A Novel Statistical Adhoc On-Demand Distance Vector Routing Protocol technique is using for preventing the Mobile Adhoc Network from Flooding Attack

Gurpreet Singh[1] and Ganpat Joshi[2]
1 Research Scholar, Department of Computer Science and Engineering, Madhav University, Abu Road, Sirohi, Rajasthan, India; E-mail- see_gurpeet@yahoo.com
2 Associate Professor, Department of Computer Science and Engineering, Madhav University, Abu Road, Sirohi, Rajasthan, India; E-mail- shiv.joshi322@gmail.com
Corresponding author's email – see_gurpreet@yahoo.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract
The Mobile Adhoc Networks are more vulnerable because in the (MANET) Mobile Adhoc Network all node works as data sink, transmitter, router. There is no centralized system in the Mobile Adhoc network, so the chances of the vulnerabilities are very high in the network. There are various security issues in the Mobile Adhoc Network. From the various attacks the flooding attacks are most difficult attacks that extremely affect in Mobile Adhoc Network. In this paper, a new statistical based technique is planned, which is used to discover the flooding attack in an positive approach than other approaches. In the planned of Statistical Ad-Hoc on Demand Distance Vector (SAODV) approach is used to detect malicious nodes in the Mobile Adhoc Network. In this technique, statistical threshold value is obtained from mean and variance. In this approach the value is utilize to locate the (RREQ) Route Request flooding attacker nodes in the Mobile Adhoc Network. The proposed method is capable because threshold values are calculated on the source of RREQs prepared by every node in the Mobile Addhoc Network. The simulation results clearly depict that the proposed approach has significant performance in the terms of throughput, delay, packet delivery ratio, and overhead.

Keywords
Flooding Attack, Mobile Adhoc Network, vulnerabilities, Security.

1. Introduction

MANET (Mobile Adhoc Network) is the wireless Network. In Manet there is not fixed infrastructure all devices are used without any support of it. In the MANET all devices are organized together in randomly. All devices communicate with each other at wireless link. When devices are communicate to each other it can change their network topologies are rapidly. In the MANET when devices or any nodes are used they will connected with the different fixed infrastructure with the radio rage. The devices are moved to one network link to another network link very fast. So MANET has big challenge of security. In the MANET the devices are workin multi hope routing. To transferring link from network to network the topologies are highly changed due this reason the link of devices constantly changes. All devices move out and into to

the radio range. Due to this process the information of routing is changed very soon. In MANET the data delivering and finding the topologies execute by the devices themselves. So these reason the MANET (wireless) is more weak the guided network. The threats are coming from inside the network. MANET has following vulnerabilities [1, 3].

- Limited Resources
- Dynamic topology
- Fixed Bandwidth
- No fixed Boundary
- Not centralized node
- Narrow power supply
- Attackers in the networks

Figure 1: MANET

There are various attacks who disturb the MANET because in MANET using dynamic topologies, there is no central computer system to handle, no perfect algorithm mange the network. The various attacks are disturb the different layers. The following attacks in MANET.

MANET ATTACKS :

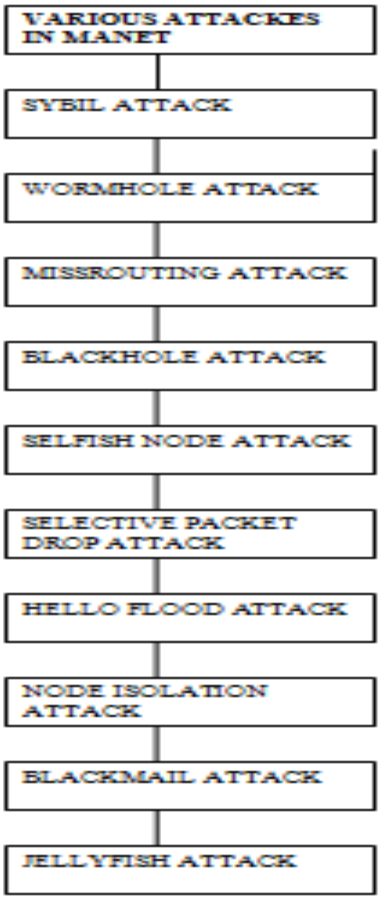

Figure 2: different attacks

The MANET has dynamic topology, uncovered medium, decentralized system, absence of strong protection mechanism and not any cooperative algorithm it is suffer from security attacks. Numerous attacks on the different MANET layers are presented in figure 2.

