DH-EAACK Secure Intrusion Detection System to detect Black Hole Attack in MANET

Sarika Patil
M.E (Computer Network),
Flora Institute of Technology, Pune,
Maharashtra, India.

Bharat Tidke
Assistant Professor, Computer Engineering
Department, Flora Institute of Technology, Pune,
Maharashtra, India.

ABSTRACT
Mobile Ad-Hoc Networks (MANETs) type of Ad-hoc wireless network. Due to mobility of nodes, MANET more vulnerable to different types of attacks and security threats. To overcome these challenges Intrusion Detection System technique used. By using the schemes of EAACK, this paper proposed dynamic hierarchical intrusion detection architecture that addresses these challenges while finding specific and conventional attacks in MANET. The proposed structural design organized as a dynamic hierarchy. Dynamic hierarchy in which hierarchy organized as group of clusters, cluster heads are selected based on topology and other criteria. Routes are initialized by using AODV routing protocol. The usefulness of the architecture demonstrated via black hole attack scenarios in which attack is detected and removed. In this paper we propose Dynamic Hierarchical Enhanced Adaptive Acknowledgement (DH-EAACK) architecture which has better performance in terms of packet delivery ratio and throughput due to cluster based IDS. Comparing results of existing systems with proposed system when there are 30% malicious nodes in the network PDR is 0.9% better than existing techniques. End to end delay, routing overhead has less performance compared with existing due to black hole nodes in the network. Future work can be extended by using election algorithms to elect cluster head and provide more security by using hybrid (AES and MD5) cryptographic algorithm.

Keywords
Ad-hoc On demand Routing Protocol, Attacks, Digital Signature, Intrusion Detection System (IDS), Mobile Ad-hoc Network, Security.

1. INTRODUCTION
Mobile Ad Hoc Networks (MANETs) has popular area of research now a days due to wireless medium and control through industrial remote access [1]. One advantages of wireless networks, its ability to allow data communication between different networks and still maintain their mobility. However, this communication is limited to the range of transmitters and receiver. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET used in the situation where infrastructure network unfeasible to install such as natural or human-induced disasters, military conflicts, and medical emergency situations [2], [3]. MANET does not require a fixed Infrastructure; thus, all nodes are free to move randomly [4]. Due to dynamic nature of the MANETs are weak to major harmful attacks and threats. . Intrusion means any set of action that attempts to compromise the integrity, confidentiality, availability of resources [5]. Intrusion detection challenging task due to dynamic topology, routing protocol attacks, limited bandwidth, noise or interference in network and continuous disconnectivity due to mobility. To overcome these constraints, existing systems have work on number of intrusion detection techniques, architectures using different routing protocols. First Intrusion Detection System (IDS) technique Watchdog [6] has detected malicious nodes in the network. There are other techniques which has removes drawbacks of Watchdog [6]. One of technique EAACK [7] is acknowledgment based IDS which increases the Packet Delivery Ratio as compared to existing system. EAACK [7] detects malicious nodes in presence of receiver collision, false misbehavior report, and limited transmission power. There are two types routing protocols in MANET, proactive and reactive and hybrid .Proactive routing protocol maintains routing tables to store route information and table updated periodically e.g DSDV [8]. Reactive routing protocols are on demand routing protocols. e.g AODV [9], DSR [10]. Depending on some criteria there are two types of attacks in MANET, active attack and passive attack [11],[12],[13]. Proposed system based on Dynamic Hierarchical Intrusion Detection architecture [14]. Dynamic Hierarchical Enhanced Adaptive Acknowledgment based IDS (DH-EAACK) to detect and remove the packet dropping attack called as Black hole attack [15]. DH-EAACK has cluster based topology. Black hole attack [15] has been studied by many researchers, but the black hole attack in acknowledgement based system is becoming more popular area of research. Black hole attack detection technique works in two phase Route Discovery Phase and Data Packet Sending phase. Black hole Attack called Dropping attacks is caused by selfish nodes or compromised nodes in the network, by dropping all data packets. It prevents end to end communication between nodes.

