Profile based Novel Approach for Jamming Attack Detection and Prevention in MANET

Aparna Raj
Department of Electronics and Communication Engineering,
Sagar Institute of Science and Technology, Bhopal

Pankaj Kumar Vyas
Professor
Department of Electronics and Communication Engineering,
Sagar Institute of Science and Technology, Bhopal

ABSTRACT
The current progression and communication in the corporate, military and industrial sectors. Nevertheless, these progressions have likewise brought new security vulnerabilities. The uses of the security methods of wired systems, for example, access control and confirmation/authentication have been unsuitable to wireless network because of the extraordinary features of such networks, for example, In dynamic evolving topology, no incorporated/centralized control and so forth. Subsequently, accomplishing security objectives for mobile ad hoc network (MANET) has increased critical consideration of the scholarly world and research community in recent years. In MANET security is the major issues in which jamming is one of them. In this attack a jamming node falsely advertise shortest path to destination node and drop all data packet in it. This paper, majorly highlight the behavior of Jamming attack and proposed flooding based defense schemes IDS against jamming attack in MANET. The performance of proposed IDS provides the normal routing performance and proving secure alternative path in MANET. The proposed scheme is simulated using NS-2 network simulator and analysis is performed using performance metrics such as routing overhead, PDR, packet analysis etc. The experimental results of the proposed scheme give improved result which means our proposed scheme is more effective to make the network secure and combat it from jamming attack.

Keywords
Security, Jamming attack, IDS, Routing, MANET, NS-2

1. INTRODUCTION
All The nodes in Mobile Ad hoc network continuously move in limited area and form link between them in dynamic environment. The MANET is self organizing network and nodes are capable of communication with one another without any fixed infrastructure. No centralized authority is present in network for watching the network activities. The wired network uses copper wire for communication, while ad-hoc networks use radio waves to transmit signals [1]. Two nodes will have multiple links between them for communication and deployed in an exceedingly complete fashion, appropriate for price and time effective setting, and for a scenario wherever infrastructure is troublesome to setup. Security is difficult in MANETs [2] attributable to its characteristics like peer to see design, operational while not central arranger, dynamic topology, insecure operational setting, and frequent link breakage attributable to mobile nodes, battery period of time, machine capability and non uniformity [3]. Communication in MANETs is through single hop in link layer protocols and multi hop in network layer protocols, supports the belief that each one of the nodes in an extensive network are cooperative in coordination, however sadly this statement isn't true in hostile setting. Malicious attacks [2] will simply disrupt network operation by violating protocol specifications. The network layer operations in MANET are bolstered through outing and knowledge packet forwarding each are vulnerable to noxious attacks. Mobile Ad hoc Networks are infrastructure less and utilize wireless link for communication which makes them unpleasantly vulnerable to an adversary's Mobile ad hoc networks. These are slanted to an outsized scope of security threats, the fundamental reality that pernicious attacks. Attackers are rigorous security threats in Ad hoc Networks which can be used without inconvenience by misusing weakness of on-request steering conventions like AODV. This tries to utilize Intrusion Detection (ID) to stop attacks made by each single and multiple nodes and hence the Detection and mending routing misbehavior below MANET. We attempt to reach up to the particular solution which expands network performance by the assistance of minimizing generation of control (routing) packets and also effectively restricting attacks against mobile ad hoc network [1].

1.1 Security Criteria
The mobile ad hoc network introduces various criteria which is considered to be secure.

1. Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [9].

2. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [22]:

- Malicious altering
- Accidental altering

3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it.

4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [9].

5. Non-repudiation

Non-repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message

6. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should be default and kept private and not be distributed by the node itself or the system software

2. ROUTING PROTOCOLS IN MANET

In dynamic network the topology regularly changes which are the cause of link splintering that are created as multiple-hop till the destination is not found. The routing protocol is playing an essential part at network layer for data accepting and forwarding through every router or node from which the data is originated by sender and accepted by receiver in that procedure routing approach it plays a very significant part of communication [4, 5]. For connecting to end and information delivery the routing protocol is necessary for routing the data in connecting sender to receiver every routing protocol has different routing approaches of link establishment however has same method of selecting shortest path in between sender and receiver. The shortest path is decided on the basis of least hop count importance in MANET. The classifications of routing protocols in MANET are as follow:-

2.1 Proactive Routing Protocol

The proactive routing protocols are also called as table driven routing protocol, In these protocols each and every other node maintains the routing information of every other node and these routing protocols collaborate in routing method. In Mobile ad hoc network, the topology of network changes by the transparency of maintain the information of each node is extremely complex and required immense arrangement of memory for storing routing information in the network. In ad hoc network if the nodes moves at slow speed then that protocol is assumed to be better for communication. The instance of proactive routing protocol is DSDV routing protocol.