1.1Flooding Attack

In Flooding attack means one node is sending packets to the other nodes. That node is not a valid node or legal in the Mobile Adhoc Network. This illegal node is sending the packets to any legal node and breaks the security of MANET. It simply re-broadcast overhead packets with enough power to be received by every other node in the network. This Flooding attack uses packets as a weapon to convince MANET. In Flooding attack an attacker use a high radio transmission range and processing power sends packets to a lot of Mobile Adhoc Network nodes which are dispersed in a large area within a Mobile Adhoc Network.[2**]**The flooding attack can easily be launched by an attacker node, but this attack causes the most damage to the MANET. This attack can be implemented by using the excess of RREQs (Route Requests) or data flooding. In RREQ flooding attack, the malicious node floods the RREQs in the network, which results in consuming a lot of network resources. This attack is

launched by selecting IP addresses which do not exist in the MANET and due to this, no node is able to reply RREP (Route Reply) packets against these flooded RREQs. In data flooding attack, the malicious node establishes various paths with the number of nodes in the network. Once paths get established, the malicious node starts transferring a large number of useless data packets r to decrease the performance of the MANET. These large numbers of data packets make congestion in the MANET. The motive of flooding attack is to degrade the performance of the network by exhausting various network resources.

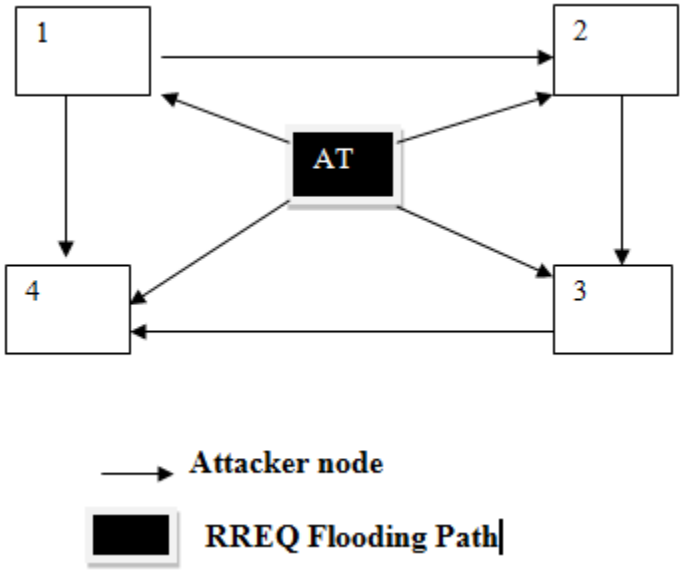

Figure : 3

2 . Literature Review

In this section we discuss the previous approaches which are deliberate for preventing and detecting from flooding attacks. These approaches are good for this attacks but no one is perfect so we study these approaches and evaluate the different weakness of the existing approaches.