2. LITERATURE REVIEW
Watchdog & Pathrater proposed by S. Marti, T. J. Giuli, K. Lai, and M. Baker [6] which increases throughput of network in the existence of malicious nodes. Disadvantages are that it does not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping.

Huang and Lee [16] proposed a cluster based cooperative intrusion detection system able to detect type of attack and attacker. Disadvantages are if the system does not implement clusters then the detection accuracy is poorer. Does not elect compromised or malicious node as cluster head.

Kejun liu et.al.[17] proposed 2ACK scheme solves the difficulty of detecting misbehaving links rather than misbehaving nodes.2ACK packet has been assigned route of two hops which is fixed in the opposite direction of the data

traffic route. Disadvantage of 2ACK, is higher routing overhead due to transmission of 2ACK packets.

TWOACK[18] detects misbehaving links. The TWOACK scheme successfully solves the receiver collision and limited transmission power. Disadvantages are acknowledgment packets needs to transfer for each packet, increases congestion and network overhead.

AACK[19] is an end-to-end acknowledgment. Disadvantages of AACK it does not detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

EAACK [7] proposed by Elhadi M. Shakshuki Malicious nodes are detected by using Enhanced Adaptive Acknowledgement scheme. EAACK scheme is incorporated with digital signature to provide security. Compared to RSA [22], DSA[23] has more overhead. These techniques have drawbacks due to the collusions of packets and distribution of keys between nodes becomes overhead. The researchers have been studied on drawbacks of EAACK system such as key exchange problem and the hybrid cryptography problems. Our focus study and removes the drawback of EAACK scheme such as partial dropping problem which does not completely removed by the EAACK system. Table1. Shows the comparative study of Various Misbehaving Techniques with black hole.

M.Umaparvathi et.al in [20] uses AODV to detect single node acting as a black hole. Group of nodes collectively &co-operatively detect black hole attack. Proposed system works on two-tier. Tier 1 detects single black hole node using verification message. Whereas tier 2 detect group of nodes creating black hole attack using number of Control messages and number of data packets.

Murugan et.al [21] has proposed cluster based technique to detect misbehavior nodes called black hole node, using cluster based technique and threshold cryptography. The proposed scheme has used Proactive Secret sharing technique to share secret key among nodes which is deployed along with threshold cryptography to provide more security.

In summary, the architecture proposed in this paper different from existing researchers on intrusion detection for MANETs; the main focus of the architecture to find the attacks on MANET using the hierarchical cluster based topology [13].

Table 1.Comparitive study of Various Misbehaving Techniques

Technique	Malicious Routing	Routing Overhead	False Misbehaver our Detection	Packet Delivery Ratio	Detection & Prevention of Forged acknowled gement	Black Hole attack Detection & Removal
Watchdog[6]	No	Low	No	Low	No	Yes
Cooperative[16]	Yes	Large	No	Medium	No	Yes
2ACK[17]	Yes	Lesser than TWOACK	No	Large	No	Yes
TWOACK[18]	Yes	Large	No	Medium	No	No
AACK[19]	Yes	Lesser than above technique	No	Large	No	No
EAACK[7]	Yes	Same as AACK	Yes	Large	Yes	Yes

3. PROPOSED SYSTEM

The project implementation starts with the creation of topology and then a routing protocol is used AODV [9] or DSR [10] according to the requirements. Among the nodes in the topology any of the two nodes are selected as the source node and destination node pairs. The source and destination nodes then exchange the simple Digital Signature according to the RSA [22] and DSA [23] algorithms.

3.1 Block Diagram of System

The schemes of EAACK [7] are Acknowledgment, Secure-ACK and MRA (Misbehavior Report Authentication) are described below. In Fig.1 Working Block Diagram represents the flow of the proposed system. Each module in block diagram described below as.

