EasyChair Preprint

№ 3789

A Flooding based IDS Security against Jamming Attack in MANET

Gaurav Soni and S. Sudhakar

July 8, 2020

An IDS Security against Unwanted Flooding of Jamming Attack in MANET

Gaurav Soni
Ph.D. Scholar in CSE
Swami Vivekananda University (SVU)
Sagar, India
gauravsoni.rits@gmail.com

Dr. R Sudhakar
Professor in CSE
Swami Vivekananda University (SVU)
Sagar, India
sudhavk1983@gmail.com

***Abstract*— The attacker/s are easily modified or infected the routing performance by flooding unwanted packets in Mobile Ad hoc Network (MANET). Each node in MANET is performing the role of sender, receiver and intermediate node. In this open network Security is the one amongst the most important problem. The multipath routing has a benefit to reduce routing overhead in network by proving the alternative path if the already established path is fail in communication. In this paper, we propose the Intrusion Detection System (IDS) for Jamming attack. The proposed IDS is reliable and provides a secure path for exchanging information. In multipath routing, the possibility of secure routing is enhanced in the presence of an attacker and proposed IDS able to handle it. The jamming attacker slowly-slowly injected the packets in network and these packets quantity is rapidly enhance according to time instance. After some time the attacker is consuming the link capacity by that communication between the nodes is uncertain and the whole network is jam. The IDS is identified as the attacker nodes through its behavior of unwanted flooding and identified the infection from the attacker. The performance of the proposed security system provides the usual routing performance and providing a secure different path in MANET. The proposed scheme is continuously watching the activities of all nodes in the network and the activities of the malicious node are completely different from normal nodes and they are not behaving like a normal node. The attacker infection according to time instance is enhanced by IDS are control it provides secure routing.**

***Index Terms*—Security, Flooding, Jamming attack, IDS, Routing, MANET, Multipath**

I. INTRODUCTION

All The nodes in Mobile Ad hoc network are continuously moves in limited area and forming 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 presence in network for watching the network activities. The wired network is uses copper wire for communication and on the other hand in MANET uses a radio waves to transmit signals [1]. The two mobile nodes have different connections between them is reliable for connection and conveyed in an exceedingly complete manner, suitable for cost and time successful setting, and for a situation any place foundation is problematic to arrangement. Security is troublesome in MANETs [2] inferable from its qualities like companion to see structure, operational while not focal arranger, dynamic topology, uncertain operational setting, and continuous connection breakage owing to mobile nodes, battery timeframe, nodes capacity and non consistency [3]. Communication in MANETs is through single jump in connection layer protocol and multi bounce in network layer protocol, bolstered the conviction that everyone the mobile nodes in an exceedingly network are pleasant in coordination strategy, however unfortunately this statement isn't valid in unreceptive setting. Malicious assaults [2] disturb well organize activity by damaging protocol specification. The network layer activities in MANET are supported routing and acknowledgement of packets sending each of node are vulnerable due to presence of jamming attack. MANET needs strong support for forwarding data in between genuine nodes in presence of malicious node/s or attack. In MANET due to the open environment of communication security is necessary against malevolent attacker/s and these attackers are very harmful for network . Attackers are extreme security threats in network which may use with no issue by abusing vulnerability of on-demand routing protocol like multipath AODV. This attempts to utilize Intrusion Detection System (IDS) to stop attackers compulsory by each single and numerous mobile nodes and along these lines the Detection and recuperating routing trouble making underneath MANET. The proposed IDS to the particular approach maximize routing performance by the assistance of limiting creation of control (unwanted) packets just as effectively restrict the jamming attacker in MANET[1].

II. ROUTING PROTOCOLS IN MANET

In MANET the topology is normally changes that are the reason for connection breakage are made as mutihop connectivity till the goal isn't found. The routing protocol is having a basic influence at network layer for data receiving and sending through each node. The data is send by sender and acknowledged by receive, in that procedure routing procedure is significant piece of communication [4, 5]. For interfacing with end and data conveyance the routing protocol is fundamental for routing the information in between of sender to receiver. Each routing protocol has distinctive routing

methodologies of connection establishment however has same strategy for select path in between sender and receiver. The direct path significance in MANET is decided on the basis of minimum hop count. The classification of routing protocol in MANET are as following:-

A. Proactive Routing Protocol

The proactive routing protocol are additionally called as are keeping up the routing data of every mobile node counter determined routing protocol and these routing protocol that are work together in routing technique. In MANET the topology in network is change by that the straight forwardness of keep up the data of every mobile node is very complex and required larhe memory for store routing data in network In dynamic network, if the mobiles are moves at moderate speed, at that point that protocol is accept to be better for communication. The case of proactive routing protocol is DSDV routing protocol.