2.2 Reactive Routing Protocol

The Reactive routing protocols are also called as on demand routing protocol and these routing protocols maintain the routing information on the basis of demand of request receives by the neighbor. There is no routing information stored of each node that collaborates in routing process. In Mobile ad hoc network the topology in network changes by that the overhead of maintain the information of each node is not desired to maintain. In ad hoc network if the nodes move on random speed then that protocol is supposes to be enhanced for communiqué. The example of reactive routing protocol is AODV routing protocol.

2.3 Hybrid Routing Protocol

Proactive and reactive protocols work finest in oppositely different scenario, hybrid method uses both. It is used to find a balance between both protocols. Proactive operations square measure are restricted to small domain, whereas, reactive protocols square measure are used for locating nodes outside those domains.

3. TYPES OF ATTACK IN MANET

There are various kinds of attacks at intervals on the mobile ad hoc network, nearly all of which may be classified as the following 2 types.

3.1 External attacks

In External attack, attacker aims to cause congestion, propagate duplicate routing information or bother nodes from providing services.

3.2 Internal attacks

In Internal attack the individual needs to gain the ordinary access to the system and including at interims of the network behavior, either by some noxious pantomime to discover the access to the network as novel node or by straightforwardly compromise an existing node and utilizing it as a premise to play out its malicious behavior. In the two classes shown above, external attacks square measure like the normal attacks at intervals of the conventional wired network in which the individual is at intervals and closeness is not yet a reliable node at intervals of the network, in this way, this kind of attack can be denied and recognized by the security techniques, for example, membership authentication or firewall, that square measure moderately average security solutions.

In any case, because of the determined communication character and open network media at intervals of the mobile ad hoc network, internal attacks area unit are comparatively more dangerous than the internal attacks: in light of the fact that the compromised nodes square measure initially the benign users of the ad hoc network, they will basically exceed the authentication and acquire protection from the security mechanism.

As a result, the adversaries can make use of them to gain normal access to the services to facilitate thought to only be available to the authorized users at intervals of the network, and they can be used by the compromised nodes to hide their malicious behaviors. Therefore, we must always pay extra consideration to the internal attacks that are initiated by the malicious insiders once we consider the safety problems in the mobile ad hoc networks.

In the following points, we discuss the foremost attack sorts that emerge in the mobile ad hoc networks.

3.2.1 Flooding Attack

Flooding attack [9] can also be a denial of service method of attack at intervals that the malicious node broadcast unnecessary false packet in the network to consume the market resources so that valid or legitimated user are able to use the network resources for valid communication. Because of the restricted resource constraints in the mobile ad hoc networks resource consumptions a result of flooding attack reduces the throughput of the network.

The flooding attack is probable in almost all of the network that require routing, relying upon the kind of packet used to flood the network, flooding attack can be classified in two classes.

3.2.2 RREQ Flooding

In the RREQ flooding attack, the attacker broadcast the various RREQ packets at regular time interval to the information science address that doesn't exist in the network and disable the restricted flooding feature. On demand routing protocols uses the route discovery method to support the route connecting the two nodes. In the route detection the available node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher than information packet, at the high load also RREQ packet are transmitted. A malevolent node exploits this feature of on demand routing to start the RREQ flooding attack.

3.2.3 Jamming Attack or data flooding

In the data flooding, malicious node overflow the network by sending useless data packets. To begin the data flooding, first malicious node engineers a path to all or any of the nodes then sends a large amount of imitative data packets. These ineffective data packet exhausts the network resources and thus legitimate users are not able to use the resources for valid communication.

The main influence brought by the attacks against routing protocols includes network partition, routing loop; resource deprivation and route hijack [8]. There are some attacks against routing that are studied and documented [10]:

- Impersonating another node to send-up route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with incorrect sequence selection to contain different reasonable route messages.
- Because of the quality and constantly changing topology of the mobile ad hoc networks, it's very tough to validate all the route messages.