3.2 ACK (Acknowledgement)[7]

ACK is an end - to - end acknowledgment EAACK [7] scheme. Goal is to reduce network overhead when no network misbehavior is detected. If source node send packet through intermediate nodes to destination, within predefined threshold say 20 second source node has to get ACK from destination node. Source node does not receive ACK packet from destination node within defined threshold, then resend packets count ¡=5 to check whether there is link broken between the nodes or if any node has limited transmission power, if this condition is satisfy go to check packet mode and if not then send Secure Acknowledgement(S–ACK) packets. Source node switch to S–ACK mode and send out S-ACK data packet to detect misbehaving node in the route.Fig.2 a) shows the working of ACK mode. The packet format of Data packet (PAD) and Acknowledgment packet (PAK) is as elaborated in Table 2.

3.3 Secure Acknowledgement(S-ACK)[7]

S-ACK scheme works in groups, of three consecutive nodes to detect malicious nodes in network. Third consecutive nodes in the route, need to send S-ACK to the first node in group. Flow of SACK mode is shown in Fig 2.b).The purpose of introducing S–ACK Mode is to find misbehaving nodes in the presence of receiver collision or limited transmission power. If first node in group of three nodes does not receives acknowledgment packets within predefined threshold say 20 seconds, then second and third node in group reported as misbehaving or malicious. This misbehavior report is send to the source node. If the acknowledgment packets within predefined threshold say 20 second then no needs to switch to MRA mode. Otherwise Source node has to verify the report by switching to MRA mode. S–ACK packet format of PSAD and PSAK is as shown in Table 3. PSAD data packet and PSAK is acknowledgement packets.

Table2.Packet format of PAD and PAK Packets

Packet	Packet Format								
PAD	SouNode	DesNode	Packet type	Packet ID	Hop Count	PAD packet route	Reply PAK packet Route		
PAK	SouNode	DesNode	Packet type	Packet ID	Hop Count	Previous Hop count	PAK packet Route	PAK Sender	PAK Signature

Table 3. Packet format of PSAD and PSAK Packets

Packet	Packet Format							
PSAD	SouNode	DesNode	Packet type	Packet ID	Hop Count	PSAD packet route	Reply PSAK route	Reply MRA Route
PSAK	SouNode	DesNode	Packet type	Packet ID	Hop Count	PSAK Destination	Previous Hop Name	PSAK packet Route