B. Reactive Routing Protocol

The Reactive routing protocol are also called as on demand routing protocol and these routing protocol are keep up the routing information based on request accepted by the neighbor. There is no routing data is put away of every mobile node that are work together in routing method. In MANET the topology in network is change by that the overhead of keep up the data of every mobile node isn't wanted to keep up. In MANET on the off chance that the nodes are move indiscriminately speed, at that point that protocol is assumes to be improved for communication. The case of receptive routing protocol is AODV routing protocol.

C. Hybrid Routing Protocol

Proactive and receptive protocol each work preeminent in oppositely unusual scenario, hybrid technique utilizes both. it is utilized to discover a harmony between the two protocol. Proactive tasks are limited to small province, while, reactive protocol are utilized for finding nodes outside these province:-

III. TYPES OF ATTACK IN MANET

There are different sorts of attackers inside the portable specially appointed network, almost which can all be delegated the accompanying two sorts.

A. External attacks

The External attacker plans to cause jamming, spread facsimile routing data or trouble nodes by providing services .

B. Internal attack

In Internal attack the malicious node needs to gain the ordinary access to the network and include you inside the system conduct, either by some malignant pretense to discover the entrance to the network as a new mobile node, or by straightforwardly compromise a existing mobile node and utilizing it as a premise to lead its injurious practices. In the two classes appeared above, external attacker are almost same as like the ordinary attacker in the wired network. The attacker is in the nearness yet not a dependable mobile node in the network, thusly, this sort of attacker can be denied and identified by the security strategies, for example, participation validation or firewall, that are security arrangements.

1) Flooding Attack

Flooding attacker or flooding [6] might be a Denial of Service attacker that interims which the malevolent mobile node communicate the pointless false packets in the network to devour the available resources so, that substantial or legitimated client can't ready to utilize the network resources for significant transmission. Due to the limited asset limitations in the versatile specially appointed networks asset utilizations an aftereffect of flooding attacker diminishes the throughput of the network.

The flooding attack is likely in all most all the on require routing, depending upon the sort of packets used to flood the network, flooding attack can be characterized in two classes.

1) RREQ flooding
2) DATA flooding
3) RREQ FLOODING

RREQ flooding information flooding RREQ flooding in the RREQ flooding attack, the aggressor communicate the different RREQ packets per time interim to the IP address that doesn't exist in the network and restricted the confined flooding highlight. Reactive routing protocol utilizes the route discovery procedure to help the course associating the two mobile nodes. In route finding the accessibility node communicate the RREQ packets in the network. Since the need of the RREQ control packets is higher than data packets then at the high burden likewise RREQ packets are transmitted. A pernicious mobile node misuses this component of on on demand routing to dispatch the RREQ flooding attack.

2) Jamming Attack or Data Flooding

In the data flooding, malicious node flood the network by sending pointless information packets. To begin the information flooding, first malignant node built a path to all or any the mobile nodes at that point sends the huge measure of imitative information packets. These pointless information packets debilitates the network resources and in this manner legitimated client can't ready to utilize the resources for significant communication.

The main influence bring by the attacks against routing protocol incorporate network packets, routing loop, asset deprivation and route hijack [7]. There are a few attacks against routing that are considered and archived [8]:

1) Impersonating another node to send-up course message.
2) Advertising a bogus route metric to distort the topology.
3) Sending a route message with wrong arrangement determination to contain other sensible course messages.
4) Because of the portability and always changing topology of the versatile networks, it is extremely hard to approve all the route messages.

3) Denial of Service (DOS)

The primary class of attack is Denial of Service, which expects to crab the openness of certain node or even the services of the whole incidental networks. In the regular wired network, the DOS attack are acknowledged out by flooding some wisely network traffic to the target in order to debilitate the processing power of the target and make the services provided by the target become inaccessible. Anyway it ends up not reasonable to play out the standard DOS attack as a result of the versatility and consistently unique topology of the network. In addition, the dynamic networks are more vulnerable than the wired networks on account of the interference prone radio channel and the restricted battery control. In the perception, the assailants precisely utilize the radio jamming and battery exhaustion techniques to direct DOS attacks to the portable inadvertent networks, which well related to the two vulnerabilities.

