MANTECH Publications

Journal of Research in Electrical Circuits and Systems
Volume 7, Issue 1, January-April 2022

Enhanced Aodv Implementation to Identify Passive Based Intrusion Detection Threats in Wireless Ad Hoc Networks

N. Anitha Devia[1], Sunidhi Chouhan[2]
Assistant Professor[1], Student[2]
Department of Electrical Engineering
Kumaraguru College of Technology, Coimbatore
Corresponding Author's E-mail: *sundhichouhan5@gmail.com*

Abstract

Wireless networks are made up of nodes, computers, or devices that connect with one another through network communication. Security is a growing difficulty job in wireless network communication. Some assaults arise in wireless ad hoc networks as a result of excessive internal data transfer activity. AODV (Ad hoc On-Demand Distance Vector) is an intrusion detection attack detection technology that provides a way to minimise packet delivery with regard to variable throughput dependent on data transmission. We use Enhanced AODV (which combines signature authentication with AODV) to increase network performance in terms of delivery ratio, throughput, and capacity across nodes in a static wireless communication architecture. Our experimental findings show that upgraded AODV can successfully identify distributed assaults through wireless network communication with low false positive rates.

Keywords: *Signature Authentication, wireless ad hoc networks, Static Topology, Ad hoc On-Demand Distance Vector, False Positives*

INTRODUCTION

Wireless ad hoc networks are made up of several computers, nodes, or devices that operate together with each client without the need of any pre-training topologies such as a central server or access point. There is no predefined centralised infrastructure required for node management in data transmission across wireless networks in this form of network.

Furthermore, a hop-by-hop routing sequence is employed to construct dynamic topology for cooperative communication from all wireless communication nodes. As a result, calculation of routing in a group of nodes data sharing is not feasible due to dynamic topology, which node trusted or not trusted in data transmission. Because of dynamic routing in communication, wireless ad hoc networks may be subject to internal assaults (both passive and active interfering attacks), denial of service attacks, and intrusion protection measures such as secure authentication and redundant data transfer. To address these issues, certain review approaches for detecting internal assaults were included.

Detection of various forms of assaults based on security monitoring of network dynamic topology and misbehavior of different network users in conventional intrusion detection attacks, there are two types: anomaly detection and misuse detection. In anomaly detection attacks, previous and historical network data with intended misbehaving of different nodes in construction of node profile with respect to normal behaviour with comparison of patterns of normal user with attacker behaviour in network communication. In this sort of modelled attack, misuse detection algorithms identify abuse actions of each node with evidence in network connection through wireless data transfer. Both anomaly and misuse-based attacks have benefits and drawbacks. Traditional intrusion detection algorithms identify misbehaving and anomalous behaviour based on patterns, with regard to false positives and the costly overhead associated in wireless connection. Another shortcoming of older techniques is the inability to mimic huge networks with changeable topology. The AODV (Ad hoc On-demand Distance Vector) proactive routing protocol was designed to define real-time intrusion and detection in wireless networks using a position-changed abuse detection technique that provides effective attack detection while reducing false positives in data transfer. AODV is only applicable for false information passive behaviour of node in dynamic topology. In passive attacks, another problem is encountered, namely collision-based attacks due to dynamic routing sequence in ad hoc wireless networks, so node identification and separate data transmission levels for wireless network communication. As a result, in this work, we propose to create Enhanced AODV. Enhanced AODV includes node verification based on signature authentication, followed by

simulation of dynamic routing between distinct nodes with successful data transfer using a static network design. This method combines simulation and implementation testing in the creation of outcomes in data sequences.

The rest of this paper is arranged as follows: Section 2 discusses related work in wireless communication and several sorts of strategies for detecting wireless communication assaults. Section 3 discusses the AODV protocol for wireless intrusion detection. Section 4 formalises the suggested method for detecting various sorts of assaults. Section 5 mimics the Enhanced AODV implementation outcomes, and Section 6 finishes the overall conclusion of assaults detection.