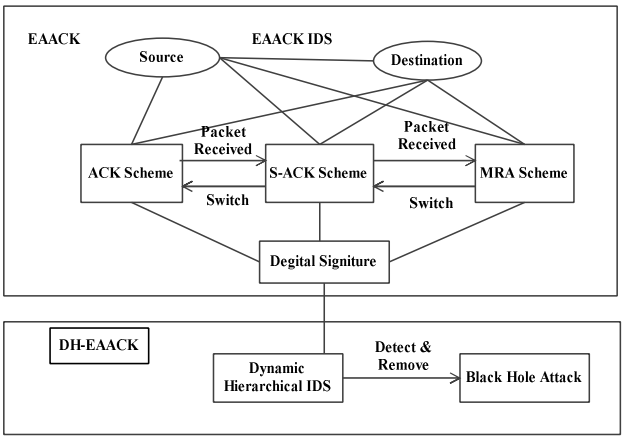

Figure 1.Working Block Diagram of System

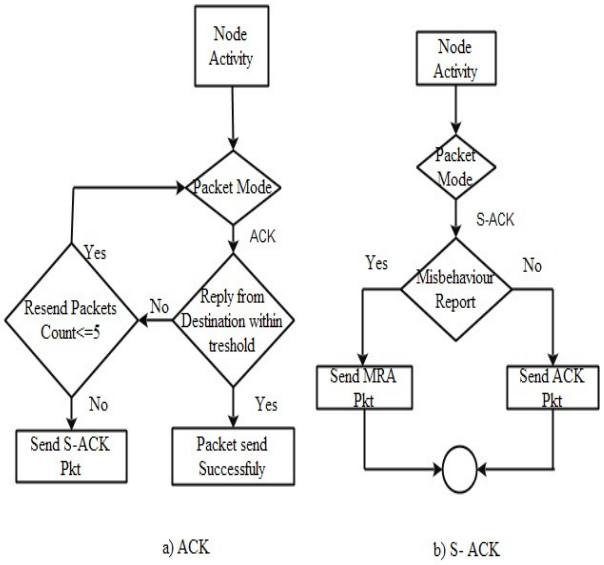

Figure 2.Flowchart of ACK and S-ACK Mode

3.3 Misbehavior Report Authentication (MRA)[7]

This scheme designed to detect malicious nodes or attackers in the presence of false misbehavior report. This report generated by an attackers to report innocent nodes as misbehaving node. And there has possibility of MRA report dropped by Intermediate node, and MRA report does not reach to the source node within time period 60 seconds then source node starts DACK verification routine to find black hole attack. MRA report message format is as described in Table 4.

Table 4. Packet format of MRA Mode

Packet	Packet Format									
MRA	SouNode	DesNode	Packet type	Packet ID	Hop Count	MRA Packet Source	MRA Packet Verification ID	MRA Packet Report	Previous Hop Name	MRA Packet Route

3.4 Dynamic Intrusion Detection Hierarchy [14]

In cluster based IDS nodes are prearranged in a hierarchy with the top level nodes as Cluster Heads. Being cluster based as shown in Fig.3 improves the efficiency of IDS in terms of memory usage and network overhead. Each node incorporated with acknowledgment based IDS. Proposed architecture works on Dynamic Hierarchical based IDS [14] in which nodes are divided in clusters. Node with maximum 1 hop count is chosen as Cluster Head (CH). AODV [9] routing protocol has modified using cluster based technique to detect hijacked node causing black hole attack inside network. 5. Black hole attack detection Reactive routing protocols are on-demand routing [25] and dynamic in nature e.g AODV [9] and DSR [10]. Fig.4 Explain the example of black hole attack using AODV routing protocol. Source node 1 broadcasts an RREQ (Route Request) message to discover a route for sending packets to

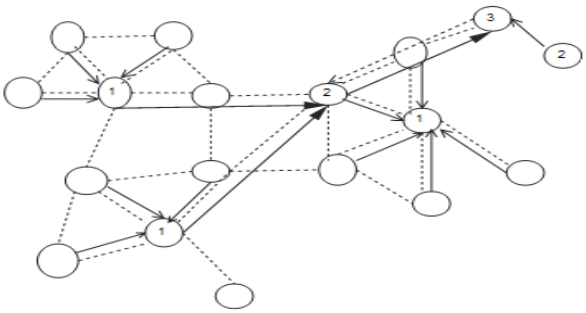

Figure 3.Dynamic Intrusion Detection Hierarchy [13]

destination node 5. An RREQ broadcast from node 1 is received by neighboring nodes 2, 3 and 4. However, malicious node 3 sends an RREP (Route Reply) message immediately without even having a route to destination node 5. Node 3 drops all packets and work as black hole. Table 5. Shows the packet format of RREQ and RREP route discovery. In proposed method all the nodes receiving data packet send acknowledgement to the node from which it received it. If source node receives acknowledgement from destination within threshold time, path is found to be secure against black hole node and originator takes no action.

Otherwise source starts verifying nodes. Source node starts DACK verification routine to detect black hole attack in the network. Table 6. shows the DACK verification routine packet format. If source node does not received MRA report generated by intermediate node within predefined time period then source node unicast verification message (VREQ) to all the nodes whose details it has stored by considering the node as destination node.

