International Journal of Engineering Applied Sciences and Technology, 2015
Vol. 1, Issue 2, ISSN 2455-2143, Pages 43-51
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

DETECT AND ISOLATE SELECTIVE PACKET DROP ATTACK IN AD-HOC NETWORK THROUGH SECURE CHANNEL ESTABLISHMENT

Jaspreet Kaur
Computer and Science Engineering
Punjab Technical University,
Jalandhar, Punjab, India

Satish arora
Computer and Science Engineering
Punjab Technical University
Jalandhar, Punjab, India

Abstract - **Wireless Networking is getting to a great degree persisting now a day as the client need wireless availability independent of their topographical area. Ad-hoc Network is decentralized, self-configuring and self-governing wireless network in which nodes can join or leave the network at whatever point they require. The term Ad-hoc implies no fixed infrastructure i.e. Dynamic Topology. Besides these components, Ad-hoc Networks endures from many security issues i.e. active and passive attacks. To arise a mechanism that allows firm security and comprehends the malicious node activity in the network. Permitting a secure communication among source and destination is one of real issue in ad-hoc network. This paper depicts Key Distribution and Monitoring (KDAM) technique used to detect and isolate malicious node on selective path in AODV routing protocol and secure the channel. The strategy gives enhancement over the antecedently characterized techniques as far as delay, packet loss and throughput. The simulation is acted on Network Simulator-2.**

Keywords *- Wireless Ad hoc Networks; Dynamic Topology; Attacks; Security; Selective Packet Drop Attack; NS-2*

I. INTRODUCTION

To exchange information, a number of devices are joined to together to form network between them [1, 2]. Networking is applied to broadcast information and data communication. Wireless Networking is a technology is an innovation in which two or more PCs alluded to as nodes speaks with one another utilizing wireless connections. Wireless network can be basically either infrastructure based network or infrastructure less network. The infrastructure networks use altered base station, which are in charge of organizing correspondence between the nodes. The ad-hoc network goes under the classification of infrastructure less systems. Ad-hoc Network is gathering of many devices fitted with wireless communication and network capabilities. [7]Ad-hoc Network is decentralized with no pre-subsisting infrastructure, for example a router in wired networks and access focuses in wireless networks on which it is depended. In routing so as to direct every node shares information for different nodes in specially Ad-hoc network the determination of which nodes forward information is made strongly on the substrate of network availability. Ad-hoc Networks are a nascent standard of wireless communication for mobile hosts. Nodes within each other radio range communicate directly by means of wireless connections while these which are far separated depend on different nodes to relay messages. Wireless networks make usage of radio waves or microwaves in order to set up communication between the conveniences [3, 4, 5]. Every node taking an interest in the network behaves both as a host and a router and hence willing to forward packets for other nodes. For this reasons a routing protocol is required.

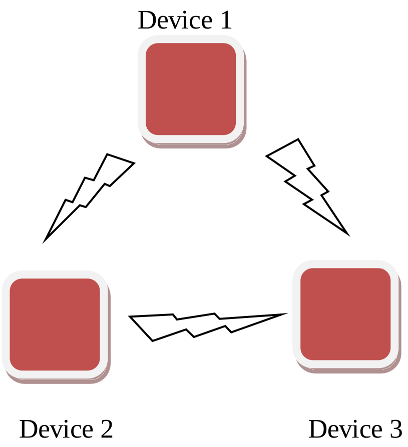


Figure-1 Example of Ad-hoc Networks

Wireless Ad-hoc Network is a self-arranging, self-configuring and quickly deployable network in which neither a wired backbone nor a centralized control exists. The nodes are frequently energy constrained. The primary characteristics of wireless Ad-hoc networks are -: Dynamic Topology, self-organization, multi-hopping, energy conservation, scalability. Ad-hoc Routing Protocols can be categorized as Proactive or Reactive. Ad-hoc Networks are threatened to security attacks. Attack is the mechanism which disrupts the normal behavior of the network [6]. There are varieties of attacks possible in Ad-hoc networks. These are discussed below:

A. Passive Attack

A passive attack gets information exchanged in the network without disturbing the operations. The passive attacks are hard to detect as the operations are not influenced. This attack does not disrupt the normal operations of the network. The operations supposed to be achieved by a malicious node which is ignored and attempt to recover significant information by listening to the channel. Snooping and Eavesdropping are examples of passive attacks [3].