Abdulai, Ould-Khaoua & Mackenzie (2009) recommended two new probabilistic methods that employ simple flooding method. In the proposed method, a mobile node takes the responsibility of broadcasting received RREQ packets. The broadcasting process continues until it discovers a route to destination. Continuous broadcasting leads to contention of high channel, duplicate retransmissions, thus causing too much packet clashes in the MANET. The proposed method equipped AODV with a suitable probabilistic route finding technique which showed significant performance improvement by minimal end-to-end delay, achieving good throughput and reduced routing overhead, MAC collision.[4]

Jiang, Lin & Wu (2014) demonstrated that MANETs are unsafe from flooding attack done by cooperative nodes since the network is organized without any centralized coordinator. If the source node wants to transmit data, RREQ is disseminated to all of its neighbors. If the flooding

attack is launched by the intruder node enters with IP address as its destination address, then it tries to flood huge number of packets into the network. The intermediate nodes perform forwarding process lead to process resources and consumption of power. In the planned technique, duplicate RREQ packets are suppressed depending on the cooperation of neighbor nodes and destination and inside one hop distance of the intruder node. The place net design has been incorporated to model the planned technique and registers the entire processing aspects of a system for a quantitative and more concise analysis. The relevant simulations were conducted for quantitative analysis using NS-2 simulator. The proposed energy saving method has experimentally proven to extend the lifetime of MANET under flooding attack[5]

Ms Monika Y. Dangore**,** MANET (Mobile Adhoc Network) is the wireless Network. In Manet there is not fixed infrastructure all devices are used without any support of it. In the MANET all devices are organized together in randomly. All devices communicate with each other at wireless link. AODV (Ad-hoc On-demand Distance Vector) is individual starting environment of mobile devices. The performance of MANET are compared in throughput, average end to end delay and packet delivery ratio [6].

Madhavi & Duraiswamy (2013) recommended solutions for hello flooding attack. Due to this attack, the neighbor nodes could not process other packets, resulting in the deterioration of total networking performance due to the legitimate node‘s diversified behavior. At the end of that the adjacent device has drop down is made due to the absence of hello packet. Hence the intermediate adjacent device transmit RERR message and the route find process is again start by the source node. The hello interval values are switch randomly and it is communicated to extra nodes in a secure way. There are some factors consider like delay, throughput and packet delivery[7].

Virendra Pal Singh, Sweta Jain, and Jyoti Singhai in their paper entitled “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks,” propose a solution for detection of hello flood attack. Authors make some primary assumption and provide an algorithm for hello flood attack prevention. In this method author gives us two concept like puzzles method and signal strength. All nodes are used in same radio range. All nodes get hello packet is called radio range strength. if the packets are not same then it call “stranger” otherwise it called “friends”. When any node identify “stranger” then use the puzzle algorithm. But when number of packets sent any node it is not possible to solve puzzle algorithm[8].

Keecheon Kim**,** the author introduced the Secure Rout Discovery AOD protocol to prevent the black hole attacks. It establish a connection between receiving node and sending node and check the Route reply and Route Request packets which are depends on the threshold value [9].

Geetha K. et al. in this approach the author planned a game theory technique the game theory to prevent the Mobile Adhoc Network from flooding attack. This technique is preventing the Mobile Adhoc Network from malicious nodes, which are answerable for needless delays. By using this technique, performance of the Mobile Adhoc Network is improved packet delay and throughput.[10]

Anchit B. et al. In this technique the author used the investigation of different bot flooding attacks. The various bot flooding attacks guide to Distributed Denial of Services (DDOS). Denial of service attacks are investigation by utilizing user datagram protocol. In this paper the author using simulation results, which represent the performance of the Mobile Adhoc Network with and without (DOS) denial of service attacks.[11]

Song, J. et al in this paper the author preventing Mobile Adhoc Network to using a novel filtering scheme against RREQ flooding attack. The two different threshold values are applied to detect malicious nodes. In this paper threshold values indicate the highest limit of RREQs which is used for showing a node as malicious node.[12]

3. Research Gaps

1) There are so many researches in this field but the point of threshold value is not mostly considered in the past research.

2) The mostly researches has done on the basis of filtering based schemes, trust and game theory but some challenges are still pending for the design of efficient approach.

3) A research gap for uncover an capable statistical based method to avoiding the Mobile Adhoc Networks from hello flooding attack under the AODV protocol.