1) **Impersonation**
   Impersonation attack is a severe menace to the security of dynamic network [9]. As should be obvious, if there isn't such a reasonably validation scheme between the nodes, the human can catch a few mobile nodes in the network and organize them rise like favorable nodes. Along these lines, the trade off mobile nodes can be a piece of the network as the typical nodes and start to lead the malicious practice, for example, provoke spurious routing data and addition unseemly need to get to some confidential information.
2) **Eavesdropping**
   Eavesdropping is another type of attack that generally occurs in the MANET. The objective of eavesdropping is to get some private data that ought to be kept mystery during the communication. The confidential data may incorporate the location, private key, public key or even passwords of the nodes. Since such information are critical to the security condition of the nodes, they ought to be avoided the unauthorized access.

IV. Literature Survey

We should watch out different researchers effectively done by different resarch in field of protection from jamming attack and other different attacks are referenced in this segment.

In this paper [10], proposed the detection for responsive jamming attacks in the intentional MANET. Since strategic networks are commonly used in emergency the board and field activities, trust worth and secure communication is a basic issue for mission achievement. In this way, jamming assault must be identified and relieved immediately by the remote network. New methodologies for the identification and alleviation of jamming attack are required, especially for strategic networks dependent on versatile unplanned innovation where incorporated discovery calculations are unrealistic. They present another network to find jamming in strategic unplanned networks, which depends on the necessary number of re-transmission attempt of transmitted packets and packets conveyance pace of got packets.

In this paper [11] protocols that can reply of communication aggravation on-request. Specifically, a source node chooses various ways for arriving at the goal ahead of time. The accessibility history of ways are proficiently recorded and determined by means of "accessibility history vectors". Utilizing AHVs, we've get introduced two AHV-based multipath choice calculations: one chooses various ways through the total data of AHVs in the network, and the different processes the way in an appropriated way. AHV-based calculations can viably recognize numerous ways that give top of the line to-end openness, even within the sight of another jammer that didn't trouble the network before way choice. Furthermore, the proposed disseminated AHV-based strategy achieve higher accessibility than AODV at a littler communication cost for enduring communication session

In this paper [12] they incontestable the achievability of dynamic progressive trust association and application level trust optimization design concepts with trust based generally geographic routing and trust-based IDS application, by recognizing the best method to type trust just as use trust out of individual open and QOS trust properties at runtime to advance application execution.

In this paper [13] proposed a trust-based IDS methodology away performs customary abnormality based IDS strategies in the recognition possibility while keeping up adequately low false positives. They are talk about the various types of security attacks that can be launch effectively in MANET and related arrangements required for guarantee organize security. This paper executes the protected specially appointed on-request separation vector routing protocol (SAODV) and contrasts the exhibition of protocol and open AODV protocol within the sight of dark gap attack.

In this paper creator proposed FACES (Friend-Based Ad-hoc steering utilizing challenge to set up Security) [14], that gives a rundown of confided in nodes to the source node by causation difficulties and sharing companion records. In view of the degree of effective data transmission and in this way the anticipated association with elective nodes in an exceedingly arrange, the nodes inside the companion records are rate. The trust level of each node differs from 1 to 4. The nodes in the network are set in one among the 3 records, for example accentuation mark list, friend list and unauthenticated list. The steady flooding of unwanted packets and sharing of companion records will expand the management transparency.

V. PROPOSED SECURITY SCHEME AGAINST JAMMING ATTACK

Jamming of link between the nodes could cause severe damage, constant fails in entire dynamic network. In this scheme secure the nodes communication by identified jamming misbehavior of nodes. In this method first explore the routing behavior of malicious nodes against the behavior of electronic countermeasures attack then concern the appropriate well planned security scheme on it that block the whole misbehavior of malicious nodes and improve the network performance. The steps of identify jamming attack are:-

- Calculate the number of paths established through multipath AOMDV routing protocols.
- Check the proper packet delivery up to end of simulation for identified the 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.

A. Proposed Algorithm for identified Jamming Attack

```
Create node =IDS ; //  Node as a IDS
Set routing = AOMDV;
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,
                pkt_type,time)
                Captute infection type;
                Infect data;
                Block the infected or attacker node;
                }
        Else
        {
        Maintain routing information;

        }       }
    else
{
    "node out of range or destination unreachable"
    }
        }
```

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

VI. Simulation Tool used and Results

Network Simulator (NS-2) NS2 [15] is an open source event driven simulator designed specifically for research in computer networks or specially in field of wireless communication. Since, In the beginning of 1989, NS2 has incessantly achieved fabulous interest from, academician, industry and administration. NS2 contains modules for numerous network components such as routing, transport layer protocol, application, etc. and modules will continuously under the enhancement in years and years. We use the IEEE 802.11 for wireless technology. The AOMDV roruing protocol is taken at network layer. In this simulation, in parameters we first talk about number of nodes i.e. taken 50. The nodes move in an grid area of 800m×600m for 50 seconds simulation time. In the scenario each node moves independently with the different mobility speed. All nodes have the same transmission range of 550 m. In simulation, the speed is varied from 10 to 30 meters/seconds. Random Way Point mobility model is used.

