Secure Congregate based Intrusion Detection System in Infrastructure Less Network

Sarika Patil
Assistant Professor, Department of Computer Engineering, Pune, India

***Abstract*: Security is an important concern in mobile ad-hoc network environment caused by nature of dynamic topology. In Mobile Ad-hoc Network multiple nodes moves from one position to another position in same transmission range due mobility. In this paper we have described design and implementation of dynamic cluster based Intrusion detection systems to select the leader nodes or cluster head dynamically based on resource capability and power backup. If a selected leader node suddenly moves out of range another leader node elected on the basis of above resource constraints. MANET is more vulnerable to attacks compared to other network and also different attacks are restricted to the network operations. Advanced Encryption Standard and message authentication code based message digest 6 (MAC-MD6) algorithms for secure transmission of data over the MANET with AODV routing protocol. This proposed model will provide better performance in terms of Throughput, packet delivery ratio (PDR) and minimizes routing overhead as well as effective bandwidth utilization.**

***Keywords*: Ad-hoc on demands Distance Vector, Election Algorithm, Intrusion Detection System, Message Digest 6, Mobile Ad-hoc Network.**

1. Introduction

Mobile Ad-hoc network (MANET) is an emerging as well as most popular technology in wireless network provides transferring a data within transmission range. MANET provides mobility over wireless network environment and also supports scalability as well as flexibility. It also known as an infrastructure less network and it has no centralized monitoring and controlling systems [1]. This network is more vulnerable to attacks due to mobility because it does not have secure data transmission over the communication medium and result number of malicious nodes is manipulate the network operations. There are two types of attacks in wireless networks such as Active attack and Passive attack. An Intrusion is an unauthorized attempt to access or manipulate information of a system. The solution is to detect the intrusion with help of intrusion detection systems. A process of monitoring the events which is occurred in computer system or network and analyzes them for possible incident which violates the security policies is known as IDS. It uses the clustering techniques to form the cluster of nodes and then select the cluster head on the basis of battery power. To tackle the different attacks in mobile ad hoc network by using dynamic cluster based techniques and Ad-hoc on demand distance vector routing protocol by using hybrid cryptography techniques such as Advanced Encryption Standard and Message Authentication code message digest 6 (MAC-MD6) algorithms. The rest of the paper is organized as follows Section II focuses on the Background study, Section III presents Literature survey, section IV presents Motivation, Section V describes Design of the system and proposed algorithm and finally section VI Conclusion.

2. Background study

A. *Mobile Ad-hoc network*

MANET is a collection of multiple nodes or mobile nodes which is move from one location to another location and communicates with each other in the absence of central administration. It is responsible for creation, operation and maintenance of the wireless network. A one nodes help to other intermediate nodes to establish communication channel and these communications achieved by using multi hop wireless links [1]. During data transmission i.e. transmit a packets from one mobile nodes to another mobile nodes to another mobile nodes in the networks dynamically sets up the paths. In the network each and every node maintains the routing information in the routing table for forwarding a data it includes IP addresses of the nodes, next hop, etc. and same time nodes acts as a host or router moves randomly in a network without reporting to any nodes. MANET is used in an industrial application such as Industrial remote access and controls the operations using wireless network. It is an open medium, supports mobility and dynamic topology this features provides the network which is more vulnerable to security threats.

B. *Security Issues in Mobile Ad-hoc Network*

The MANET is a dynamic network due to this feature, makes more vulnerable for attack during data communication. Security issues arise in MANET as follows.

- *Confidentiality:* It is a guarantee that confidential information is not available to unauthorized entity.
- Integrity: It is a guarantee that information and programs are changed only in a specified and authorized manner.
- *Availability:* A loss of availability is the interference of access to or use of evidence or an information system.

- *Authorization:* The security goal that makes the prerequisite for actions of an entity to be copied uniquely to that entity [2].