According to our knowledge there is not any technique to prevent the Mobile Adhoc Network from the hello flood attack

4. PROPOSED APPROACH

In this paper we introduce, a novel statistical based technique which protect Mobile Adhoc Network from the flooding attack. In SAODV, the distribution is used as a statistical reason in browsing the node which is disorderly the network by an overload of RREQs. For computing spreading, the variance of RREQs completed by dissimilar nodes in the Mobile Adhoc Network is calculated. This technique is very helpful for detecting and preventing the Mobile Adhoc Networks below the AODV protocol. This algorithm is based on the statistical threshold value. This threshold value depend upon the variance of the RREQs created by many nodes in the MANET and variance of every of RREQs from the mean. According this technique, there are 'n' nodes in the MANET and then x_i stand for the number of RREQs by the exacting node 'i' in the Mobile Adhoc Network where i= 1,2,3,…… n. The mean of every of the RREQs created by 'n' dissimilar nodes is computed as

$$Mean\ of\ Route\ Requests\ (MRREQ) = \sum_{i=1}^{n} \frac{x_i}{n}$$

After computing the mean, further is to compute the variance of RREQs created by every node in the Mobile Adhoc Network. The variance of all route requests from the nodes from x_1, x_2, x_3,x_4,.....x_n is calculated as

$$Variance^2 = \frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}$$

$$Variance = \sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}}$$

After that computing the variance is to describe various threshold value for find flooding attacker malicious nodes in the MANET. This value is called as STV and will be obtained from mean and variance values as

$$STV = 2 * \sum_{i=1}^{n}\frac{x_i}{n} * \frac{\sum_{i=1}^{n}\frac{x_i}{n}}{\sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}} + 1}$$

The STV is the threshold value, which is employed to find the malicious node in the MANET. As $x_1, x_2, x_3, x_4, \ldots\ldots\ldots\ldots x_n$ represent the whole number of RREQs created by dissimilar n nodes in the mobile adhoc network, Now test for each x_i where i=1, 2, 3,…….. n whether $x_i > STV$ or not. If the cost of $x_i > STV$ is true, then it represents the node $'i'$ is transferring false RREQs in the mobile adhoc network to reduce the performance. After finding the node as a malicious node, a packet will be broadcasted on the mobile adhoc network to separate that particular node from the mobile adhoc network. This method is repeated for each node in the mobile adhoc network, that is distributing RREQs to various destinations. The malicious nodes are efficiently separate from the mobile adhoc network. This algorithm for the planned statistical and threshold based method.

5. Algorithm

Step 1: Start

Step 2: Calculate the number of RREQs from each node in the network and store these values in the variables as $x_1, x_2, x_3, x_4, \ldots\ldots\ldots\ldots, x_n$ by increasing the source node counter as x_i++

Step 3: Find out the mean of the RREQs in the whole network as

$$MRREQ = \sum_{i=1}^{n}\frac{x_i}{n}$$

Step 4: Calculate the Variance of the RREQs by the various nodes requesting the route in the network, for calculating the Variance

$$Variance^2 = \frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}$$

$$Variance = \sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}}$$

Step 5: Calculate Statistical Threshold Value (STV) as

$$STV = 2 * \sum_{i=1}^{n} \frac{x_i}{n} * \frac{\sum_{i=1}^{n} \frac{x_i}{n}}{\sqrt[2]{\frac{\sum_{i=1}^{n}(x_i - MRREQ)^2}{n-1}} + 1}$$

Step 6: For any node x_i where i=1, 2, 3,……, n

If $x_i > STV$ then move to step 7 else go to step 8

Step 7: Drop RREQs from the node i, declare this node as a malicious node which is launching a flooding attack on the network.

Step 8: End

In this algorithm, each node is scanned for detecting attacker node in the network. As the value of variance is calculated on the basis of the deviation of RREQs made by each node in the network, so this method of isolating malicious node is more efficient than other statistical and threshold based techniques used for detecting flooding attacker malicious nodes in MANET.

6. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

In this part, we use AODV protocol in the NS simulator to check the performance of the purposed mechanism, The different parameters employ for simulation are show in the following table 1.

Table 1: List of different parameters

PARAMETERS	VALUE
Protocol	AODV
Simulator	MATLAB
No.of nodes	10
Size of packets	512
Mac layer	IEEE 802.11
Transmission rage (meters)	260
Area of simulation (meters)	800 by 800
Traffic pattern contant bit rate	(CRB)

This technique is planned the statistical method is employ for detect and prevent the flooding attack in Mobile Adhoc Network by using simulation. Diagram 1 stand for the separation of flooding attacker node after execution of SAODV. After implementing SAODV the various parameters it measured the performance of the MANET. The outcome represent the better performance of MANET after eliminate the flooding attacker nodes.

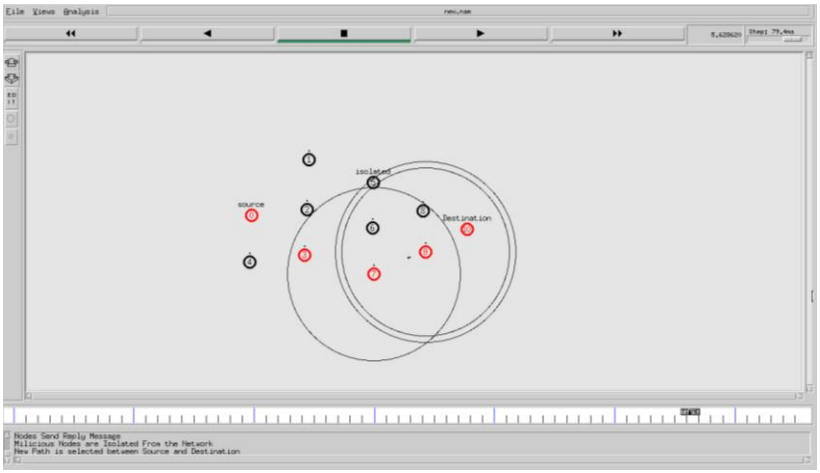

Diagram 1: Isolation of the RREQ flooding attacker node in MANETs

6.1 Overhead

Overhead is the spare time required by the Mobile Adhoc Network for sending the data packets from sending node to the receiving node. Diagram 2 show the reduced overhead after executing the planned technique.

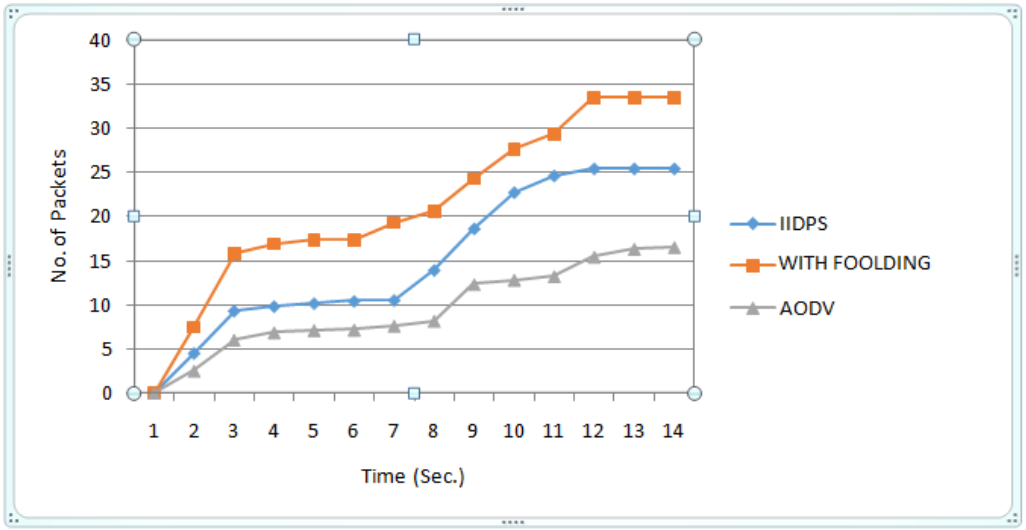

Figure 2: Improvement of overhead after implementing SAODV

6.2 Packet Delivery Ratio

The packets are accepted at the receiving to the packet created at source node is called Packet Delivery Ratio. Following the PDR computed

$$PDR = \frac{\text{Packets reached at the destination}}{\text{packets produced at the source}} \times 100$$