B. Active Attack

An active attack is that attack in which any data or information is embedded into the network so that data and operation may be harmed. The attacker attempts to alter the data being exchanged within the network. The active attacks disrupt the normal functioning of the network. It includes modification, fabrication and disruption of information which influence the operation of the network. Examples of active attack are impersonation and spoofing [3].

The primary goal of this paper is to detect and isolate selective packet drop attack from routing path in AODV routing protocol of Ad-hoc Network. Wireless Ad-hoc Networks are normally tested with an extensive number of the network vulnerabilities. In general, nodes are commonly thought to be a trustworthy and cooperative. Unfortunately, clients in Wireless Ad-hoc Networks tend to drop alternate’s packets to terminate an information communication, known as a Packet Drop Attack. To impersonate as a normal one and does not forcibly secure a routing path. To terminate the communication, the attack discards to forward information packets for a receiver.

The remaining paper is organized as follows. Section II discusses the background and related work. In section III describes the Selective Packet Drop Attack. Section IV shows the research methodology. Section V illustrates the simulation results. Finally, section VI gives the conclusion and future work.

II. BACKGROUND AND RELATED WORK

Recently Wireless Networks are getting more and more popular. **El-Haleem et al. (2011)** proposes methodology to isolate packet dropping attack by using two disjoint routes protocol in MANET. In this procedure two node disjoint routes are chosen situated in their trust value and use to routes from source to destination. They utilize DLL-ACK (acknowledgement) and end-to-end Tcp-Ack to distinguish and examining the conduct of routing path, node. On the off chance that any malicious node find in the way then path search engine tool get run and distinguish the malicious node and forestall it. [8].**H-M Sun et al. (2012)** propose an acknowledgment-based technique, called NACK, to detect and mitigate the dropping attacks. Besides, NACK can oppose the collusion attack by utilizing the timestamp component. In spite of the fact that NACK can oppose effectively collusion attack, it just considers the instance of two successive nodes. For our future work, we will improve the capacity about opposing more sorts of collusion attacks. Contrasted and different methodologies, for example, the overhearing technique, the NACK plan has better execution. Our simulation results demonstrate that the NACK plan keeps up to 80% packet delivery ratio in every attack even when the adversary ratio is 40% [10].**Sharmila et al. (2012)** discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to identify selective forward attack in mobile wireless sensor networks. The scheme is assessed as far as packet delivery ratio and throughput. The malicious node is distinguished in light of the acknowledgement and energy level of the node. The energy utilization of the scheme is less when contrasted and existing schemes. From the simulation outcomes, byte overhead is 0.39 and identification exactness is 80% are watched and in this way expanding the throughput. These outcomes demonstrate that the packets can be sent with no selective packet drop by minimizing the malicious node in the system. The further upgrade of the proposed plan is to enhance the achievement rate to 100% with different portability and beneficiary affectability of the node [11]. **Mohanapriya et al. (2013)** presents a Modified Dynamic Source Routing Protocol (DSR) to identify and prevent selective black hole attack. With the help of Intrusion Detection System (IDS) the malicious nodes are kept from the framework where the IDS nodes are set in promiscuous mode exactly when required, to recognize the temporary difference in the amount of data packets being sent by a node. The proposed method used to accept the adequacy of proposed intrusion detection system [20]. **Aaseri et al. (2013)** discusses Trust Value Algorithm the black hole node can be detected based on the trust values which will result into the low false positive rates. So, Our Approach solves the problem of Packet drop attack with 92% of the success which is far better than the earlier prevention technique to packet drop attack. We used UDP connection to calculate the packets at sending and receiving nodes. In the event that we had utilized the TCP connection among nodes, the sending node would be the end of the connection, since ACK packets don't come at the sending node. The disclosure the black hole node with connection situated protocols could be another future work [16].**Chuachan et al. (2013)** depicts new methodology how to detect and prevent selective packet drop attack. In this paper they discuss 4 previous methods to protect against 1.reputation based 2. Acknowledgement based 3. IDS based 4. Trusted based. The new proposed composition called challenge and response schema. It contain 2 stage I) Key distribution II) Challenge ad response. The message is encrypted utilizing the public key and routed in two-hop neighbor, assume ratio of local one compare it with neighbor node. The malicious node can be identified by setting threshold value to reserve and towards the end this quality to the neighbor's value. To simulate this result they use Common Open Research Emulator (CORE) [18]. **Edemacu et al. (2014)** Wireless ad-hoc networks have derived lots of consideration due to their easiness and minimal effort of deployment. This has made ad-hoc networks of incredible significance in versatile military and civilian applications. Be that as it may, the absence of centralized management of these networks makes them vulnerable to several security attacks. One of the attacks is packet drop attack, where a compromised node drops packets maliciously. A few techniques have been proposed to detect the packet drop attack in wireless ad hoc networks. Subsequently, in this paper we survey some of the packet drop attack detection methods and relatively break down them basing on their ability to detect the attack under different strategies (partial and or cooperate attacks), environments and the computational and communication overheads induced in the process of detection [23]. **Sangeetha (2014)** proposes strategy to secure transmission in the MANET utilizing Ad-Hoc On-Demand routing protocol (AODV). Because of absence of asset and foundation ad-hoc network is not ready to demonstrate consistent operation. Proposed technique called Enhanced Adaptive Acknowledgment (EAACK) which raises Integrity of IDS (Intrusion Detection System) by utilizing computerized signature. It lessens overhead which emerge amid directing in AODV convention.

