Empirical Study of NDTAODV, SAODV and AODV Routing Protocol in the presence of RREQ Flood Attacks in MANETs

Nirbhay Kumar Chaubey [†] and Lal Bihari Barik [††*],

[†]S.S.Agrawal Institute of Computer Science, Affiliated to Gujarat Technological University
Navsari, Gujarat, India
[††]Department of Information Systems, Faculty of Computing & Information Technology in Rabigh,
King Abdulaziz University, Kingdom of Saudi Arabia

Summary
Mobile Ad-hoc Network (MANET) is a decentralized wireless network, in which, mobile nodes are free in moving in and out from the network. MANET has several independent nodes that organize themselves in different ways and work without strict top-down network administration. In this scenario, designing a secure and efficient routing protocol with less delay and overheads is a major challenge. In this paper, extended work of our proposed Neighbour Defense Technique for AODV (NDTAODV) is presented and studied the impact of resource depletion RREQ flood attacks of NDTAODV with Secure Ad-hoc On-demand Distance Vector (SAODV) and Ad-hoc On-demand Distance Vector (AODV) protocol wherein a number of source node communicating in MANETs are varying. For the assessment of performances, Packet Delivery Fraction (PDF), Average Throughput (AT), End-to-End Delay (AED), and Normalized Routing Load (NRL) are considered. Simulation results demonstrate that the NDTAODV gives better security and outperform the AODV in all performance metrics and nearly same result as that of SAODV with improved AED and NRL without using any complex cryptography processing on the mobile node in MANETs.

Keywords:
MANET, NDTAODV, SAODV, AODV, Flood Attacks, algorithm and Security.

1. Introduction

MANET is composed of mobile nodes, arranged themselves and operate without centralized administration. This network has no fix routers, in fact, all nodes work as a router and as a host [1]-[2]. In early days of MANET, routing was the major challenge and researchers struggle to provide the best routing protocol for MANETS, researchers proposed a range of routing protocols but AODV protocol is more reliable and used with no security measures. 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 limitations and constraints. The cryptographic-based secure routing protocols are too expensive for MANETs [6]-[7]. In this paper, we present extended work of our NDTAODV to mitigate resource depletion RREQ flood attacks in MANETs while increasing number of source nodes communicating in the networks.

This paper is organized in the following ways: Section 2 describes the fundamental working of AODV, SAODV, and NDTAODV protocols. Section 3 describes the resource depletion RREQ flood attack. Section 4 discusses related works. Section 5 and Section 6 provide details of the simulation environment and result analysis respectively followed by conclusion in Section 7.

2. Theoretical Analysis of AODV, SAODV, and NDTAODV

This section discussed basic functionalities of AODV, SAODV and NDTAODV routing protocol.

2.1 Fundamental working of AODV

AODV uses Route Request (RREQ) and Route Reply (RREP) control packets to establish a path from source to the destination in the MANETs. AODV protocol does not support updated information about the network topology unlike proactive routing protocols [8]-[10]. The route request reaches to a mobile node, either destination itself or having a path to the destination. When the established route is broken and affected, AODV uses another control packet, i.e., Route Error (RERR) to send the affected source nodes. After receiving the RERR, it initiates a search to the route to finish [10]. Figure 1 show route discovery process of AODV.

Manuscript received November 5, 2017
Manuscript revised November 20, 2017

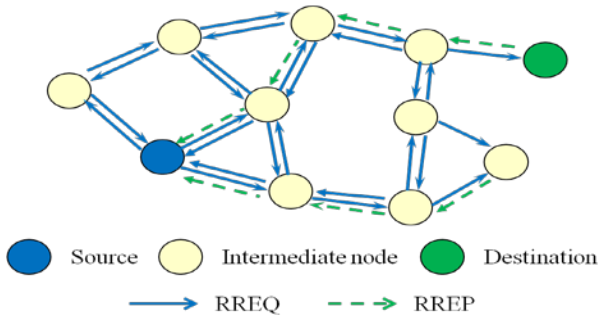

Fig. 1. AODV Route Discovery Process [10]