The following diagram 3 stand for the enhanced the performance of PDR of the Mobile Adhoc Network after separation of flooding attacker nodes.

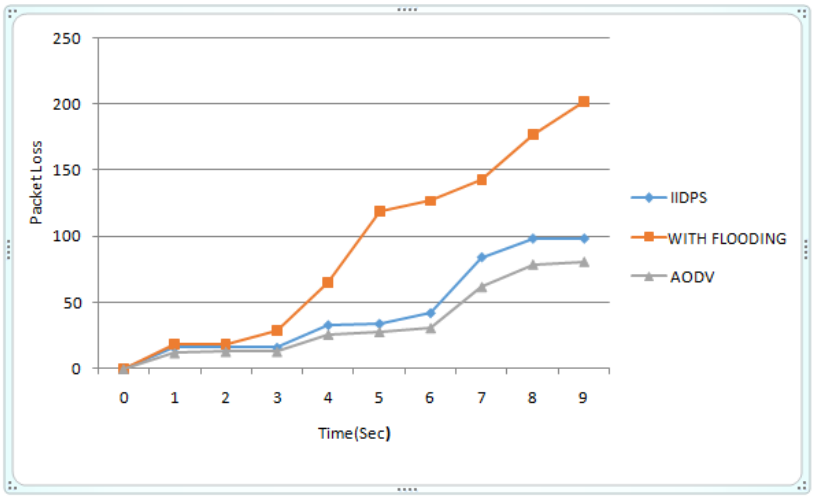

Diagram 3: Improvement of PDR after implementing SAODV

6.3 End-to-End Delay

End-to-End delay calculated as the entire time used between the message made at the source node to appear of the data packet at the receiving node. The diagram4 show the enhanced performance of the MANET in the terms of end-to-end delay.

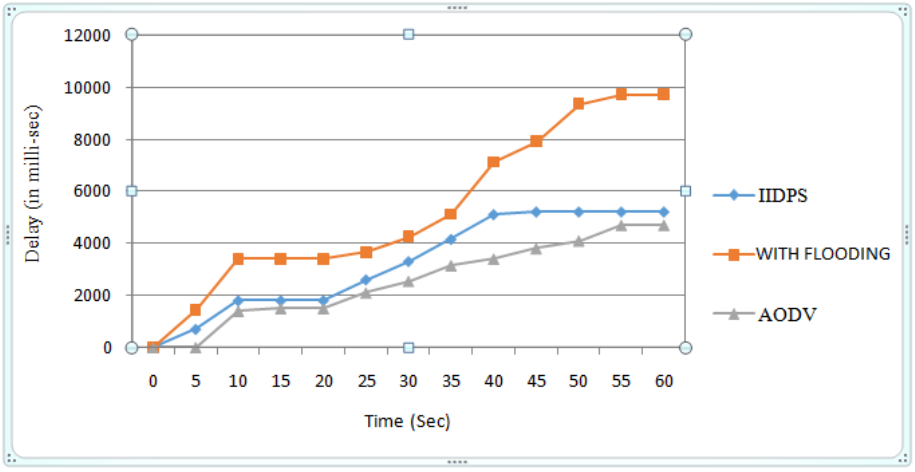

Figure 4: Improvement of end-to-end delay after implementing SAODV

6.4 Throughput

In this section, we use the throughput parameters, which is the main parameter for calculating the performance of Mobile Adhoc Network. It is calculated as the rate of sending packets per unit of time. The diagram 5 shows the enhanced throughput of the Mobile Adhoc Network after separation of flooding malicious nodes.