III. SELECTIVE PACKET DROP ATTACK

Selective forwarding attack is a form of denial of service attack where a malicious node depicts packets and drops them specifically without sending to the destination. Packet dropping attack is found in the forward stage. So it is extremely composite and hard to isolate. Selective forward attacks may ruin some discriminating applications. In this attack, basically malicious node goes about as normal nodes yet specifically drop sensible packets, for example packet describing the development of the disagreeing forces. Such Selective dropping is very firm to recognize. Counter measures to specific forwarding attacks cannot understand malicious node or include time synchronization. Then again, when malicious node is show on a route by which packets are forwarded, attackers can introduce selective forwarding attacks by merely dropping packets [10]. In this attack, nodes in way expected to forward the packets towards destination yet malicious node dispose of the some measure of packets to upset the system [10, 23].The malicious node can succeed this attack selectively so it is called selective packet drop attack.

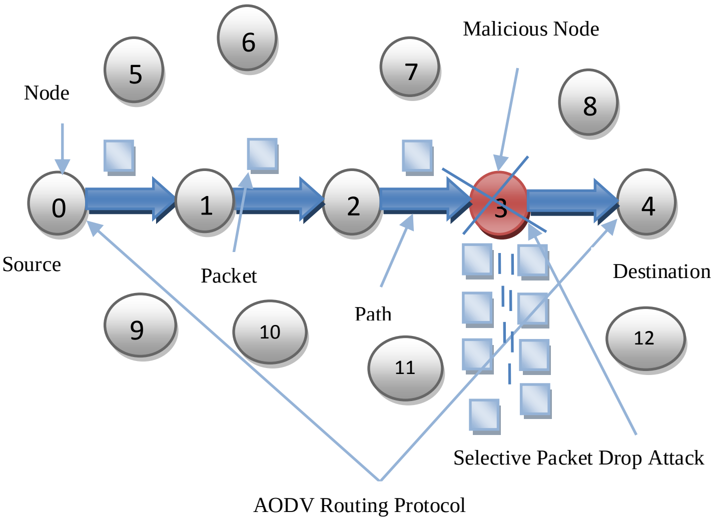


Figure-2 Selective Packet Drop Attack

Selective forwarding attacks can root genuine danger on numerous applications. These attacks have few nodes which drop some or all packets. Attacker can begin the selective forwarding attack and stroke the allocation of packets for which it expect to store set as forward the rest. This attack is exceptionally hard to distinguish, since packet drops in networks potentially created by untrusted wireless communication or node failure [12,13].