C. *Attacks in mobile ad-hoc network*

The different types of attacks are occurred during data transmission in wireless network. Attackers capture the entire session and manipulate the network operations. The mobile Ad-hoc network has two types of attacks such as passive attack and active attack as shown in Fig 1. Passive Attack is difficult to detect as it tries to read or listen network traffic or eavesdropping of data packet in the network. An active attack is attempted to perform various action in the systems or network such as modification, repetition and removal of exchanged data over the network [3]. Due to this, network suffers with congestion and restricts the operation which decreases the performance in terms of throughput.

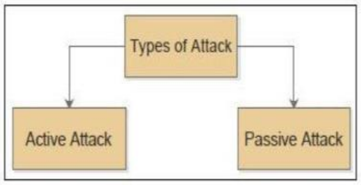


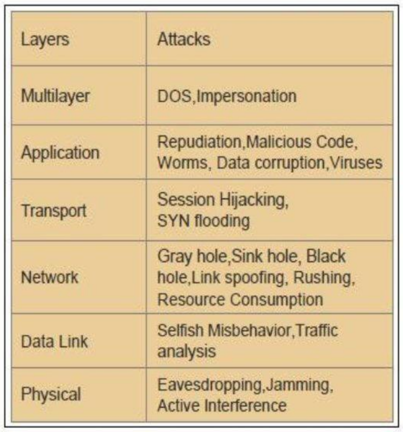
Fig. 1. Different types of attacks in MANET

Gray hole is a network layer attack which drops the content of the packet during data transmission. It also known as data traffic attacks because node that selectively drops and forwards data packets after it announces itself as having the shortest path to the end point node in response to a route request message from a source node [4]. The solution to this problem is to use intrusion detection systems (IDS).

D. *Intrusion detection systems*

Intrusion Detection System is a device or software applications that monitors the events which is occurred in computer systems or network and examines them for possible events which violates the computer security rules, acceptable use rules and standard security practices. An intrusion is set of action that tries to compromise the confidentiality, integrity and availability of the resources. In other word it is a deliberate unauthorized attempt to access or manipulate information or systems [2]. Management console and sensors are the components of intrusion detection systems. In management console, it can be performed management task and report it to console. Sensors are an agent that monitors host or networks on real time base. Sensors detect malicious activity within network and report to management console. There are two types Intrusion Detection System such as Host based IDS and Network based IDS. HIDS monitor only system level activities such as audit and events logs. It responds after suspicious log entry into systems and IDS uses Operating systems in its analysis. NIDS Captures and examines packets from network traffic and these IDS apply predefined attacks signs to each frame to recognize hostile traffic. NIDS better for detecting attacks from outside as well as inside attacks which is Miss HIDS. IDS have different architectures such as Stand-alone, Distributed and cooperative, hierarchical and mobile agents.

Table 1
Different types attacks in layers



Layers	Attacks
Multilayer	DOS,Impersonation
Application	Repudiation,Malicious Code, Worms, Data corruption,Viruses
Transport	Session Hijacking, SYN flooding
Network	Gray hole,Sink hole, Black hole,Link spoofing, Rushing, Resource Consumption
Data Link	Selfish Misbehavior,Traffic analysis
Physical	Eavesdropping,Jamming, Active Interference

It also uses detection techniques such as anomaly, signature and specification base detection. Cluster based IDS techniques are used to detect misbehavior nodes in the network [2]. Evaluation of IDS by using accuracy in terms of detection rate and false alarms and these categorized into three types such as Signature based IDS, Anomaly based IDS and Specification based IDS.

E. *Hierarchical intrusion detection systems*

Hierarchical IDS provides the information guarantee through real time sharing technology in distributed, scalable and coordinated environment. This architecture is efficient during large network because we divide the network into cluster i.e. a group of nodes which is connected with each other within same transmission range. Due to hierarchical cluster based IDS improve the efficiency in terms network overhead and memory usage. Hierarchical IDS every node in the MANET must contribute in the intrusion discovery and response by having an IDS agent running on them by using multilayered network infrastructure where network is dividing into cluster. In clustering a nodes is organizes into group of clusters and due to cluster improve the efficiency in terms of network overhead and also minimizes the updating overhead during topology change [5]. Selection of cluster heads based on election algorithm which is nodes with highest connectivity, power backup or bandwidth capabilities.

