing network size (30 – 70 node) than the SAODV, however, AED of AODV is always high above 1200 ms till 1800 ms. AT of our proposed NDTAODV is higher than that of the AODV and a little bit lower than the SAODV while NRL of NDTAODV is always less than that of SAODV and AODV (fluctuating 300 to 8110 rp).

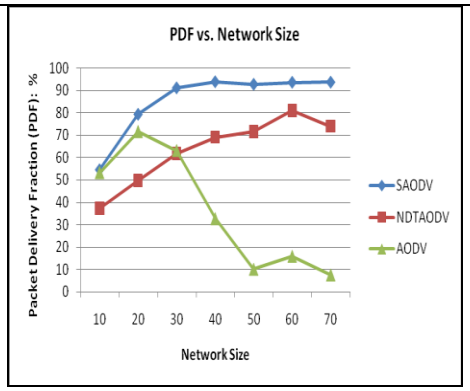

Figure 3 (a) : PDF vs Network Size

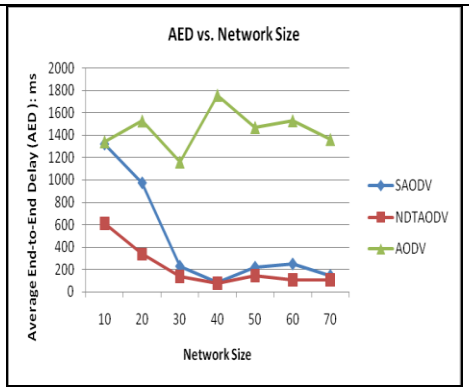

Figure 3 (b) : AED vs Network Size

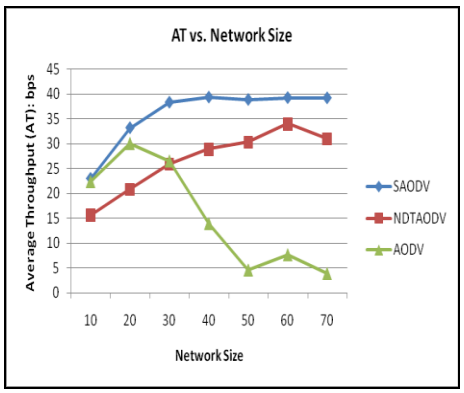

Figure 3 (c) : AT vs Network Size

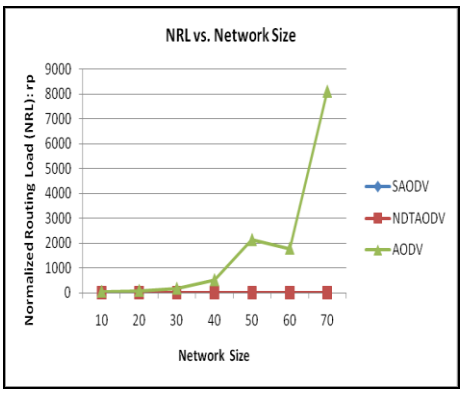

Figure 3 (d) : NRL vs Network Size

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.

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
Network Size : 70 Nodes	7	1358	3	8110	93	148	39	11	74	106	31	9

7. Conclusion and Future Scope

This paper presented an extended work of our proposed NDTAODV routing protocol. NDTAODV protocol is capable of delivering packets to the destinations even in the presence of multiple attacks while increasing network size and demonstrates better performance in almost all performance metrics as compared to AODV and almost similar result as that of SAODV with the improved AED and NRL. It can be concluded that in case of RREQ flood attack, NDTAODV is very efficient and able to mitigate malicious nodes and isolates them from the active route without using any cryptographic mechanism unlike SAODV. Performance of NDTAODV is better

in the malign environment (presence of attacks) whereas NDTAODV and normal AODV perform almost similar in the benign environment (absence of attacks). The future scope of the paper is to more focus on implementation of Byzantine attacks and Location Disclosure attack.

References

[1] C Siva Rama, C. Murthy, B.S Manoj, Ad Hoc Wireless Networks Architectures and Protocols, Low price Edition, Pearson Education, 2007.
[2] D. P. Agrawal and Q.A. Zeng, "Introduction to Wireless and Mobile Systems", Brooks/Cole Publishing, August 2002
[3] 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
[4] A. Agarwal, S. Gandhi and N. Chaubey, "Performance Analysis of AODV, DSDV and DSR in MANETs", International Journal of Distributed and Parallel Systems (IJDPS), Vol. 2, No.6, November 2011, pp:167-177
[5] 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.
[6] 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.
[7] Farooq Anjum and Petros Mouchtaris, "Security for wireless ad hoc networks," John Wily, 2007.
[8] 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.
[9] C. E. Perkins, "The Ad Hoc On-Demand Distance-Vector Protocol (AODV)" Ad Hoc Networking, Addison-Wesley, pp. 173–219, 2001
[10] C. Perkins, E Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing", RFC 3561, July 2003
[11] 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).
[12] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", Proceedings of ACM Workshop on Wireless Security (WiSe-2002), pp. 1–10, 2002
[13] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", IETF Internet Draft, http://ietfreport.isoc.org/idref/draft-guerrero-manet-saodv/
[14] 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
[15] Ming-Yang Su, Chih-Wei Yang proposed "A Resilient Routing Approach for Mobile Ad Hoc Networks". In Proceedings of the 2015 International Conference on High Performance Computing & Simulation (HPCS), Amsterdam, The Netherlands, 20–24 July 2015
[16] 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.
[17] 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.
[18] Kasiran, Z.; Mohamad, J. Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV. In Proceedings of the 2014 Fourth International Conference on Digital Information and Communication Technology and It's Applications (DICTAP), Bangkok, Thailand, 6–8 May 2014.
[19] Liu, S.; Yang, Y.; Wang, W. proposed Research of AODV Routing Protocol for Ad Hoc Networks1, American Applied Science Research Institute (AASRI) Procedia 2013, Volume 5, Page 21–31.
[20] Ehsan, H.; Khan, F.A. Malicious AODV: Implementation and Analysis of Routing Attacks in MANET. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25–27 June 2012.
[21] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," Information Security, IET, vol. 4, issue 4, pp. 212-232, Dec 2010.
[22] X. Li, M. R. Lyu, and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," in Proc. Aerospace Conference, IEEE, vol. 2, pp. 1286-1295, 2004.

[23] Swarnali Hazra, S. K. Setua, Sybil Attack Defending Trusted AODV in Ad-Hoc Network. In Proceedings of the 2012 2nd International Conference on Computer Science and Network Technology (ICCSNT), Changchun, China, 29–31 December 2012.
[24] "The Network Simulator-NS-2", Home page, [Online] http://www.isi.edu/nsnam/ns/ns-build.html
[25] Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns". http://www.isi.edu/nsnam/ns/tutorial/
[26] Network Simulator - 2 (NS-2) http://mohit.ueuo.com/NS-2.html
[27] Tcl Developer Xchange, Main Tcl developer site, [Online] http://www.tcl.tk/
[28] 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
[29] 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.
[30] 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.
[31] 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
[32] 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

Dr. 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.