2.2 Fundamental working of Secure AODV (SAODV)

Earlier in 2002-2004, M. G. Zapata and N. Asokan [11, 12] proposed secure AODV routing protocol called Secure AODV(SAODV). SAODV include two schemes (i) nodes signing the control messages (using digital signature) and (ii) protecting the mutable information such as the hop-count using Hash Chain. The node authenticity is guaranteed through the knowledge of public keys in each node of the network. The originators of routing messages verify each authenticity digital signature content which ensures that nodes do not impersonate other nodes. However, hash chains are applied to the hop count certification where on each note for every hop can verify that the calculation of the hop was not maliciously reduced. Due to asymmetric key cryptographic nature of SAODV, it is unable to verify the digital signature of nodes in MANET as they have the processing power and limited battery life, which ultimately leads end to end delay.

2.3 Fundamental working of Neighbour Defense Technique for AODV (NDTAODV)

The purpose of our extended research work on NDTAODV is to mitigate RREQ flood attacks to secure AODV by varying number of the source to destination nodes connecting in MANET without using any complex cryptography algorithm. The revised AODV routing protocol is applicable in the NDTADV algorithm to reduce the flood attacker using a timer, 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_counttable is used to trace the number of requests received from each neighbouring node and expiry value as a time stamp 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 the number of requests exceeds 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 seconds. 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. Hello Alarm Technique (HAT) is applied in this protocols to inform nodes in the network about the existence of malicious node [13].
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
```

Fig. 2. Proposed algorithm-NDTAODV [13]

3. Description of RREQ flood attack

MANETs are particularly vulnerable to resource attenuation attacks, in which intruder node transmits mass

RREQ packets to eliminate bandwidth and communication nodes, where valid communication cannot be continued between the nodes. Injected packets are fake packets; the attacker node has made this attack more dangerous by putting its set value in REE packet. Throughout the network, Flooding RREQ packets consume a lot of resources of the network. AODV protocol adopts following method to reduce congestions: Limits the number of messages originating from a node to RREQ_RATELIMIT RREQ messages per second [13].

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 2016, Houda Muwdani, Mohammad Er-Ruedi, et al., [14] proposed a technique for attacking the blackhole and analyzed its effectiveness using network simulator NS-2. The results confirm that the flood and infiltration attacks have less impact as compared to blackhole attack on the performance of the network.

In 2015, Kuldeep Singh et al., [15] implemented Blackhole, Grayhole, Flooding and Rushing attacks. Their impact is studied on the protocols using parameters like AT, PDF, NRL, Packet Loss and Mean Hop Count.

In 2015, Chaubey N., Aggarwal A. et al. [16] proposed Trust Based Secure On-Demand Routing Protocol (TSDRP), studied the simulation based outcome of blackhole attack and compared the result with that of AODV for making it secure. TSDRP performs better than that of the AODV with respect to almost all performance metrics.

In 2015, Chaubey et al.[17] studied Effect of Pause Time on AODV and TSDRP Routing Protocols under Blackhole Attack and DoS Attacks in MANET. The simulation results illustrate that performance of TSDRP is enhanced than that of AODV in relation to NRL, AT, AED, PDF.

In 2014, TSDRP protocol was proposed by Aggarwal A., Chaubey N., Gandhi R. et al. [10] and further, evaluated the result using network simulator by changing the number of malicious nodes and also source node communicating in the network. TSDRP confirms that the packets are not assigned to the malicious nodes in the network, and the packet delivery ratio is very high, the AED is low while AT is maintained.