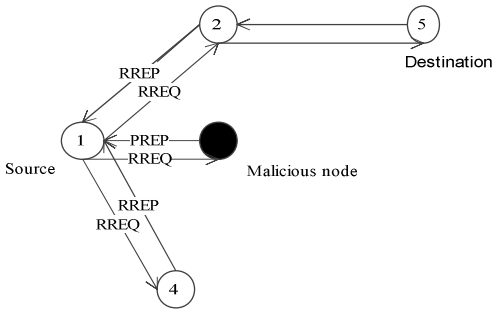

Figure 4.Black Hole Attack [15]

Table 5: Packet format of RREQ and RREP

Packet	Packet format					
RREQ	Source	Destination	Packet type	Hop count	Discovered Routes	
RREP	Source	Destination	Packet type	Hop Count	Discovered Routes	Reply packet Route

Through verification message Source asks the corresponding nodes to reply corresponding packet has been received or not in the form of verification reply (VREP).Assume that hijacked node would always intend to hide itself. If IMn has received acknowledgement from its next node it replies otherwise the node act as black hole node does not identify the message contained in VREQ packet. Source creates VREP map and compare that VREP map with discovered route if node acting as black is present in selected route but does not present in VREP map, that node is act as black hole node in the network. Node acting as black hole can be removed manually by deleting the node in the discovered route. Alert to other nodes in the cluster to does not send packet through this node, node is discarded from network.

Table 6: Packet Format DACK Routines

Packet	Packet Format							
DACK	SouNode	DesNode	Packet type	Packet ID	Hop Count	Previous Hop Name	DACK Packet Route	
VREQ	SouNode	DesNode	Packet type	Packet ID	Hop Count	Previous Hop Name	VREQ Packet Route	Reply VREP Packet Route
VREP	SouNode	DesNode	Packet type	Packet ID	Hop Count	Previous Hop Name	VREP Packet Sender	VREP Packet Route

3.5 Digital Signature

In EAACK, it is important that all the coming acknowledgment packets are authentic and pure. If the attackers made the forge acknowledgment packets then all the above three mode are weak. For this concern digital signature incorporated in proposed scheme. EAACK [7] needs all acknowledgment packets are digitally signed before they are sends out and get verified till they are accepted. Here by using two digital signature algorithms called as RSA [22] and DSA [23] identity-based cryptography [24] acknowledgment packets are encrypted and decrypted. Public key is used to encrypt the ACK packets and to verify the signature. Private key is used for decryption and to sign the ACK packets.

4. ALGORITHEMIC STARTEGY

The algorithm mentioned below implements cluster based technique to detect malicious node i.e. node causing black hole attack in network. Routing protocol used to test the functionality and to evaluate the performance of proposed system is AODV [9]. The algorithm is implemented in two phase; route discovery phase of AODV [9] and data packet sending phase.

Input = Source IP; Destination IP; Data packet
Output = Attacker node
Terms used: DACK–Dynamic Acknowledgment
RREQ–Request for Route
RREP–Request for Reply
VREQ–Verification Request
VREP–Verification Reply

As described in flowchart in Fig.5 and Fig.6 algorithm of black hole attack detection works in two phases as first phase Route Discovery phase and second Data Packet Sending phase.