IV. RESEARCH METHODOLOGY

This section represents the methodology used to detect and isolate selective packet drop attack and establishing the secure path in Ad-hoc network. The methodology depends on the throughput of the system. At the point when the throughput of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and recognize the malicious node. The technique is to detect packet drop attack in wireless Ad-hoc Network and enhance the efficiency of the network. The basic idea use in the techniques depends on the Key Distribution and Monitoring Mode techniques. The schemes can be divided into two parts:

A. Key Distribution Technique
B. Monitoring Mode Technique

4.1 Key Distribution:

Wireless Ad-hoc Network is made with limited number of nodes. Choose the source and destination from the committed nodes. At that point check for the accessibility for the path between nodes. Whenever path does not exist between the nodes then called the AODV routing protocol and deploy the optimal path between the nodes. The node who takes part in routing will become an active node. Presently start to flood the packets from the source to destination. The attacker on the path who selectively drops sore packets and consequence will be the packet loss in the imparted network. To identify this malicious node, first we need to make the channel secure so the outcome will be no intrusion in the communication.

To establish secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties. The source node become master and destination node become slave, master and slave select their private keys ‘a’, ‘b’ respectively. The master calculates new value “M” from their selected public and private numbers.

$$M= g^{a} \bmod n \qquad (1)$$

The Slave calculates new value “S” from their selected public and private numbers

$$S= g^{b} \bmod n \qquad (2)$$

The Master and slave exchange their calculated “M” and “S” values through intermediate nodes. When Slave receives “M” and Master receives "S” both parties will calculate mode inverse value.

When master receive value “S” from slave and calculate r value “K1” from the received “S” value.

$$K1=S^a \bmod n \qquad (3)$$

Slave receives value “M” from master and calculates new value”K2” from the received “M”

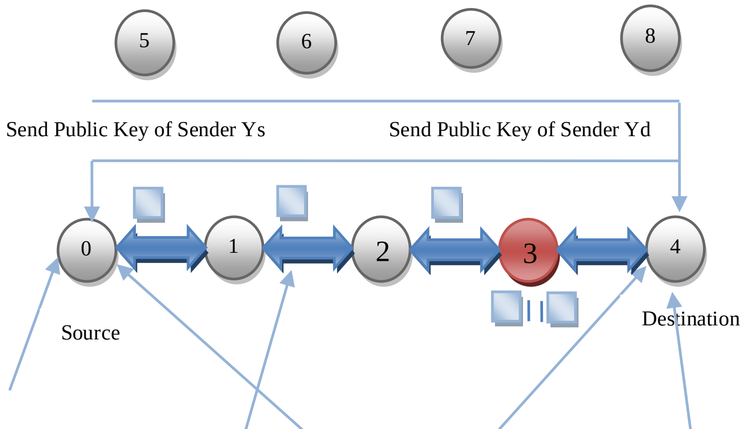
$$K2=M^b \bmod n \qquad (4)$$

After calculating “K1” and “K2”, both parties establish secure channel, by calculated new key “K”. If both communicating parties have same “K1” and “K2” values, secure channel is established between Master and Slave.

$$K=K1+K2 \qquad (5)$$

When secure channel is established between master and slave, communication starts between both parties. The communication between Master and Slave is encrypted with public keys. Each parties use their own private keys to decrypt the communication.

In this research paper apply Key Distribution Technique (Diffie-Hellman Algorithm) on both sender and receiver to make secure channel. Now source sends private key “A” to the destination and when destination receive it, also send “B” to the source. When packet reaches to malicious node it does not have key “B”. Then this path will not be established due to present of malicious node.