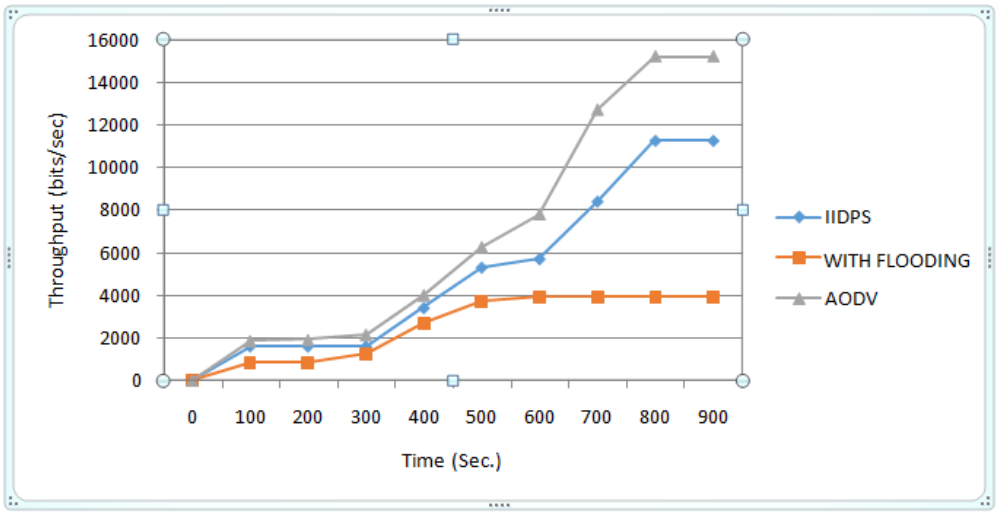

Figure 5: Improvement of throughput after implementing SAODV

In this section we see the experiments from the different parameters that shows the enhanced the performance of the Mobile Adhoc Network.

7. Conclusion and Future Work

In this paper we discuss a algorithm SAODV, which is used for preventing the Mobile Adhoc Network against RREQ flooding attacker nodes. The algorithm applied for detecting and preventing the Mobile Adhoc Network from malicious nodes is more capable because it based on the behavior of all node in the Mobile Adhoc Network. The major characteristic of this algorithm is that it is the grouping of statistical methods along with the threshold values. This threshold values are define on the source of mean and variance as statistical factors. The SAODV algorithm is very good algorithm for solving inbuilt vulnerability against RREQ flooding attack. The result of the simulation is showed that the planned algorithm is best in the case of different parameters like Throughput,Overhead, End-to- End Delay and Packet Delivery Ratio,. The SAODV algorithm is answerable for damage the consequence of the RREQ flooding attack in Mobile Adhoc Network. This algorithm can be continued by utilizing data mining methods for various other attacks in Mobile Adhoc Network.

References

[1] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", "International Journal of Multidisciplinary and Current Research", Volume 2, Jan-Feb, 2014, ISSN: 2321-3124.

[2] Jatinder Singh, Lakhwinder Kaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", International Arab Journal of Information Technology, Volume 9, No. 3, May 2012 and ISSN: 1683-3198.

[3] Jianga, F., Lina, C., and Wub, H., "Lifetime Elongation of Ad Hoc Networks under Flooding Attack using Power-saving Technique", Ad Hoc Networks, Elsevier, Vol. 21, pp. 84-96, 2014.

[4] J. Abdulai is with the Department of Computing Science, University of Glasgow. Glasgow, G12 8RZ, UK. (+44-141-330-1637); (e-mail: jamal@ dcs.gla.ac.uk).

[5] fuu-Cheng jiang " Department of computer science, Tunghai university, no.1727, sect. 4, Taiwan Boulevard, Taichung 40704, Taiwan.