VII. Simulation Results

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

A. 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 inundation of huge amount of unauthorized packets in network..

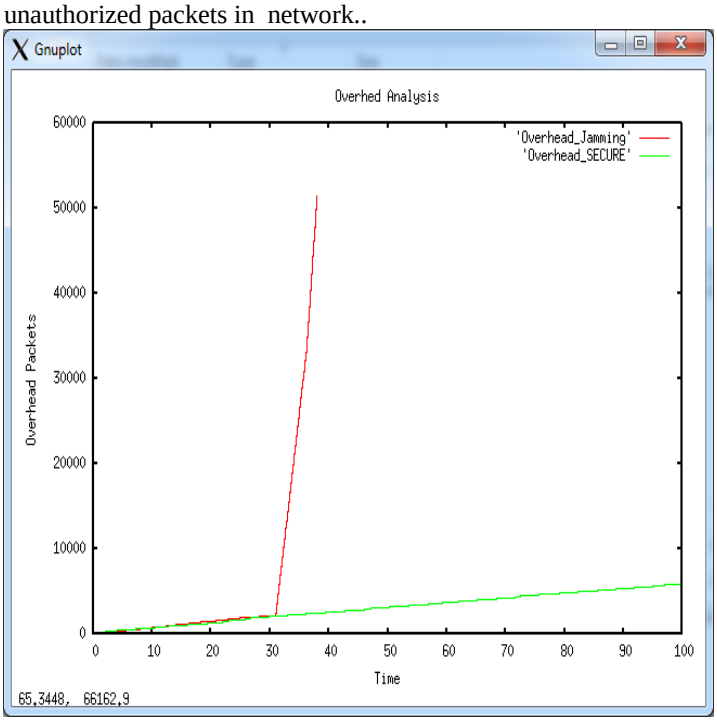

Fig. 1. Routing Overhead Analysis

These packets are the packets send by attacker to reserve the available bandwidth of links by that the links are congested That's why the routing overhead in network in case of attack is about 45000 packets in network in a given simulation time. The proposed security scheme against 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 secure scheme is improves the performance in presence of jamming attacker. The overhead of the routing as equal to normal routing load.

B. 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 is consumes the whole network bandwidth then the AOMDV be unsuccessful to handle the load in network. That's why the PDR in case jamming attack is only deliberated up to 35 seconds in network and after that the data delivery is completely end in network so no PDR is scrutinize in network. The proposed flooding identification security against jamming attack has completely eradicate the effect of attacker that's why in case of proposed scheme the PDR is about 95 % at the end of simulation in network. The proposed scheme is sustained the normal behavior of network in presence of attacker.