In 2014, A. Aggarwal et al. in [13] proposed NDTAODV a simple and effective technique to secure AODV routing protocol against flood attacks with different pause times by varying malicious nodes in small size network with 20 nodes. Simulations based results show that attacks have a significant effect on the network performance and security and NDTAODV efficiently detect the malicious nodes and isolate them from the active route to make the network available.

In 2013, Madhavi, S. and K Duraiswamy [18] considered hello flooding attack; performance of SAODV and Flooding Attack Aware SAODV (FAA-SAODV) was evaluated to decrease the control overhead by 2%.

In 2012, Humaira Ehsan, Farrukh Aslam Khan, et al., [19] studied sinkhole attack, blackhole attack, selfish node behavior and RREQ flood attacks through the simulation. Result demonstrate an enormous routing overhead in RREQ floods and hello floods.

5. Experimental setup and network scenario

This section gives details about the simulation set up and network scenario. Network Simulator (NS-2) [20] is used in the proposed NDDADOV to test and measure the performance metrics. Simulation setup, network scenario, and performance metrics are briefed in the following table.

Table 3. Outline 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
Number of Malicious Nodes in the Network	2
Terrain Area	1000m x 1000m
Mobility Model	Random Waypoint
Size of the packet	512 bytes
Packet Rate	4pkt/s
MAC Protocol	IEEE 802.11 with RTS/CTS
Propagation Model Used	Two-Ray Ground Model
Antenna Type	Omni Antenna
Flood Interval	0.009 sec
Cache Interval	1 sec
Peak Value	10 (no. of request)
Entry Expiry Time	CURRENT_TIME+1

Table 4. Outline of network scenarios

Sr. No.	**Network Scenario**	**Description**
1.	Malign environment (with attack)	Sources node communicating 1- 4

Table 5. Outline of Performance Metrics

Sr. No.	**Performance Metrics**	**Description**
1.	PDF	Ratio of the number of packets

		generated and then successfully delivered to the destinations.
2.	AED	Average delay of the packet transmission from source to destination node.
3.	AT	The rate of data packets efficiently transmitted in unit time.
4.	NRL	Amount of routing packets communicated per data packet delivered at the destination node across the network.

6. Result analysis of NDTAODV, SAODV, and AODV under RREQ flood attacks

We simulated our approach within the platform NS-2.35 network simulation [20], and the performance of our proposed NDTAODV is compared with that of SAODV and AODV in the malign network environment as per given network scenario in Table 4. [21]-[23].

Impact of Traffic Load (sources node communicating in the network 1- 4)

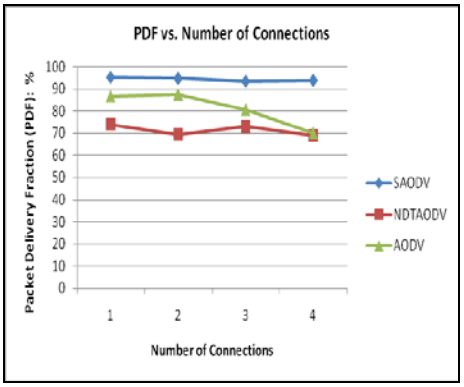

Fig. 3 (a): PDF vs. Number of Source Node Connections

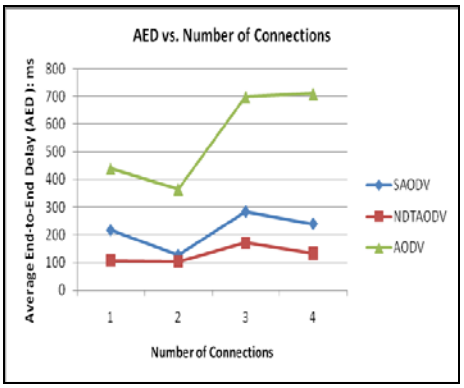

Fig. 3 (b): AED vs. Number of Source Node Connections

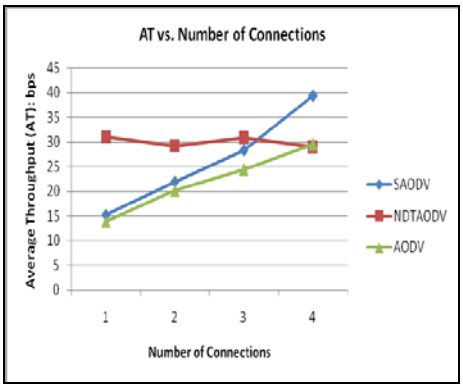

Fig. 3 (c): AT vs. Number of Source Node Connections

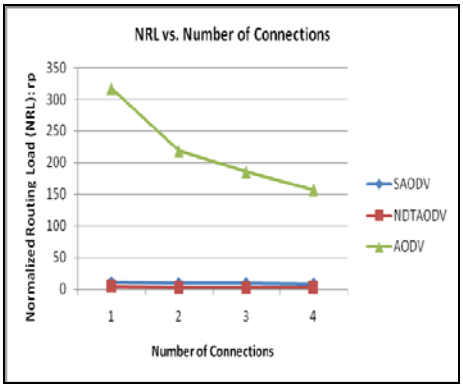

Fig. 3(d): NRL vs. Number of Source Node Connections

The effect of RREQ flood attacks on these three protocols with four performance metrics as per table no. 5 are shown in the above figures while transmitted source nodes in the network vary from 1 to 4. These figures are seen from the fact that PDF of NDTODV is consistently maintained above 70%, which is slightly lower than the SAODV, and that of AODV continuously falls down. AED of NDTAODV is always lower, and further, it is maintained below 180 ms than the SAODV due to none use any cryptographic mechanism, however, AED of AODV is always high in between 350 ms to 700 ms. The AT of our proposed NDTAODV is higher than that of the AODV and a little bit lower than the SAODV. NRL of NDTAODV is always less than that of SAODV and AODV (fluctuating 300 to 150). For the sake of brevity, Table 6 highlight the significance of the contributions of NDTAODV by varying number of connection for 70 node network size under Resource Depletion RREQ flood attack for the 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