CONNECTED WORK

Hu et al.[8] proposed another framework called "Ariadne" in the context of the DSR technique for security redirection. A few affirmation structures, such as mechanised imprints, MACs discovered using combine insightful vital important components, or TESLA, might be applied with the suggested approach. Hash shops are employed to verify each bearing excitement, sheltering the system from over-trouble, and therefore avoiding organisation strikes. The suggested technique strongly discourages attacks from afflicted centre points from tampering with the uncompromised centres. To protect the discovered tracks, a combination of TESLA authenticators (MACs) is combined with cutting-edge switches and a hashing algorithm. The suggested method's security mechanisms are viable and may also be used to a wide range of occupied approaches.

Bhalaji et al.[9] distinguished between the diminish gap and the solid dull gap strike, which is one of the novel and probable strikes in off-the-cuff systems. In this attack, a dangerous centre positions itself as having the quickest route to the centre point whose groups it must identify. To lessen the possibility, it is advised to wait and examine the replies from all nearby centres to select a safe path. The mischief will be outstanding if these dangerous focal points join in a social gathering. This kind of strike is known as a solid dull gap strike. By selecting and selecting dull fissure centre locations, our treatment determines the secure path between source and range. In this chronicle, the proposed remedy is assessed using proliferation methodologies and compared to traditional DSR approach in terms of throughput, Bundle flow rate, and dormancy.

Dadhania et al.[10] investigated the profitability of AODV and DSR in the vicinity of a dull fissure strike (toxic centre point) and without a dull fissure strike with CBR (Constant Bit Rate) development under various flexible system flexibility. Propagation was used to examine and assess the impact in terms of throughput, Bundle assignment rate, and End to End Wait using a routine manner. Extensive testing were carried out for a 50 centre point offhand system utilising the structural test framework 2. The results show that the AODV is more vulnerable to Black Hole strikes than the DSR.

They have devised a fresh technique to recognise reduce cleft ambush in DPSAODV (Detection, Protection, and Sensitive AODV) [11], which separates that horrible centre point from the structure. The authority stores the Destination plan of action number of incoming bearing answer packages in the redirecting table and selects the edge quality to look at the expert get ready data in each day and age.

AODV

The AODV steering convention [12] is a remote impromptu system responsive convention. When a source hub requires a path to a goal, it initiates a route disclosure operation to locate the target hub. As shown in Figure 1(a), the source hub S floods the system with a route request packet (RREQ), requesting that a course be set up to the objective D. When an RREQ is received, middle of the road hubs update their steering table with a turnaround route to the source. All accepting hubs that do not have a path to the destination broadcast the RREQ bundle to their neighbours with a higher hop count. When the RREQ query arrives at the objective or another middle of the road hub with a current path to the goal, a route reply (RREP) is sent back to the source hub. As the RREP spreads to the source, the forward path to the destination is updated via middle-of-the-road hubs accepting an RREP bundle.

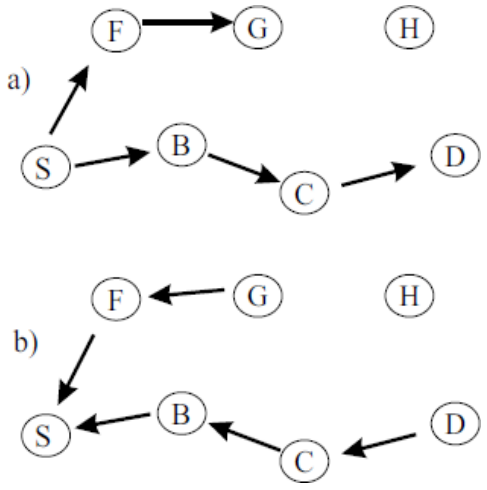

Figure 1: AODV route discovery specification

Figure 1(b) shows that both the goal hub D and the intermediate hub G have a path to the objective. They will now respond to the RREQ with an RREP bundle. To determine the freshness of direction data and to assure circle-free paths, AODV employs grouping numbers. If many highways intersect, a hub selects the route with the highest significant succession number. If many courses have a similar grouping number, the hub selects the course with the shortest hop-count. Clocks are used to keep course portions fresh.