F. *Cluster formation*

Select one node as initiator which is send broadcasts message to neighboring nodes for make a cluster. A message includes information about the Battery power, neighbor nodes list, IP addresses of all nodes, bandwidth, and transmission range. After obtaining the information from different nodes, initiator arranges the all nodes in descending order of their battery values. Initiator select the cluster head with respect to their battery power and sends information's to the cluster heads.

For selection of cluster heads, it uses self-stabilizing leader election algorithm for frequently changing network. It uses the time interval for checking the battery power continuously. Cluster based topology has been described in Fig. 2.

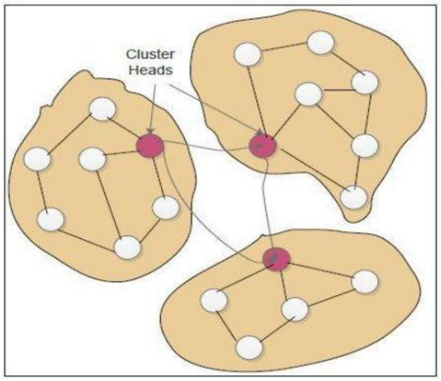


Fig. 2. Cluster formation and selection of heads

In cluster based structure, topology updating information can be efficiently exchanging with various nodes. This concept restricts the traffic updating and control messages which are periodically leads to efficiently bandwidth utilization in MANET. In clustering technique which has two mechanism such cluster formation and cluster maintenance. Cluster head responsible for managing the cluster process, updating routing table and discovering of new routes [5].

G. Cryptographic techniques

MD6 is a Message authentication code base message digest 6 (MAC-MD6) algorithms is used to secure the AODV packets. It calculates the message digest by using MD6 hash function for AODV packets and then transmits the packet over network. It provides robust security to the wireless network during transmitting data packets to the network and used to both encryption and decryption. AES is a symmetric key algorithm which is a same key is used for both encrypting and decrypting the data. AES process the 128-bit data blocks and uses the key length of 128, 192 or 256 bits. AES provides the security against all known attacks in the network. In AES cipher key size is specifies the number of repetition of transformation of rounds convert the input called Plaintext into output called cipher text. Each round consists of some processing step containing five different stages.

H. Routing protocol

In mobile Ad-hoc network different types of routing protocol is used to find the route from source to destinations in the network. It has different types of routing protocols in the mobile Ad-hoc networks such as a proactive, reactive and hybrid routing protocols. Ad-hoc on demand distance vector (AODV) is a reactive routing protocol is used to discover the paths or routes only when you need it. The function of this protocol is to saves the energy and bandwidth during inactivity. It uses two messages for secure routing such as routing messages and data messages and also it has two phases which is route discovery process as well as maintenance process [2]. Fig. 3 shows types of routing protocols in MANETs.

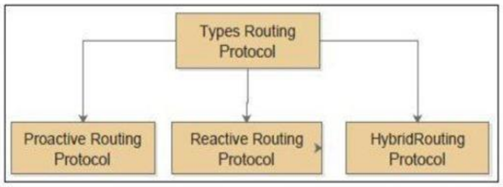


Fig. 3. Different types routing protocol in MANET

3. Literature survey

Sarika patil et.al. [2] Proposed by the architecture base on EAACK Systems, to detect and remove the packet dropping algorithm such as black hole attack. In their work used cluster based topology to organizing the group of nodes in MANET and it also uses detection techniques such as watchdog and EAACK to find the attacks.

Huang and Lee [6] Proposed by the cluster based cooperative Intrusion detection system to detect different types of attacks in the mobile Ad-hoc network and apply some rules i.e. anomaly detection for identifying attacks and randomly elect a monitoring node i.e. the cluster head for the entire neighborhood. The drawback of this system is if system does not implement dynamic clustering for the selection of heads.

BaharehPahlevanzadehet.al. [7] Proposed the distributed hierarchical based an Intrusion detection systems based on NIDS and HIDS over Ad hoc on demand routing protocol. It provides an efficient technique to detect an attack in mobile ad-hoc network. The model is based on CPU usage, accuracy and detection rate and design methodology is to distribute hierarchical IDS for attacks occurred in the network.