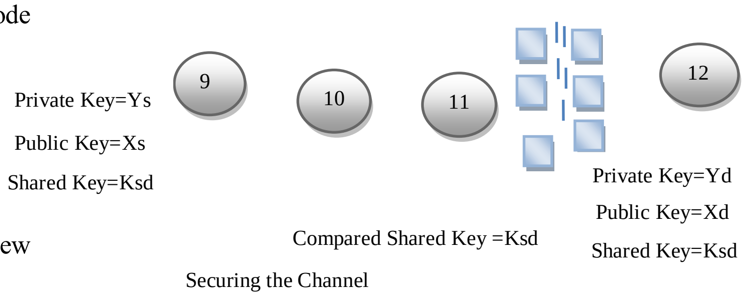


Figure-3 Key Distribution

4.2 Monitoring Mode:

Whenever the source flood the ICMP messages all the nodes in the network separated from node who are taken part in the routing become a passive node. These passive nodes commence monitoring to one hop node, which is use for routing. Each monitoring node send request to node which is on path. If the replay did not comes in particular time stamp it considered as malicious node and all the data about malicious node is send to the source node [18,19]. Source node prepared its as malicious node and initiates the new path for destination and secures it by Diffie – Hellman.

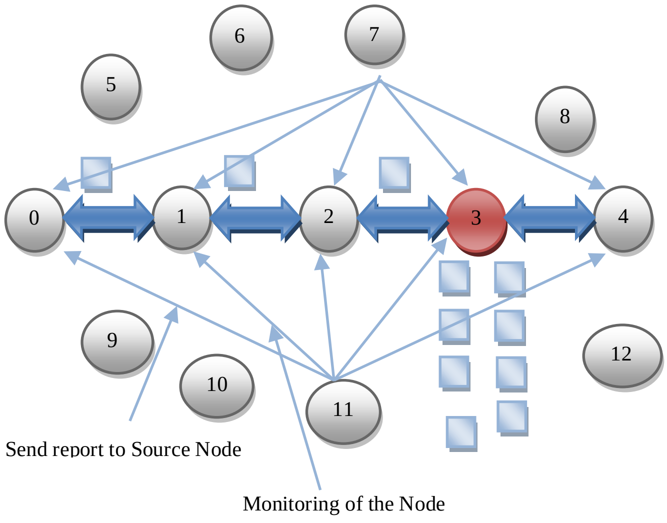


Figure-4 Monitoring Mode

In this way, malicious node will be detected and isolated from the network and secure route is established between source and destination.

V. SIMULATION RESULTS

With the help of Network Simulation (NS-2) we generated the network with 24 nodes as for the Selective Packet drop attack in formal AODV. A UDP is used to create connection between source and destination. With the help of Constant Bit Rate (CBR) traffic is generated.

The simulation has been taken out in NS-2 tool and the parameters used for the validation are discussed below:

S.No.	Parameters	Settings
1.	Terrain Area	800 m x 800 m
2.	Simulation Time	14 s
3.	MAC Type	802.11
4.	Application Traffic	CBR
5.	Routing Protocol	AODV
6.	Data Payload	1000Bytes/Packet
7.	Pause Time	2.0 s
8.	Number of Nodes	23
9.	Number of Sources	1
10.	No. of Adversaries	1 to 3

Table-1 Key Parameters of Simulation

5.1 Delay: The delay is used to transmit data from source to destination with respect to time. The delay graph shows that packets are broadcast within the network then number of packets can be dropped at particular time interval which is responsible for delay in the network. The x-axis shows the simulation time and y-axis the no. of packets.

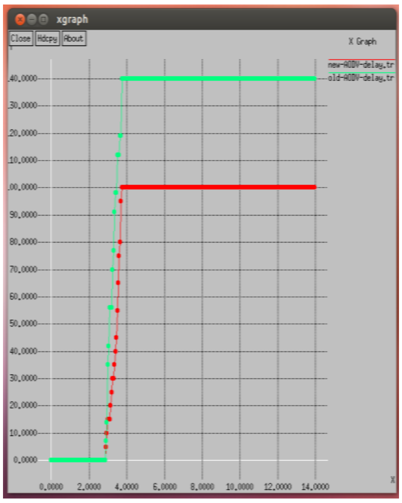


Figure-5 Comparison of Delay Graph

Fig.5 shows the variation in end-to end delay after deployment of the KDAM technique. It demonstrates that KDAM schema reduce end-to-end delay when packet is going to transmit from source to destination. In the preceding schema, the delay begins instantly increasing when there is region of malicious node in the path check as green line whereas without malicious node delay decreases that mark as red line.