When a connection fails, route error (RERR) packets multiply down the inverse path to the source, nullifying any softened passes up the steering tables of the midway hubs. AODV also sends out HELLO messages on occasion to maintain the network of surrounding hubs up to date. The AODV convention does not have a specific security component, such as solid confirmation.

As a result, there is no obvious way to predict nefarious behaviour, for example, MAC satirising, IP parodying, dropping packages, or modifying the content of control parcels. Conventions such as SAR [9] and SAODV [12] protect AODV against a limited number of attacks, but at the expense of execution in terms of overhead and idleness.

WIRELESS AD HOC NETWORK INTRUSION DETECTION SYSTEM PROPOSED

In this part, we build and implement an enhanced intrusion detection system, known as Enhanced AODV, to identify internal AODV assaults in wireless ad hoc networks. It is a host-based or network-based intrusion in static topology wireless ad hoc networks that is based on dynamic or stateless route sequences. In this section, we will present the route states approach, also known as the Transition Analysis Technique (TAT).

TAT depicts PC intrusions as a set of behaviours that an attacker does to compromise the security of a computer system. States allude to the representation of a framework's erratic, semi-perpetual, and long-lasting memory.

A depiction of an attack has a safe starting point, at least zero middle of the road states, and at least one traded off finish state. Methods for affirmations, which are abilities with at least zero contentions yielding Boolean esteems, are used to represent states.

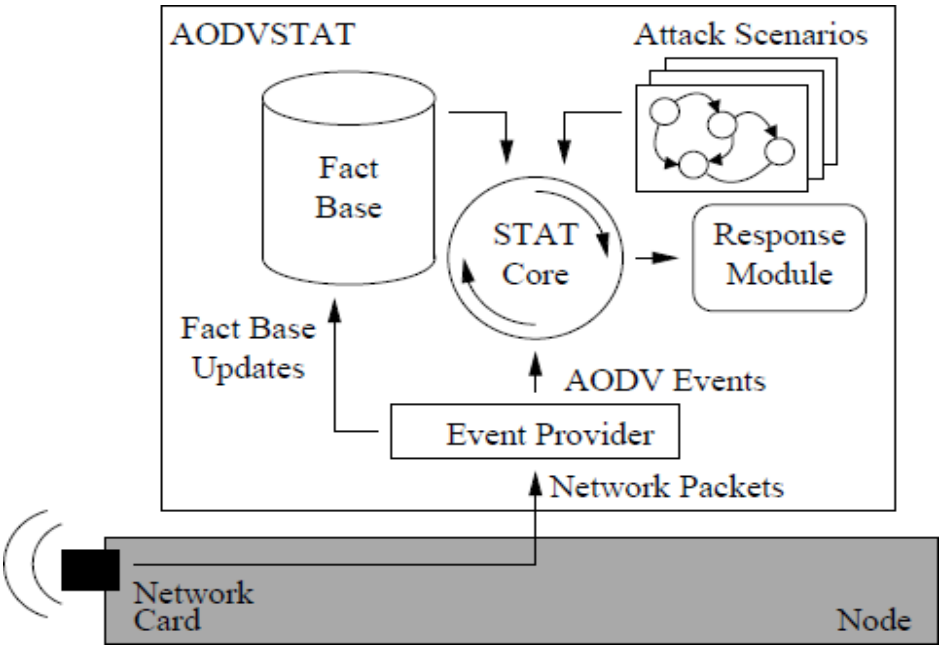

Figure 2: The suggested system's basic design.

Typically, these affirmations depict a few aspects of the framework's security situation, such as document ownership, client ID, or system activity features. Moves between stages are described with trademark activities that depict the actions that, if left out of the execution of an attack scenario, would prevent the assault from being completed successfully. An event demonstration is used to convey mark actions. Figure 2 depicts the basic design of the proposed AODV.