B. Pahlevanzadeh et.al. [8] Proposed the model based on cluster based distributed hierarchical IDS its divides the nodes into number of overlapping or disjoint 2 hop diameter clusters in distributed fashion and due to clustering Techniques to minimize the flooding traffic during route discovery. The cluster based routing protocol (CBRP) using mobile agents to enhance the security in MANET and it did not increases the communication message overhead due to energy consumption by using CBRP for managing communication message. The accuracy of finding malicious nodes is less due to CBRP protocol.

S. Marti et. al. [9] Proposed by Watchdog and Pathrater, the detection model for identifies the misbehaving nodes and it helps routing protocols to avoid these nodes. With this technique it increases the throughput of a network in the existence of malicious nodes. The disadvantage was it could not detect misbehaving nodes in the presence of Limited transmission power, Partial dropping, Ambiguous collisions, and false misbehavior and Receiver collisions. Watchdog detection techniques depends on Dynamic source routing protocol and each nodes detect an intrusion on route from source to destination with make sure that retransmitted packet without alternation.

To overcome the effects of misbehaving nodes Pathrater techniques select the route from source to destination based on the rating algorithms as compared to shortest path. Pathrater is run by each and every nodes present in the network. The drawbacks of pathrater techniques is too fixed binary states new node anonymity, reentrance of formerly nodes.

Elhadi Shashuki et. al. [10] Proposed by the EAACK scheme malicious nodes are detected by using Enhanced adaptive acknowledgment method. In this method during data transmission, data is secured by using Digital signature algorithms and these algorithm results more overheads due to collision of packets and distribution of the keys between different nodes in the network. Problems are that due to use of this method key exchange and use of hybrid cryptography are responsible for overhead.

Chin Yang et. al. [11] Proposed a specification based an intrusion detection system for AODV protocol it analyzes the vulnerability, attacks against AODV protocol that manipulate the routing message. It uses the finite state machines for requiring it to correct AODV routing behavior and distributed network monitors for detecting run time destruction of specification.

2ACK [12] proposed the scheme to detecting misbehaving links rather than misbehaving nodes. In this packet has been assigned route of two hops which is in opposite direction and drawbacks is higher routing overhead due to transmission of 2ACK to the source nodes.

S. Talapatra et. al. [13] Proposed algorithm for cluster head selection and cluster maintenance and this algorithm use self-organizing principle for binding a node with cluster which can reduce the explicit message passing in cluster maintenance. The Drawback of this system is to it does not elect the cluster head dynamically and requires more messages during transferring data.

Minakshi et.al. [14] Proposed a Modified HMAC-MD6 algorithm for securing the AODV protocol and increasing resistance to key search attacks and providing authentication as well as integrity. It uses the power of HMAC by making this non vulnerable in the wireless environment to provide security. This algorithm on two types of networks one purely cluster-based and other having General MANET structure with random clustering to secure data for reliable transmission over network.

4. Motivation

As per explained in section I and II the issues concerned with the MANET are security, mobility, open medium, dynamic changing topology, lack central monitoring and administration. These factors are responsible for suffering attacks in mobile Ad-hoc network. An availability of network services, confidentiality and integrity of data can be achieved by using routing protocols. With this vulnerability an intrusion detection system provides solutions is to detect and prevents against various types of attacks in different layers. With the help of routing protocol and using MD6 algorithms to improve the security provides high efficiency of securing the data over the Wireless Network.

5. Design

In dynamic cluster based architecture an IDS to detect attacks in the mobile ad-hoc network by using routing protocol which is responsible for creation, operations and maintenance of the networks. The Fig. 4 shows the Block diagram of dynamic cluster based Intrusion detection system.