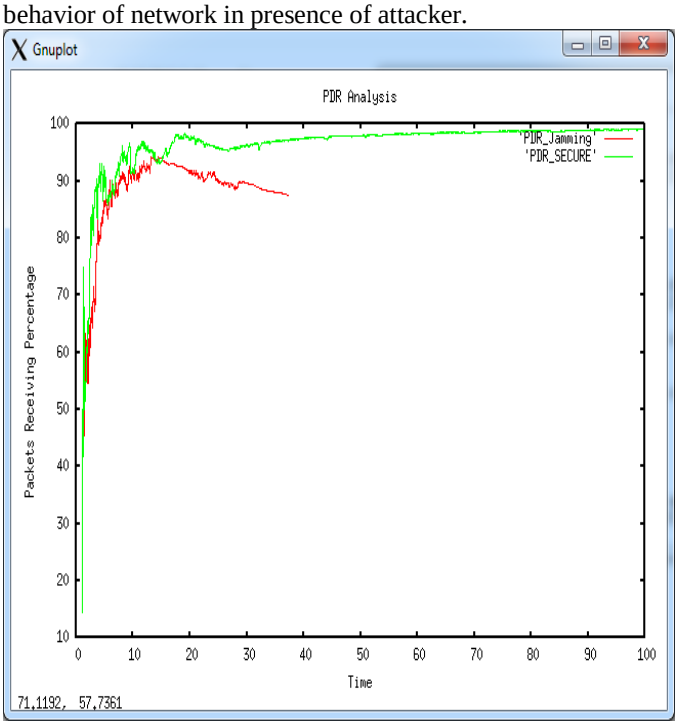

Fig. 2. PDR Analysis

C. Infected Jamming Packets Analysis

The Infected packets that are flooded in network through attacker consume the whole bandwidth and emerged the conditions of jamming links in network. In this graph the 0 to 5 second the attacker has not sending the packets only sense the neighbor to forwarding the data in network. After 5 second the attackers started the packets injection and at time about 32 sec high injected packet is deliver in network because the attacker has congested or jammed the whole network bandwidth so that the packet forwarding and receiving is stop in network i.e. the main aim of attacker. The security scheme is applied in network that finally block the injected packets deliver by attacker so that in case of proposed infection no packet is deliver and the performance is upgraded.

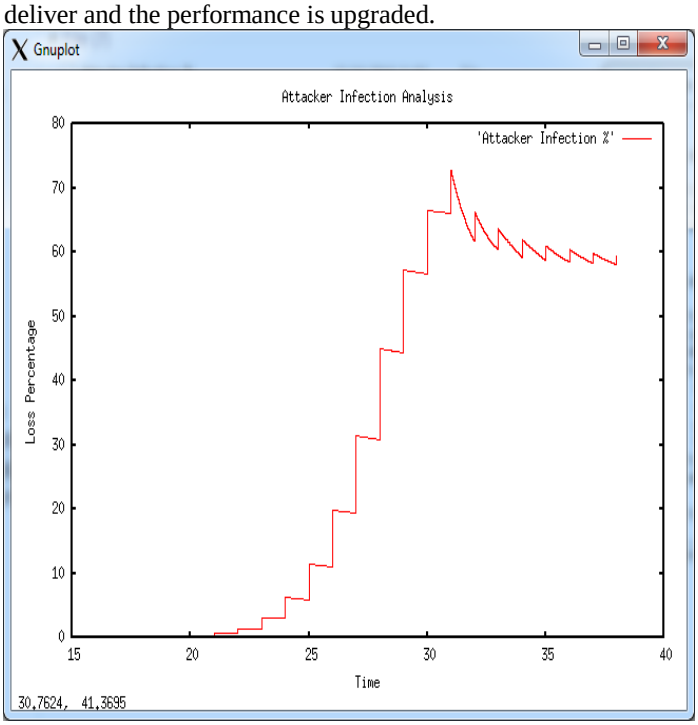

Fig. 3. Attacker Infection Analysis

D. Jamming Packets in case of Jamming Attack and Prevention Scheme

The packets that the jammer nodes are injected in network and also in case of proposed scheme no packet is inundated in network mentioned in table 1. Here the Node 9, Node 15 and 21 are the attacker nodes that are injected the infected packets in network. The security scheme is completely block 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

VIII. CONCLUSION & FUTURE WORK

The attacker in MANET is infected the actual routing performance. The network is completely dynamic and the nodes movement is creating the problem in strong link establishment. The secure data communication is necessary for

deliver the actual information in right way to receiver. In this paper, the proposed flooding identification based security against jamming attack is effective and reliable as compare to previous scheme. The multipath AOMDV routing protocol is used for communication is for better and reliable route. But the other a variety of routing protocols could be replicated also. Proposed reliable Intrusion Detection System looks the multipath in the AOMDV level and Finding the attacker nodes for secure network communication. The proposed scheme is identified the attacker through their flooding behavior and this behavior is continuously activate in network to consumes link limited bandwidth. The proposed IDS is identified the unwanted message source to take strong action against them. The attacker node is only node in network which is not receive the any request of any node but flooded the unwanted messages that enhance unnecessary load in network. The IDS node is also receives that messages and identified that these messages is completely useless then identified that node/s and completely prohibited that kind of malicious action in network. The proposed scheme is hinder the communication of attackers and multipath protocol is able to provides the reliable path if the existing one is failure due to any reason. The IDS showing the better throughput, PDR and routing load in network.

In future we proposed the IDS 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 scheme on vampire attack and also proposed the scheme for packet dropping attack in MANET.

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] [8]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, 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] Detection”, IEEE Transactions on Network and S Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho, “Hierarchical Dependence Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion ervice 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.

[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] The Network Simulator NS-2 content available on link https://www.isi.edu/nsnam/ns/ns-build.html