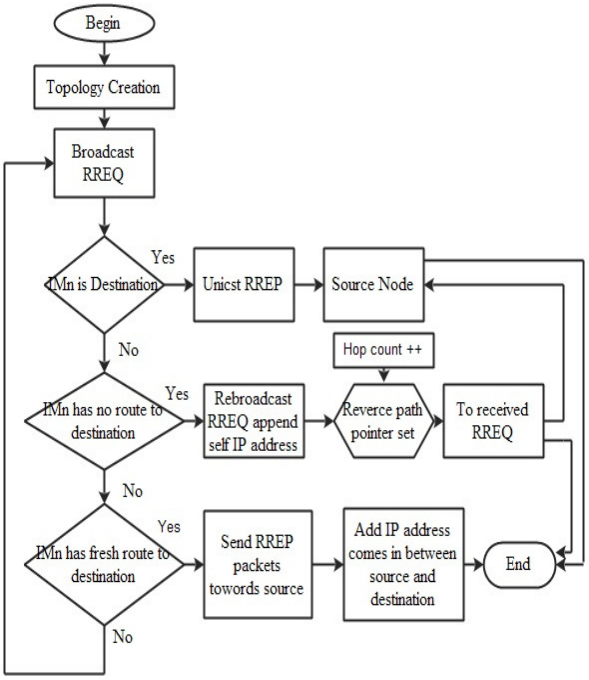

Figure 5: Flowchart Route discovery phase

5. COMPARATIVE RESULTS

Result analysis of proposed Dynamic Hierarchical IDS (DH–EAACK) system to detect routing protocol attack called black hole attack compared with existing systems such as Watchdog[6], EAACK[7]. System developed compared with black hole attack and without black hole attack.

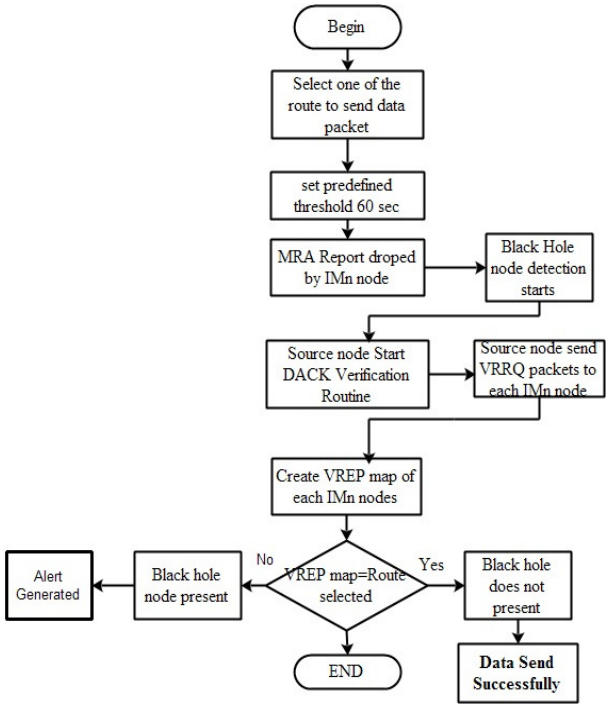

Figure 6: Flowchart Data Packet Sending phase

5.1 Packet Delivery Ratio

PDR is shown with DH–EAACK without black hole by comparing results of existing system in Fig 7. PDR of the proposed system is increased when malicious node are 10% of DH-EAACK system performance observed 1.3% better than EAACK, Watchdog.

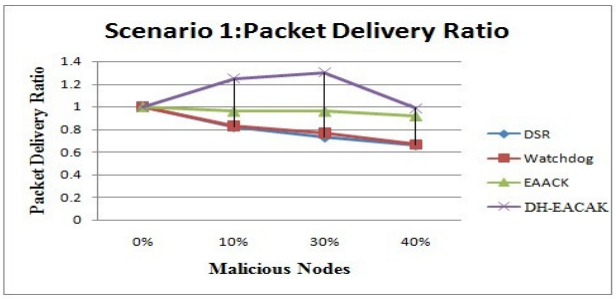

Figure 7: Results for Packet Delivery Ratio

5.2 Routing Overhead

Routing overhead of EAACK and DH-EAACK maintains more network overhead than DSR and Watchdog schemes when malicious nodes are 40% the proposed system DH-EAACK has 1% of routing overhead due to more acknowledgment packets are send out over the network as shown in Fig 8. Due to black hole node detection in the network more number packets are send out and received.

5.3 Throughput

Fig9.shows DH–EAACK without black hole out performs better than DH-EAACK with Blackhole attack. In case of DH-EAACK with black hole attack there is no increase in throughput due to malicious nodes. DH-EAACK without black hole has better throughput than DH-EAACK with black hole. Fig 9.describes that when there are node mobility of 30% throughput 100% of DH-EAACK than DH-EAACK with black hole attack.