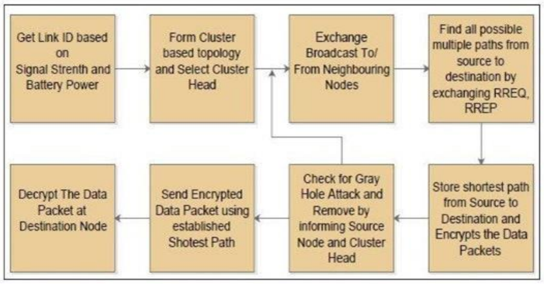

Get Link ID based on Signal Strenth and Battery Power
Form Cluster based topology and Select Cluster Head
Exchange Broadcast To/ From Neighbouring Nodes
Find all possible multiple paths from source to destination by exchanging RREQ, RREP
Store shortest path from Source to Destination and Encrypts the Data Packets
Check for Gray Hole Attack and Remove by informing Source Node and Cluster Head
Send Encrypted Data Packet using established Shotest Path
Decrypt The Data Packet at Destination Node

Fig. 4. Working block diagram of system

Cluster based IDS means to organize as a group of cluster due to this technique the network performance increases. In this, one node acts as initiator which broadcast the message to all nodes for make cluster head based on the Signal strength i.e. transmission range, battery power, computational capacity. Initiator maintains the table for information about different values and after receiving the message from all nodes organizes the nodes with respect to battery power and transmission range in descending order and finally elect the cluster head. If selected leader nodes suddenly move out of range at the same time another node elect as leader nodes on the basis of above resource constraints. A leader node keeps all information related to all nodes which is in cluster and maintains the routing information for route of the entire network. After that form a topology and select a source and destination nodes. Source nodes broadcast the message for route to transfer the data.

Table 2
Requirement and Specifications of Proposed System

Functional Requirement	Design Specification
Low Routing Overhead	Reactive Routing Protocol
Low End-to-End Delay, Jitter	Cluster based or Shortest Path
Reliable Routing	Based on signal strength
Throughput	Election Algorithm
Security	Using AES and MD6 algorithm

Table 2, shows the requirement specification and functional requirement of the specified problem.

A. *Election Algorithm*

Step-1: Select one of the nodes as initiator, which broadcasts a message to make a cluster. The information included the

Table 1
Table title comes here

Proposed System	By	Attacks	Protocol	Parameters
Cluster Based Distributed Hierarchical IDS	B. Pahlevanzadeh, S.A. Hosseini Seno, et.al.[8]	Flooding traffic	Cluster based routing protocol	Bandwidth utilization and energy consumption
Cluster Based Cooperative IDS	Huang and Lee [6]	Dos, black hole, Routing loop, Sleep deprivation	Timed Efficient Stream Loss Tolerant Authentication protocol	Network overhead, CPU speed up, Accuracy
Watchdog and Pathrater	S. Marti, T. J. Giuli, et.al.[9]	Misbehaving Nodes	Dynamic Source routing	Throughput, Overhead, PDR
Distributed Hierarchical Based IDS	BaharehPahlevanzadehet.al.[7]	Denial of service	Ad-hoc on demand distance vector	Accuracy, Detection rate and CPU usage.
DH-EAACK	SarikaPatil et.al.[2]	Black hole	Ad-hoc on demand distance vector	End-to-End delay, PDR, Jitter
EAACK	Elhadi M. Shakshuki et.al.[10]	Malicious Node	Ad-hoc on demand distance vector	Routing overhead, PDR, Delay

message is memory size, CPU power, neighbor nodes list with IP addresses and battery power.

Step-2: At starts of the algorithm every node is in the INITIAL state. Each node finds its neighbors node by broadcast HELLO packets and collects its neighbor information.

Step-3: All nodes enter into CLIQUE state and nodes which is presents in the network calculates the election parameter viz. computational power and battery power and finally send it to initiator nodes.

Step-4: After obtaining information from neighboring nodes, initiator node arranges all nodes in the table in a descending order of their energy value with respective IP address.

Step-5: The initiator node selects the cluster head with highest energy or battery power values. After selection, initiator sends the table of information it to the head node and also start timer to check battery power.

Step-6: The head node should broadcast the message which contains their IP addresses to all nodes in the cluster.

Step-7: It checks the battery power after 20 secs and exchanges the message to the initiator about power. If battery power < Threshold, then

Repeat the step 3 and 4 for selecting new cluster head. Step 8. If link fails or a leader node leaves the network then enters into LOST state and repeat the step 1 and 2.