Figure 2 depicts the architecture of the suggested solution, which includes a practical step-by-step process with sequential data transfer. Which is a packet sniffer-based network monitoring system that receives packets from network infrastructure through state transmission in route sequences with a number of transition assaults that define a specific attack sequence in the form of an intrusion warning in ad hoc wireless communication. The discovery technique is based on an inside reality foundation that has updated data about adjacent hubs. By breaking down the monitored information packets and AODV control messages, the reality foundation is updated. More precisely, information parcels are used to determine how much movement has been produced, received, and transmitted by each hub, while AODV control bundles are used to extricate the AODV arrangement numbers of the dynamic hubs, the IEEE 802.11

header subtle elements (for example, the casing control field and the IEEE succession number), and the MAC/IP address sets of the hubs in the sensor's range. When a sensor is in circulating mode, the reality base also incorporates data obtained from other nodes through UPDATE messages.

1) Algorithm Process

The enhanced AODV's general procedure includes the following data communication steps.

Table 1 shows an improved AODV implementation procedure for detecting intrusion in wireless ad hoc networks.

STEP 1: To uniquely identify this route request message, the E-AODV Route request message has the following fields: source IP address, destination IP address, hop count, broadcast ID, source sequence number, request time, and destination sequence number.

STEP 2: After receiving the original route request message, the destination node creates a turn around route request (TA-RREQ) message and sends it to neighbour nodes within the transmission region.

STEP 3: The following fields are included in the E-AODV turn around route request message: broadcast ID, destination IP address, Destination Sequence Number, Source IP address, Reply Time, and hop count.

STEP 4: When a TA-RREQ packet is broadcast, the intermediate node checks for duplicate messages.

STEP 5: If it has already received a comparable message, it discards it; otherwise, it passes the message to succeeding nodes.

STEP 6: When the source node receives the first TA-RREQ message, it begins delivering packets.

STEP 7: Late-arriving TA-RREQs are saved for future use.

STEP 8: When the primary route fails, the other routes may be utilised.

We create standard solutions for dynamic route sequences in network communication with sequential data transfer through network using this approach.

EXPERIMENTAL ANALYSIS

Dark opening strike has been linked to ns-3 [13] proliferation. We use CBR (Constant Bit Rate) programme, TPC/IP (full duplex correspondence), IEEE 802.11b MAC, and genuine physical course taking into account true era arrange for our models. In a 500 by 500 rectangular of smooth area, the repetitive pattern comprises 30 subjectively assigned wi-fi central spots. The centre point transmitting combination has a driving range of 250 metres. For circumstances with centre flexibility, a unique route point diagram is employed. The selected stop time is 30 seconds to several minutes. A visitor producer was created to replicate continuous piece entirety (CBR) resources. The information payload is 512 bytes long. In our case, we take 30 centre points, with centres 1-22 and 25-30 being clear, and centres 23 and 24 being risky or dark gap centres. The recreation is completed using ns-3 to test the structural sufficiency by varying the centre point flexibility [11][12].

The tests used to evaluate performance are listed below.

a) Packet Delivery Ratio: The speed of group formation initiated by "application layer" CBR resources and group formation acquired by the CBR channel at a definitive region.

b) Throughput: Throughput is a critical measure of persuading thought movement over an affiliation path. Table 2 shows the simulation parameters for the suggested design. Figure 3 depicts a sample node simulation screen for the suggested technique

Table 2: Simulation Parameters.