3.3 Denial of Service (DOS)

The first type of attack is denial of service that aims to curb the accessibility of certain node or even the services of the entire accidental networks. In the conventional wired network, the DOS attacks are caused by flooding some reasonably network traffic to the target so as to weaken the processing power of the target and causing the services provided by the target become unavailable. However it is not wise to perform the standard DOS attacks because of the quality and continuously dynamic topology of the mobile. In the mobile accidental networks because of the distributed nature of the services, the mobile accidental networks are weaker than the wired networks because of the interference-prone broadcasting channel and the limited battery power. In the observation, the attackers precisely use the radio jam and battery exhaustion ways to conduct DOS attacks to the mobile accidental networks that correspond to the two vulnerabilities.

3.4 Impersonation

Impersonation attack could be a severe threat to the safety of mobile accidental network [11]. As we can see, if there is no suitable authentication mechanism between the nodes, the human can capture some nodes in the network and arrange them like benign nodes. In this way, the compromised nodes can be a part of the network as normal nodes and initiate malicious behaviors such as spread fake routing information and gain inappropriate priority to access some hint.

4. LITERATURE SURVEY

Let's look out different researches previously done by different researchers in field of security against jamming attack and different other attacks are mentioned in this section.

Soneram Verma and Maya Yadav [15] developed trust based on-demand routing protocols for knowledge transmission below jamming attack in MANET. The proposed protocols should be efficient in terms of Packet Delivery ratio, End-to-End Delay, normalized routing load (NRL), Residual Energy and Throughput. Based on the motivations to produce new security measures to be incorporated in popular routing protocols AODV, the aim of this work is to implement secure on-demand routing (TAODV) protocols for data transmission in MANET and detect jamming node in MANET scenario using TAODV protocol. *Pawani Popli and Paru Raj [16]*anticipated method used for mitigating and thwarting jamming attack enforced at the medium access control (MAC) layer that has an assimilation of a number of coordination techniques. These are an assimilation of Point Controller Functions (PCF) that are used to coordinate whole network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking method that dominate the collisions on the wireless network. In this OPNET, modeler is used to simulate the complete network performance and technique. *Ashwini Magardey and Dr. Tripti Arjariya [17]* Projected Intrusion Detection System (IDS) security scheme which recognize the attacker by their routing entry offered on further nodes routing record. The attacker has dumped the complete performance of network. The Multipath routing protocol AOMDV has provided the multiple path if the attack occurs in established path. The contagion from attack and performance metrics like throughput, routing load is evaluated and observe the secure anticipated security method is immobilized the routing misconducts of jamming attacker and makes available secure AOMDV routing performance as like to normal AOMDV performance. *Krunz et al. [18]* proposed a randomized distributed scheme that allows nodes to establish a new control channel using frequency hopping. Their method differs from classic frequency hopping in which no two nodes share the same hopping sequence, thus mitigating the impact of node compromise. Furthermore, a compromised node is uniquely identified through its hop sequence, leading to its isolation from any future information regarding the frequency location of the control channel. *Dorus et al. [19]* proposed a mechanism for preventing jamming attacks on wireless networks-examines the detection efficiency of jamming attack and communication overhead of the wireless network using proactive and reactive protocols. RSA algorithm is used for providing data packets integrity information during wireless transmission. Through simulation and performance analysis, the implemented prevention mechanism and the integrity preservation provides higher packet delivery ratio in proactive routing protocol (OLSR) than reactive routing protocol (AODV). *Chen et al. [20]* Proposed a methodology to localize a wireless node by using jamming attack as the benefit of the network. The projected localization method was divided into two phases. In primary phase, they ascertain the location of the jammer using power adaptation techniques. In the second phase, they employ these properties to extrapolate the locations of jammed node, with this the author design a localization protocol using this method, and demonstrated the feasibility of the anticipated mechanism by conducting indoor experiments based on IEEE 802.15.4 wireless nodes. The projected schemes consequence indicated that for some circumstances the proposed mechanism might be used to position mobile nodes under jamming attack.

5. PROPOSED SECURITY SCHEME AGAINST JAMMING ATTACK

Jamming of link between the nodes can cause severe damage and constant fails in whole network. In proposed work we create a new protection scheme against misbehavior of nodes. In this method we first explore the routing behavior of malicious nodes against the behavior of electronic counter measures attack then apply the appropriate well planned security scheme on it that block the whole misbehavior of malevolent nodes and enhance the network performance. The steps for identifying jamming attack are:-

- Calculate the number of paths established through multipath routing protocols.
- Check the proper packet delivery up to end of simulation for identified packet drop due to presence of attacker in network.