During transmission of data in the network identifies the attack such as gray hole if detects attacks remove those nodes and inform to the source nodes and leader node. A transferring data packet encrypts the packet at source node and transmits over network by using AODV protocol to destination node and finally decrypts the data packets. After successful paths selection exchange the data between nodes by using MD6 algorithm will produced less routing overhead with the help of

During transmission of data in the network identifies the attack such as gray hole if detects attacks remove those nodes and inform to the source nodes and leader node. A transferring data packet encrypts the packet at source node and transmits over network by using AODV protocol to destination node and finally decrypts the data packets. After successful paths selection exchange the data between nodes by using MD6 algorithm will produced less routing overhead with the help of AODV protocol. Fig. 5 elaborates the security algorithm which has been used in the proposed model.

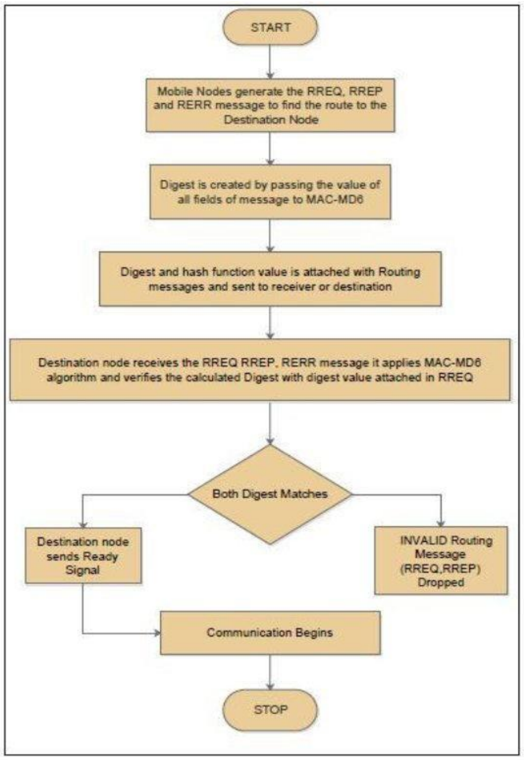

START
Mobile Nodes generate the RREQ, RREP and RERR message to find the route to the Destination Node
Digest is created by passing the value of all fields of message to MAC-MD6
Digest and hash function value is attached with Routing messages and sent to receiver or destination
Destination node receives the RREQ RREP, RERR message it applies MAC-MD6 algorithm and verifies the calculated Digest with digest value attached in RREQ
Both Digest Matches
Destination node sends Ready Signal
INVALID Routing Message (RREQ,RREP) Dropped
Communication Begins
STOP

Fig. 5. Flowchart of proposed mechanism for secure routing

6. Conclusion

Thus hereby we have introduced Dynamic cluster based IDS to detect gray hole attacks using Ad hoc on demand distance vector routing protocol. It will decrease network overhead and cluster head selection is also implemented by election algorithm which will work independently on the basis of computational capacity and power backup. Cluster based control structure provides more efficient use of resources for large networks. The network performance will be increased in terms of Packet Delivery Ratio (PDR) and throughput. The use of AES and MD6 algorithm will improve secure environment during data transmission in cluster based intrusion detection System.

References

[1] C. Logeshwari, S. Priyadarshini and C. Priyanka," A Survey on secure Intrusion Detection using routing protocol against malicious attacks in MANETs" in IJARCCE, vol. 2, pp. 4091-4094, Oct. 2013.

[2] Sarika Patil and deepali Borade "A Survey on IDS Techniques to Detect Misbehavior Nodes in mobile ad-hoc network" in International Journal of Computer Science and Information Technologies, Vol. 5 (3), pp. 2783-2787, 2014.

[3] Kirti Nahak and Babita Kubde "Security and Privacy issues in high level MANET protocol" International Journal of science and research, vol. 2, pp.1-7, Jan-2013.