Property	Value
Coverage Area	1700*1800
Number of Nodes	22
Simulation Time	30S
Transmission Range	350 m
Mobility Speed	0-30m/sec
Number of attacker nodes	03
Check point nodes	4 nodes(Fixed)

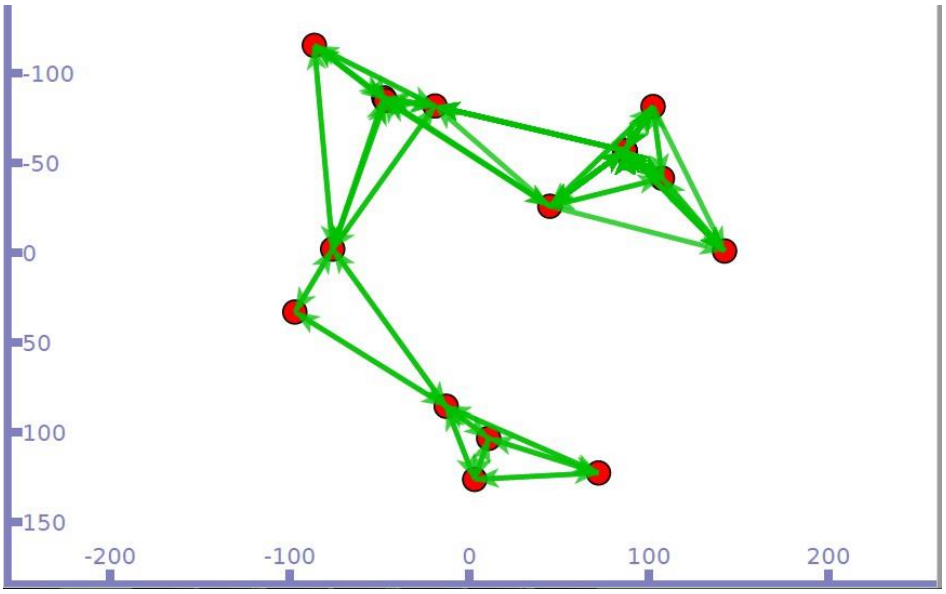

Figure 3: Proposed upgraded AODV systems with various node instances.

Figure 3 depicts the packet delivery ratio of the suggested technique with sequential data transfer, while Figure 4 depicts the simulated results.

Figure 4 shows the packet delivery ratio in improved AODV with various formats.

Figure 5 depicts the increased AODV data transmission values with sequence numbers.

```
Starting simulation for 35 s ...
20:41:44 environ              No en_IN translation found for domain kiwi
Could not load icon applets-screenshooter due to missing gnomedesktop Python mod
ule
scanning topology: 22 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
PING  10.0.0.22 56(84) bytes of data.
64 bytes from 10.0.0.22: icmp_seq=0 ttl=62 time=57 ms
64 bytes from 10.0.0.22: icmp_seq=1 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=2 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=3 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=4 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=5 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=6 ttl=62 time=2 ms
64 bytes from 10.0.0.22: icmp_seq=7 ttl=64 time=12 ms
64 bytes from 10.0.0.22: icmp_seq=8 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=9 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=10 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=11 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=12 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=13 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=14 ttl=64 time=0 ms
64 bytes from 10.0.0.22: icmp_seq=15 ttl=64 time=0 ms
```

Figure 5: Data transmission levels for various nodes in terms of sequence number generation.

Figure 6 depicts the proposed approach's throughput presentation with various nodes in wireless communication.