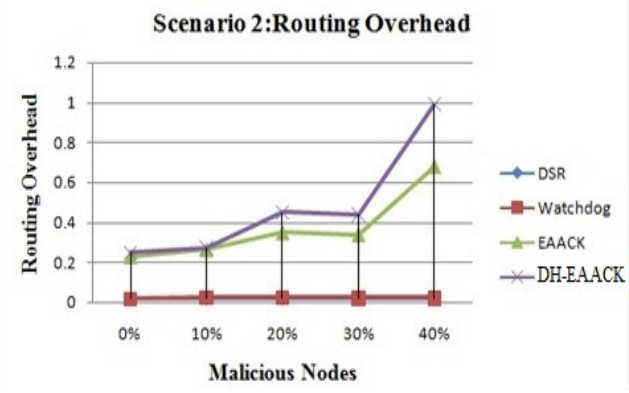

Figure 8: Results for Routing Overhead

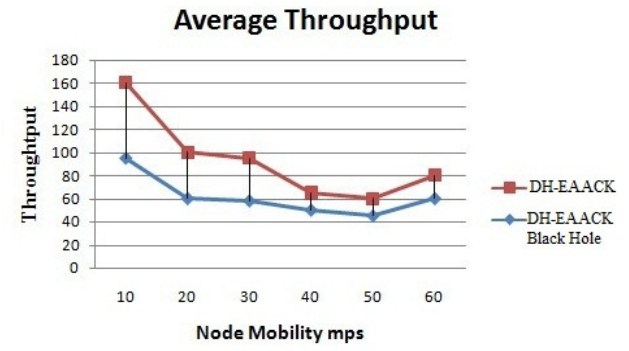

Figure 9. Result for Average Throughput

5.4 End to End delay

When number malicious nodes are high there is a significant increase in average End to End Delay. Fig 10 shows comparison results of DH–EAACK and DH–EAACK with black hole then DH–EAACK has more delay in processing of all acknowledgment and other packets. When there are 30% of malicious nodes in the network the delay is more of DH-EAACK with black hole which is 11000(ms).

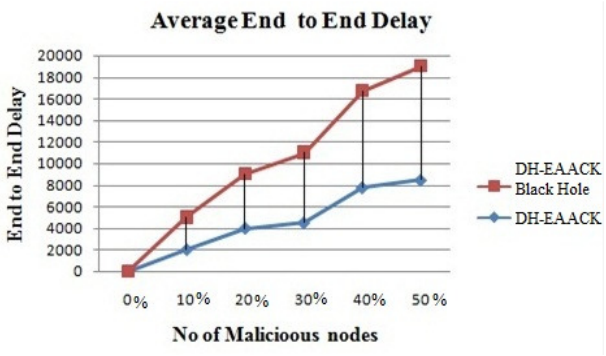

Figure 10: Result for Average End to End Delay

5.5 Jitter

When Quality of service is required jitter one of important metric measure. DH–EAACK with black hole jitter varies and jitter is more as compared DH–EAACK without black hole as shown in Fig 11. Jitter increases when there is no malicious nodes are present in route. When there is increase number of malicious node from 30 to 40 % there is a considerable increase in jitter as compared to DH-EAACK with DH-EAACK with black hole malicious node.