[4] Rusha Nandy and Debudatta Barman Roy "Study of various attacks in MANET and Elaborative discussion of Rushing attack on DSR with clustering scheme" international Journal Advanced networking and Applications, vol-03, p.p. 1035-1043, 2011.

[5] Zeba Ishaq "Secure MANET using two head cluster in hierarchical Cooperative IDS" International journal of computer applications, vol. 3 pp.1-13, Nov-2012.

[6] Yian Huang and Wenke Lee "A Cooperative intrusion detection System for Ad Hoc Networks" Proceeding of the 1st ACM workshop on security of ad-hoc and sensor networks, p.p. 135-147, Oct- 2003.

[7] Bahareh Pahlevanzadeh and Azman Samsudin "Distributed Hierarchical IDS for MANET over AODV" in Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International conference on communications, pp. 99-104, May 2007.

[8] B. Pahlevanzadeh, S. A. Hosseini Seno, T. C. Wan, R. Budiarto, Mohammed M. Kadhum "Cluster-Based Distributed Hierarchical IDS forMANETs" in International Conference on Network Applications, Protocols and Services, pp. 1-7, Nov-2008.

[9] S. Marti, T. J. Giuli, M. Baker and K. Lai "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks" in Proceedings of the 6th Annual International Conference in ACM, pp.255-265, August 2000.

[10] Elhadi M. Shakshuki, Nan Kang "EAACK A Secure Intrusion Detection System for MANETS," IEEE Transaction on Industrial Electronics, vol. 60, no. 3, Mar 2013.

[11] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt "A specification based Intrusion Detection System for AODV" Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Oct. 2003.

[12] Mike Burmester, Breno de Medeiros "On the Security of Route Discovery in MANETs" IEEE transaction on mobile computing, p.p. 1- 9, 2011.

[13] Soumyabrata Talapatra and Alak Roy "Mobility based Cluster head selection algorithm for mobile ad-hoc Network" I.J. Computer Network and Information Security, p.p. 42-49, June 2014.

[14] Minakshi and Rakesh Gill "Secure AODV using HMAC-MD6 in MANET" IJCSMS International Journal of computer science and management Studies, Vol. 13, Issue 09, p.p. 16-23, Nov- 2013.

[15] Smita Bhoir, Amarsinh Vidhate "A Modified leader Election algorithm for MANET" International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 5, no. 02, Feb. 2013.

[16] Ismail Butun, Salvatore D. Morgera and Ravi Sankar, "Survey of intrusion detection System in wireless Sensor Networks," in IEEE Communications survey and tutorials, pp. 1-17, 2012.

[17] Yang, H Leo,H Y Ye, F Lu and Zhang " Security in mobile ad-hoc Network: challenges and solutions" IEEEwireless Communications, p.p. 38-47, Jan 2004.

[18] M. Anupama and Bachala Sathyanarayana "Survey of Cluster based Routing Protocol in Mobile Ad-hoc Network" International Journal of Computer Theory and Engineering, vol. 3, No. 6, December 2011.

[19] Lidong Zhou and Zygmunt J. Haas "Securing Ad-hoc Networks" in IEEE on network security, cornell university, pp.1-12,1999.

[20] Marjan K, Zahra Zahed A, Shahla Ghasemi "Methods of Preventing and Detecting Black/Gray hole Attacks on AODV-Based MANET" IJCA on Network security and cryptography, pp. 11-17, 2011.

[21] Jane Y. Yu and Peter H. J. Chong, "A Survey of clustering schemes for Mobile Ad-hoc Networks," IEEE communications surveys and tutorials, Volume 7, No.1, pp. 32-48, First Quarter, 2005.

[22] M. Zapata and N. Asokan, "Securing ad hoc routing protocols" in Proceeding ACM Workshop Wireless Security, pp. 1–10,2002.

[23] Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol: A review" Journal Computer Science, vol. 3, no. 8, pp 574- 582, 2007.

[24] S. Sreepathi, V. Venigalla, and A. Lal, "A Survey Paper on Security Issues Pertaining to Ad-Hoc Networks" international journal on advanced computing, vol. 3, pp.1-5, Nov. 2013.