2. Packet Loss: The graph shows the packet loss. The packet loss demeans an overall functioning of the network. This graph shows that how many packets can be loss at the particular time interval. The x-axis shows the simulation time and y-axis the no. of packets.

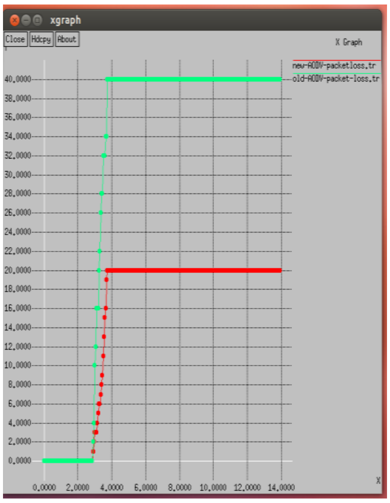


Figure-6 Comparison of Packet Loss Graph

As we have applied Key Distribution and Monitoring (KDAM) technique for setting up the path then packet loss is less when compared with the previous scenario. We make the secure channel so that the final results comes is minimization of packet loss. In former schema, malicious node ceaselessly dropping the packet so that the yield is significant loss of packet. In Fig.6 we see that the green line is persistently increased due to dropping of the packet and the red line is steady after some time on account of securing of channel.

5.3. Throughput: The shows the total amount of data a receiver receives from the sender. This graph shows that number of packets can be received by the destination within a particular time interval. The x-axis shows the simulation time and y-axis the no. of packets.

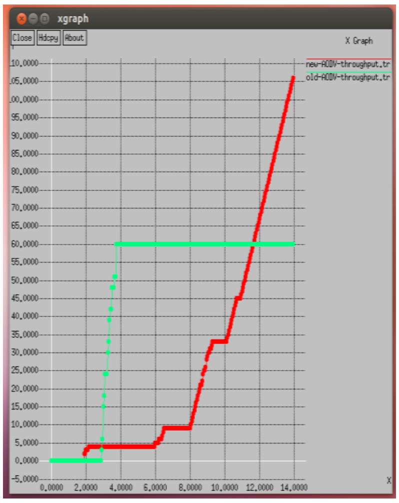


Figure-7 Comparison of Throughput Graph

Fig.7 represents the throughput after utilizing KDAM method. As delay in the network is minimal because of the isolation of malicious node, so throughput of the network is linearly expanded. From graph we can see that when number of packet increase throughput is step by step increment with time in KDAM Schema shown by red line. While green line symbolizes the past schema at whatever point malicious node is available in the network around then packet predictable drop so the line is firm for some period of time.

S.No.	Metrics	Without technique	With KDAM Technique
1.	Delay	140	100
2.	Throughput	60	107
3.	Packet loss	40	20

Table-2 Simulation at Different Metrics

Table 2 exemplifies the delay and packet loss initiates linearly increasing when there is presence of malicious node in the network. At that point when the malicious node present in the network around then packets are consistently dropping so that the throughput of the network decreases. In the wake of applying proposed strategy, delay and packet loss in the network gets to be least as a result of isolation of malicious node, so throughput of the network is straightly increased.

VI. CONCLUSION AND FUTURE SCOPE

Wireless Ad-hoc Network has been huge domain of research work from late years since its extensively utilized application in battlefield and business purpose. Because of openness and dynamic topology network is weakened from attacker. The study pores on Selective Packet Drop Attack applying AODV protocol. In the past studies, distinctive strategies to identify and isolate Selective Packet Drop Attack which keep down the performance by decreasing latency, throughput and increasing end-to-end delay. In this research work, proposed two network layer strategies Key Distribution and Monitor Mode. The technique detects the malicious node from routing path in the network so at any point new route build up and it would free from malicious node then the outcome will be raised by throughput increases and minimize delay and packet loss.