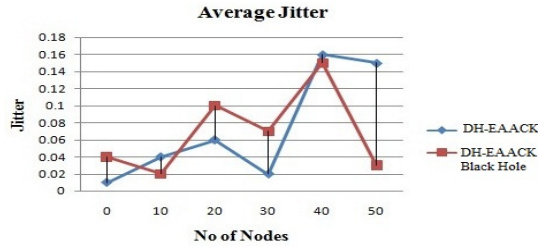

Figure 11: Result for Jitter

6. CONCLUSIONS AND FUTURE WORK

In this paper, we have designed and developed the cluster based EAACK architecture to detect and remove black hole attack in MANET. Clusters are formed in the network and cluster heads (CH) are selected manually for experimental result. The digital signature has incorporated into the data packet as well as the acknowledgement packet by using RSA and DSA algorithm. The AODV routing protocol used to test the functionality and to evaluate the performance. Following are the conclusions are drawn based on the result obtained. Due to use of cluster based architecture Packet Delivery Ratio and Throughput has been increased. As RSA and DSA based digital signature are incorporated with each acknowledgment packets, hence it provides better security. Due to transmission overhead of packets in cluster based system Routing Overhead and Jitter increased. As per the security concern, it can improve by using hybrid cryptographic techniques such as use of AES and MD5 techniques. By using the cluster head election algorithms cluster heads will be elected.

7. REFERENCES

[1] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. Instrumentation*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[2] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, pp. 1154–1159, Jun. 24–28, 2007.

[3] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc.ACM Workshop Wireless Secure* , 2002, pp. 1–10.

[4] *Jayakumar and G. Gopinath, Ad hoc mobile wireless networks routing protocolA review,J. Comput. Sci., vol. 3, no. 8, pp 574582, 2007.*

[5] S. Sreepathi, V. Venigalla, and A. Lal, *A Survey Paper on Security Issues Pertaining to Ad-Hoc Networks*. www4.ncsu.edu/ sssreepa/Adhoc-networks-Security-Survey.doc.

[6] 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 , August 2000.

[7] Elhadi M. Shakshuki, Nan Kang,et.al EAACK ASecure Intrusion Detection System for MANETS IEEE Transaction on Industrial Electronics, vol. 60, no. 3, Mar 2013.

[8] BhavyeshDivecha, Ajith Abrahame,et.al "Analysis of Dynamic Source Routing and Destination Sequenced Distance-Vector Protocols for Different Mobility models", *First Asia International Conference on Modeling and Simulation*, AMS2007. March, 27-30, 2007, Phuket, Thailand. Publisher: IEEE Press, pp. 224-229.

[9] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999, pp. 90–100.

[10] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[11] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black hole problem in mobile ad-hoc network," *5th World Wireless Congress*, pp. 508–512, 2004.

[12] M.-C. Basile, M.-Z. Kalbarczyk, and F.-R. K. Iyer, "Inner-circle consistency for wireless ad-hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 39–55, 2007.

[13] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2, pp. 825–830, 21-25 March 2004.

[14] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, and T. Bowen, "A general cooperative intrusion detection architecture for manets," in *Proceedings of the Third IEEE International Workshop on Information Assurance*, March 2005, pp. 57–70.

[15] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[16] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proc. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003, pp. 135-147.

[17] Bansal and Baker, Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs ",IEEE transactions on Mobile Computing ,P448-502, vol. 6, NO. 5, May 2007.

[18] Balakrishnan, K.; Jing Deng; Varshney, V.K., 2005 "TWOACK: preventing selfishness in mobile ad hoc networks", In Proceedings of Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp.2137-2142(March 2005).

[19] T.Sheltami, Al-Roubaiey, E.Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[20] M.Umaparvathi, Dharmishtan K.Varughese,"Two Tier Secure AODV against Black Hole Attack in MANETs" European Journal ofScientific Research, ISSN 1450-216X Vol.72 No.3(2012),pp,369-382.

[21] R. Murugan, A. Shanmugam "Cluster Based Node Misbehavior Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks" International Journal of Computer Science and Security ISSN1985-1553 volume :6;Issue:3;Start page:188;Date:2012.

[22] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[23] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[24] J. Chen and J. Wu. A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks. In Wireless/Mobile Network Security. Springer,2008.

[25] M. Abolhasan, T. Wysocki, and E. Dutkiewicz. "A review of routing protocols for mobile ad hoc networks. Ad hoc networks, "2(1):122, 2004.