Traffic Load : 4 Connections	70	710	29	157	93	240	39	8	70	133	30	2

7. Conclusion and future scope

In this paper, NDTODV has attempted to detect the effect of the malicious node RREQ flood attack and measure the performance with that of SAODV and AODV routing protocols in the presence of multiple attacks in the network by different numbers of the transmitted source nodes in the network. Our findings show that NDDADODV can reduce malicious nodes very efficiently and separates them from the active route. Further, without using any cryptographic mechanism, it can deliver packets with a less delay for the destination in the MANETs which is capable of causing high-cost discovery, unlike SAODV. The future scope of the paper is to more focus on the 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. Kumar, A. Srivastava, and S. C. Gupta, “Routing in Ad-hoc Networks under Reference Point Group Mobility,” European Modelling Symposium, IEEE Computer Society, pp. 595-598, 2013

[3] 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

[4] 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.

[5] 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 Informatics(ICCCI), pp. 1-5. 2012.

[6] Farooq Anjum and Petros Mouchtaris, ”Security for wireless Ad-hoc networks,” John Wily, 2007.

[7] 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.

[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] 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).

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

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

[13] 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

[14] Houda Moudni, Mohamed Er-rouidi et al., “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks” In Proceedings of IEEE International Conference on Electrical and Information Technologies (ICEIT), 2016, 4-7 May 2016,

[15] Kuldeep Singh, Amanat Boparai et al., Performance analysis of security attacks and improvements of routing protocols in MANET 2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM), 21-23 Sept. 2015,

[16] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, “Performance Analysis of TSDRP and AODV Routing Protocol under Blackhole 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 Blackhole 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] Madhavi, S. and K Duraiswamy “Flooding Attack Aware Secure AODV.” Journal of computer science, 9 (1): 105-113, 2013, doi:10.3844/jcssp.2013.105.113

[19] Humaira Ehsan, Farrukh Aslam Khan et. Al., “Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs” 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 25-27 June 2012,

[20] "The Network Simulator-NS-2", Homepage, [Online] http://www.isi.edu/nsnam/ns/ns-build.html
[21] Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns." http://www.isi.edu/nsnam/ns/tutorial/
[22] Network Simulator - 2 (NS-2) http://mohit.ueuo.com/NS-2.html
[23] Tcl Developer Xchange, Main Tcl developer site, [Online] http://www.tcl.tk/
[24] 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
[25] 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.
[26] 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.
[27] 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
[28] 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

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 peer reviewed International Journals, International, and National Conferences.

Lal Bihari Barik, (Ph.D. Computer Science) has over 17 years industrial & educational experience in the field of network technologies, AI, & adaptive intelligent educational system in a multi-agent environment development. He has worked on various web driven projects where exaMAIZE is one of his educational brand product. He has honored "IBM Drona Award 2008" and "Developer Super Star 2011" in the national level software development program organized by IBM. He has served as a resource person for many workshops in the area of open source software, process mining, etc. He has received research granted projects and published research papers and books.