[6] Ms Monika Y. Dangore and Mr Santosh S. Sambare," Detecting And Overcoming lackhole Attack In manet" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies

[7] Madhavi, S. and Duraiswamy, K. (2012) WAS-DP: Wormhole Attack in SAODV-
Detection and Prevention. European Journal of Scientific Research, 77, 560-569.

[8] Virendra Pal Singh, Sweta Jain, and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010. ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[9] Seryvuth Tan, Keecheon Kim," Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" in 7/2013 IEEE.

[10] Geetha, K., Sreenath, N., "Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol", "Research Article - Computer Engineering And Computer Science", Arab Journal of Science and Engineering, 2015.

[11] Anchit, B., Harvinder, S., "Investigation of UDP Bot Flooding Attack", Indian Journal of Science and Technology, ISSN 0974-5645, vol. 9, issue 21, 2016.

[12] Jian-Hua Song, Fan Hong, Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", IEEE Computer Society 2006.

[13] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", "Elsevier Journal of Computer Communications", Volume 34, Issue 1, January 2011.

[14] Jangir, S., Hemrajani, N. "Evaluation of Black hole, Wormhole, and Sybil Attacks in Mobile Ad-hoc Networks", Proceedings of Second International Conference on Information and Communication Technology for Competitive Strategies, Article No. 74, 2016.

[15] Cervera, G., Barbeau, M., Alfaro, J., Kranakis, E., "A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs", Journal of Network and Computer Applications, Elsevier, Vol.36, Issue 2, March 2013.

[16] Jaehak Yu, Hyunjoong Kang, DaeHeon Park, Hyo-Chan Bang, Do Wook Kang, "Elsevier Journal of Systems Architecture", "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques", Volume 59, 2013.

[17] IJIRST –International Journal for Innovative Research in Science & Technology| Volume 3 | Issue 02 | July 2016 ISSN (online): 2349-6010 All rights reserved by www.ijirst.org 133 Review on Hello Flood Attack in Wireless Sensor Networks

[18] Patidar, D., Dubey, J. "A Hybrid Approach for Dynamic Intrusion Detection, Enhancement of Performance and Security in MANET", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Article no. 81, 2016.

[19] Jatinder Singh, Lakhwinder Kaur, and Savita Gupta, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless Local Area Network (WLAN)", "International Journal of Computer Science and Information Security (IJCSIS)", Vol. 7, No. 1, January 2010, pp. 284-291. ISSN: 1947-5500.

[20] Sukiswo, Rifquddin, M., "Performance of AOMDV Routing Protocol under Rushing and Flooding Attacks in MANET", Proceeding of 2nd International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)", IEEE, 2015.
[21] Yu, J., Kang, J., Park, D., Bang, H., Kang, D. "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques", "Journal of Systems Architecture", "Elsevier", pp. 1005-1012, 2013.
[22] Ms. Neetu Singh Chouhan and Ms. ShwetaYadav, "Flooding Attacks Prevention in MANET", "International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Volume 1, Issue 3, ISSN 2249-6343.
[23] D. SrinivasaRao, Dr. P.V. NageswaraRao, "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network", "International Journal of Applied Engineering Research", Volume 11, 2016, ISSN 0973-4562.
[24] Dhara Buch and Devesh Jinwala, "Prevention of wormhole attack in wireless sensor network," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
[25] J. Abdulai is with the Department of Computing Science, University of Glasgow. Glasgow, G12 8RZ, UK. (+44-141-330-1637); (e-mail: jamal@ dcs.gla.ac.uk).
[26] S.Abbas, M. Merabti and D.Llewellyn-Jones, "Lightweight Sybil Attack Detection in MANETs", IEEE systems journal, vol. 7, no. 2, June 2013 , p fuu-Cheng jiang " Department of computer science, Tunghai university, no.1727, sect. 4, Taiwan Boulevard, Taichung 40704, Taiwan.