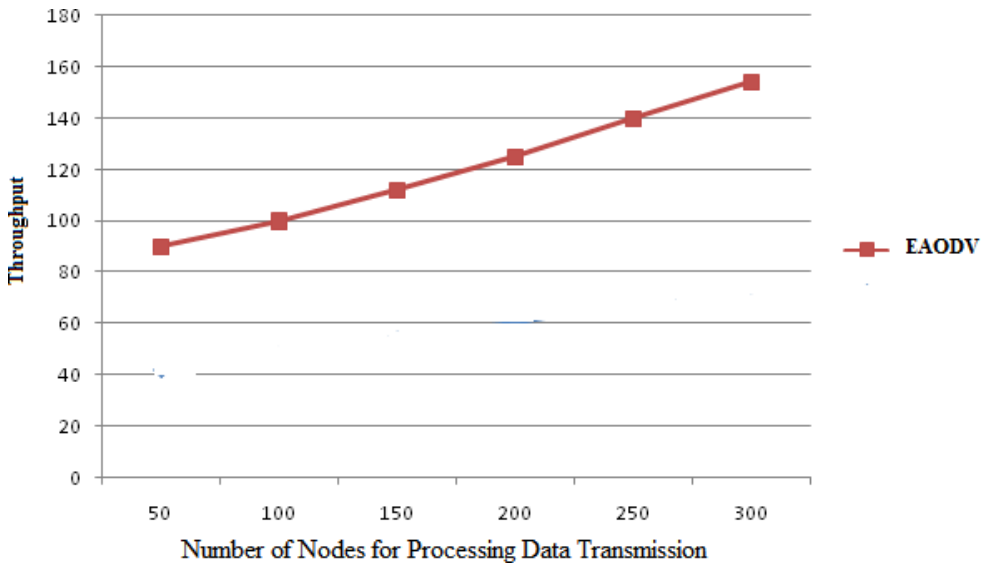

Figure 6: The suggested AODV implementation's throughput figures.

False positives occur in static topologies due to the modification of grouping numbers in RREP parcels. As a result, an increase in the number of attacks detected for no versatility scenarios leads to an increase in the rate of false positives found.

CONCLUSION

Because of their lack of security considerations during their construction, ad hoc routing protocols are vulnerable to a variety of attacks. By delivering fake routing information during the route discovery phase, a passive collision attack affects regular network operation. We also go through the AODV proactive routing methodology with various route arrangements. In this research, we propose and apply the Enhance AODV technique with regard to increasing packet delivery ratio and throughput presentations in ad hoc data transfer for effective detection of passive-based behaviour threats in wireless communication. The next step in implementing our suggested technique is to adapt it to accommodate dynamic topology innovations in wireless ad hoc networks.

REFERENCES

1. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003.

2. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

3. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.

4. Harmanpreet Kaur, P. S. Mann "Prevention of Black Hole Attack in MANETs Using Clustering Based DSR Protocol" IJCST Vol. 5, Iss ue 4, Oct - Dec 2014 ISSN :

0976-8491 (Online) | ISSN : 2229-4333 (Print).

6. Mr.Rahul Vasant Chavan 1, Prof.M S.Chaudhari " Enhanced DSR protocol for Detection and Removal of Selective Black Hole Attack in MANET", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072.

7. K.Mahamuni1 and Dr.C.Chandrasekar2, "Mitigate Black Hole Attack In Dynamic Source Routing (DSR) Protocol By Trapping", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org.

8. Bouhorma, M., Bentaouit, H., and Boudhir, A. (2009, April). Performance comparison of ad-hoc routing protocols AODV and DSR. International Conference on Multimedia Computing and Systems'2009(ICMCS'09), 2-4 April 2009, pp. 511- 514.

9. Y. Xue and K. Nahrstedt, .Providing fault-tolerant ad-hoc routing service in adversarial environments,. Wireless Personal Communications, Special Issue on Security for Next Generation Communications, Kluwer Academic Publishers, vol. 29, no. 3-4, pp. 367.388, 2004.

10. R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, .Sustaining cooperation in multi-hop wireless networks,. in Proc. of the 2nd Symposium on Networked Systems Design and Implementation, April 2005

11. M. Conti, E. Gregori, and G. Maselli, .Towards reliable forwarding for ad hoc networks,. in Proc. of Personal Wireless Communications (PWC '03),
September 2003.

12. B. Awerbuch, D. Holmer, C-N. Rotaru, and H. Rubens, .An on-demand secure routing protocol resilient to byzantine failures,. in ACM Workshop on Wireless Security (WiSe), September 2002.

13. Gundeep Singh Bindra1, Ashish Kapoor 2, Ashish Narang 3, Arjun Agrawal, " Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs" 2012 International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia

14. S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Proceedings of the 6th annual international conference on Mobile Computing an Networking (MOBICOM), Boston, Massachusetts, United States, 2000, 255-265.

15. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

16. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003

17. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.

18. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363–65.