We propose a new robust rate adaptation scheme that is resilient to capture jamming attack in a wireless multi-hop dynamic network.

Proposed Algorithm for identified Jamming Attack

Create node =IDS; // Node as a IDS

Set routing = AODV;

Output: Throughput, PDR, Attacker Loss and TCP and UDP analysis

```
{
If ((node in radio range) && (next hop! = Null)
        {
                Senders establish connection to receiver;
                Data delivery is started;
                Capture load of all _ node
                Identified normal _ profile;
                Identified abnormal _ profile;
        }
        If ((load < = max _ limit) && (new _ profile == Normal _ profile ()))
                {
                No any attack;
         }
                Else
                {
                Attack in network;
                If (new _ attack == abnormal _ Identification ())
                                {
                                Find _ attack _ info (node _ number, packet _ type, time)
                                Capture infection type;
                                Infect data;
                                Block the infected or attacker node;
                                }
                Else
                {
                Maintain routing information;

                }}
        Else
{
"Node out of range or destination unreachable"
        } }
```

The jamming attack is an identity, it is an active attack and without activeness it is not possible to flood bulk of packets in network for consuming the network bandwidth. The proposed scheme identifies the attacker according to its jammed packets. The attacker is identified through heavy flooding of unwanted packets and the nodes that performs that kind of activities which are detected by IDS nodes. The detection and prevention technique is applied by IDS in network because of recognized malicious node activities and measure infection flooded by attacker in the network. The IDS at last lump the malicious nodes and sender choosing alternative path for data sending to destination.

6. SIMULATION TOOL USED AND RESULTS

Network Simulator (NS-2) NS2 [9] is an open-source event-driven simulator designed specifically for research in computer communication network. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academic world, and government. Having been under regular investigation and enhancement for years, NS2 now contains modules for several network components such as routing, transport layer protocol, application, etc. We use the IEEE 802.11 for wireless technology. The AOMDV routing protocol is taken at network layer. In our simulation, the number of nodes is 30. The mobile nodes move in an 800×600 m square region for 100 sec simulation time. We assume each node moves independently with the same average rate. All nodes have the similar transmission range of 550 m. In our simulation, the speed varied from 10 to 30 meters/seconds. Accidental way Point mobility model is used.

7. SIMULATION RESULTS

The simulation results in case of jamming attack with AOMDV and in case of secure AOMDV are evaluated that is discussed in this section.

7.1 Routing Overhead Analysis

In this graph we illustrated the performance of AOMDV protocol in jamming attack conditions where all the bandwidth are reserved by attacker by flood of huge amount of unauthorized packets in network. These packets are the packets send by attacker to reserve the available bandwidth of links by that the links are congested.

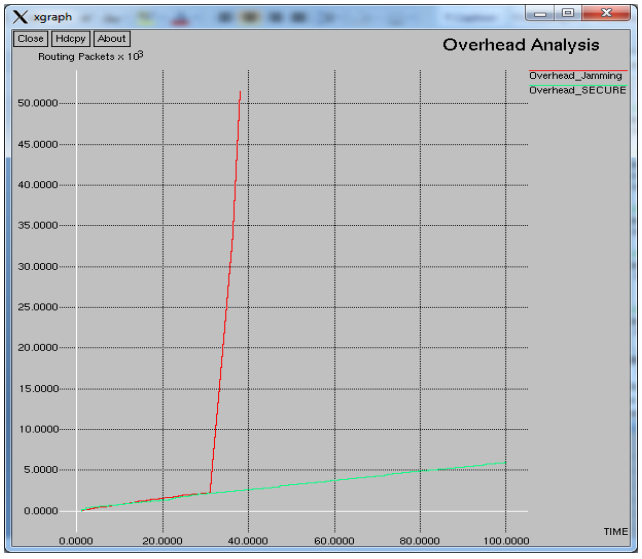

Fig. 1 Routing Overhead Analysis

That's why the routing overhead in a network in case of an attack is about 45000 packets in a given simulation time. The proposed security scheme against the attack minimizes the routing overhead to obstruct the misbehavior of attacker, that's why in case of proposed scheme with AOMDV protocol the routing load is normal, about 2600 packets at the end of simulation. The proposed scheme improve the routing

performance in presence of attacker and reach the routing load as equal to normal routing load.