We would proceed with our future work in the accompanying ways: Make further change in the acknowledgement what's more Key Distribution method posted in this research and take other determine component for our method. Thorough performance evaluation will be directed in the light of multiple packet drop attack.

VII. REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE, Volume 40, Number 10, 2002, pp 70-75.

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.

[3] LathaTamilselvan and V Sankarnarayana, "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp. 13-20.

[4] N.Bhalaji and Dr.A.Shanmugam, "Reliable Routing against Selective Packet DropAttack in DSR based MANET", Journal of Software, Vol. 4, Number 6, August 2009, pp. 536-543.

[5] Pradip M. Jawandhiya, Mangesh M. Ghonge "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), 2010, pp. 4063-4071.

[6] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, 2011, pp. 107-117.

[7] Priyanka Goyal, Vintra Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering &Management, Vol. 11, January 2011, pp. 32-37.

[8] Ahmed M.Abd EL-Haleem and Ihab A. Ali, "TRIDNT: The Trust-Based Routing Protocol with Controlled Degree of Node Selfishness for MANET", IJNSA, Volume-3, May 2011, pp.189-203.

[9] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar," End to End Delay Analysis of Prominent On-demand Routing Protocols", International Journal of Computer Science and Technology IJCST,Vol. 2, Issue 1, March 2011,pp.42-46.

[10] H.-M. Sun, C.-H. Chen, and Y.-F. Ku, "A novel acknowledgment based approach against collude attacks in MANET," Expert Systems with Applications, vol. 39, July 2012,pp.7968-7975.

[11] S. Sharmila and G. Umamaheswari, "Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 –8887) Volume 39– No.4, February 2012.

[12] A.Baayer, N.Enneya and M.Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETS", Journal of Information Security (JIS), Vol.3, 2012, pp. 224-230.

[13] (2012, 17 May). The Network Simulator - ns-2. Available: http://www.isi.edu/nsnam/ns/.

[14] G.Dini and A. Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," Ad Hoc Networks, Vol.10, 15 March 2012, pp. 1167-1178.

[15] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala," A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, pp.498-500.

[16] Rajendra Aaseri, Pankaj Choudhary, Nirmal Roberts,"Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless AD-HOC Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013,pp.99-111.

[17] S.Feslinanish Mon, Raj Kumar Shah, L.Rajaji, "A Progression Based Method for the Detection of Black and Gray Hole Attacks in MANET", IJCNWMC, Volume 3, Issue 3, August 2013, pp. 33-40.

[18] Thongchi Chuachan and Somnuk Puangpronpitag, "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANET", IEEE, 2013, pp. 173-177.

[19] Suneth Namal, Konstantinos Georgantas and Andrei Gurtov, "Lightweight authentication and key management on 802.11 with eliptic curve cryptography", IEEE Wireless communication and Networking conference(WCNC), 2013,vol. 48, no. 5, pp.1830-1835.

[20] M.Mohanapriya, Ilango Krishnamurti, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering, Vol.4, February 2013,pp 530-538.

[21] K.Sangeetha, "Secure Data Transmission in MANETS Using AODV", IJCCER, Volume-2, Issue 1, January 2014, pp. 17-22.

[22] Apurva Jain and Anshul Shrotriya," Prevention of Black Hole Attack on MANET Using Trust Based Algorithm", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014,pp.408-413.

[23] Kennedy Edemacu , Martin Euku and Richard Ssekibuule,"Packet Drop Attack Detection Techniques in Wireless Ad-hoc Networks: A Review", International Journal of Network

Security & Its Applications (IJNSA), Vol.6, No.5, September 2014,pp.75-86.

[24] P. Peethambaran and J. S. Jayasudha, “Survey Of Manet Misbehaviour Detection Approaches”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.