7.2 Packet Delivery Ratio (PDR) Analysis

This graph shows the performance of AOMDV routing protocol in case of jamming attack, conditions and proposed attacker preclusion condition. The AOMDV protocol having a capability to resolve the possibility of congestion in network but if the inundation unauthorized packets consume the whole network bandwidth then the AOMDV will be unsuccessful to handle the load in network. That's why the PDR in case of jamming attack is only deliberated up to 35 seconds in network and after that the data delivery completely ends in the network so no PDR is scrutinized in network. The proposed security scheme against jamming attack has to completely eradicate the effect of attack that's why in case of proposed scheme the PDR is about 95 % at the end of simulation in network. The proposed scheme sustained the normal behavior of network in presence of attacker.

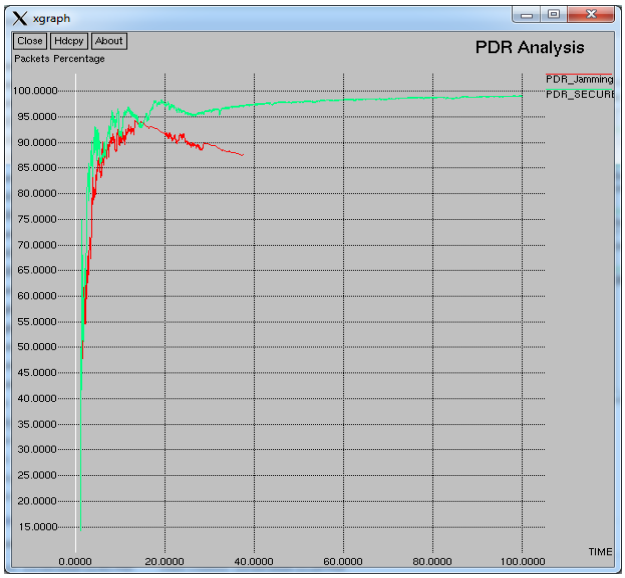

Fig. 2 PDR Analysis

7.3 Infected Jamming Packets Analysis

The Infected packets that are flooded in the network through attack consume the whole bandwidth and initiate the conditions of jamming links in network. In this graph from 0 to 5 second the attacker has not sent the packets, only sensed the neighbors for forwarding the data in the network. After 5 seconds the attackers starts the packets injection and at time about 32 sec high injected packet is delivered in the network because the attack has congested or jammed whole network bandwidth so that the packet forwarding and receiving is stopped in the network which is the main aim of attacker. The security scheme is applied in the network that finally blocks the injected packets delivered by the attacker so that in case of proposed infection no packet is delivered and the performance is upgraded.

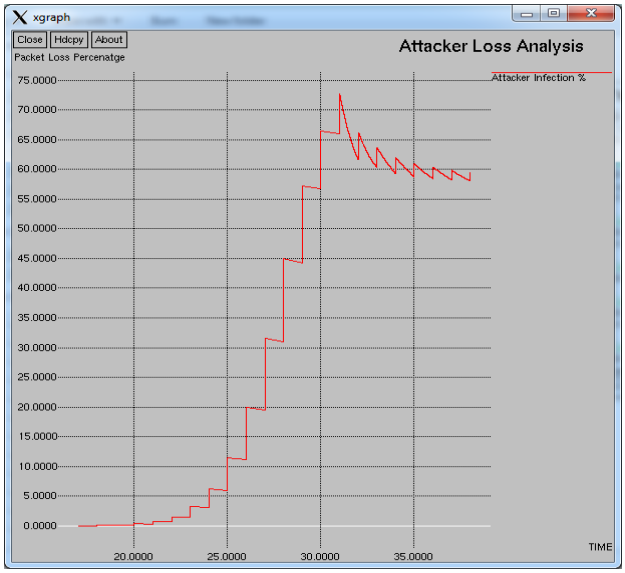

Fig. 3 Infection Analysis

7.4 Jamming Packets in case of Jamming Attack and Prevention Scheme

The packets that the jammer nodes are injected with in the network and also in case of proposed scheme no packet is inundated in network as mentioned in table 1. Here the Node 9, Node 15 and 21 are the attacker nodes that are injected with the infected packets in network. The security scheme completely blocks the jammer effect and provides zero infected data delivery in network.

Table 1 Jammer Packets Analysis

jamming Attack		Prevention Scheme	
Jammer Node	**Total Unauthentic Packets**	**Jammer Node**	**Total Unauthentic Packets**
9	99801	9	0
15	55916	15	0
21	13876	21	0

8. CONCLUSION & FUTURE WORK

Mobile ad hoc network may get compromised from different types of security threat which degrade the performance of the network. Jamming attack is one of the security threats which jams whole network. This article mainly emphases on intrusion detection system to combat the jamming attack over the network. The proposed scheme is simple and has effective IDS which can be implemented easily. The proposed IDS identifies the unwanted message source to take strong action against them. This scheme is simulated in NS-2 network simulator and comparative analysis is done using PDR and routing overhead. The experimental results of the proposed scheme gives improved value of PDR and routing overhead than the existing system which means that our scheme is more effective to combat the network from jamming attack.

In future we propose the security scheme against vampire attack. The behavior of vampire attack is same as jamming but vampire attack target is bandwidth and node energy both. Applying the proposed security scheme on vampire attack and also propose the scheme for packet dropping attack in MANET.

9. REFERENCES

[1] S. Madhavi, "An Intrusion Detection System In Mobile Ad hoc Network", International Journal of Security and Applications, Vol. 2, No. 3, pp. 1-16, July 2008.

[2] V. P. and R. P. Goyal, "MANET: Vulnerabilities Challenges Attacks Application", IJCEM International journal of process Engineering & Management, Vol. 11, pp. 32-37, January 2011.

[3] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the Energy utilization of Security Protocols," Departure on of International conference of Low Power Electronics and Design (ISLPED '03), 2003.

[4] Elizabeth M. Royer, Chai-Keong Toh, "A analysis of existing Routing Protocols for ad hoc Mobile Wireless Networks", IEEE pathetic Communications, Vol. 6, No. 2, pp. 46-55, April 1999.

[5] 5 Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of a variety of Routing Protocols for MANETS" , International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[6] P. Yi, Z. Dai, S. Zhang, Y. Zhong, "A New Routing Attack In Mobile ad hoc Networks", International Journal of information technology, vol. 11, no. 2, pp. 83-94, 2005.

[7] Yongguang Zhang and Winke Lee, "Security in Mobile Ad-Hoc Networks", In volume ad hoc Networks technologies and Protocols (Chapter 9), Springer, 2005.

[8] P. Papadimitratos and Z. J. Hass, "Secure routing for Mobile ad hoc Networks", In measures of SCS Communication Networks and Distributed Systems model and Simulation Conference (CNDS), san Antonio TX, January 2002.

[9] Amitabh Mishra and Ketan M. Nadkarni, "Security in Wireless Ad hoc Networks", In volume the instruction book of ad hoc Wireless Networks, CRC Press LLC, 2003.

[10] Aleksi Marttinen, Alexander M. Wyglinski, Riku Jantti, "Statistics-based jamming Detection algorithm for jamming Attacks Against considered MANETs", IEEE Military Communications Conference, pp. 501-506, 2014.

[11] Hussein Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, Member, IEEE, and Adrian Perrig, "Jamming-Resilient Multipath Routing", IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 6, pp. 852-863, November/December 2012.

[12] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE Transactions On Network And Service Management, Vol. 9, No. 2, pp. 169-182, June 2012.

[13] Preeti Sachan, Pabitra Mohan Khilar, "Security Attacks and solution in MANET", Proceedings of International Conference on Advances in computer Engineering, pp. 172-177, 2011 ACEEE.

[14] Pravina Dhurandher, "FACES: Friend based ad hoc Routing with challenge to establish security in MANET Systems", IEEE SYSTEMS Journal, Vol. 5, No 2, pp. 176-188, June 2011.

[15] Soneram verma1, Prof. Maya Yadav 2016 "Detection and Prevention for Jamming Attack in MANET using TAODV Protocol", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 05.

[16] Pawani Popli1, Paru Raj 2016. Mitigation of Jamming Attack in Mobile Ad Hoc Networks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 6.

[17] Ashwini Magardey, Dr. Tripti Arjariya 2013. Secure Detection and Prevention Scheme for Jamming Attack in MANET, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[18] [18] Loukas Lazos, Sisi Liu, and Marwan Krunz "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks", WiSec'09, March 16–18, 2009, Zurich, Switzerland 2009 ACM 978-1-60558-460.

[19] R. Dorus, P. Vinoth "Mitigation of jamming attacks in wireless network ",Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on Date of Conference: 25-26 March 2013.

[20] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague 2012. All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack, IEEE-2012.

[21] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.