Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2457-2470

http://www.ripublication.com

SAODV: Statistical Ad hoc On-Demand Distance Vector Routing Protocol for Preventing Mobile Adhoc Network against Flooding Attack

Opinder Singh*, Dr. Jatinder Singh and Dr. Ravinder Singh****

**Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India.*

***IKG Punjab Technical University, Kapurthala, Punjab, India.*

Abstract

Flooding attack is most challenging security threat in Mobile Adhoc Networks (MANETs). This attack is responsible for reducing the network performance of various routing protocols. In this paper, we will discuss MANETs under the AODV protocol. The existing Flooding attack prevention schemes are not much secure for resistance against flooding attacks. In this article, a new statistical based approach is proposed which can detect the flooding attack in an optimistic manner than other techniques. In the proposed SAODV (Statistical Ad-Hoc on Demand Distance Vector) approach, concept of dispersion is used for detecting malicious nodes in the network. In this technique, statistical threshold value is obtained from mean and mean deviation (Dispersion). This value is used to find out the Route Request (RREQ) flooding attacker nodes in the MANET. The proposed technique is efficient because threshold values are computed on the basis of RREQs made by each node in the 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, Security, Intrusion Detection Systems (IDSs), and vulnerabilities.

1. INTRODUCTION

MANETs are infrastructure less network of mobile computing devices as shown in figure 1. These wireless networks are self-organized. In these networks, mobile devices communicate with each other through bandwidth constrained wireless links. The network topology in MANETs change rapidly over different times. In MANETs, any two nodes can start communicating with each other, if these are within the radio range. The wireless interconnection between various nodes in the mobile networks are highly vulnerable due to dynamic topology.

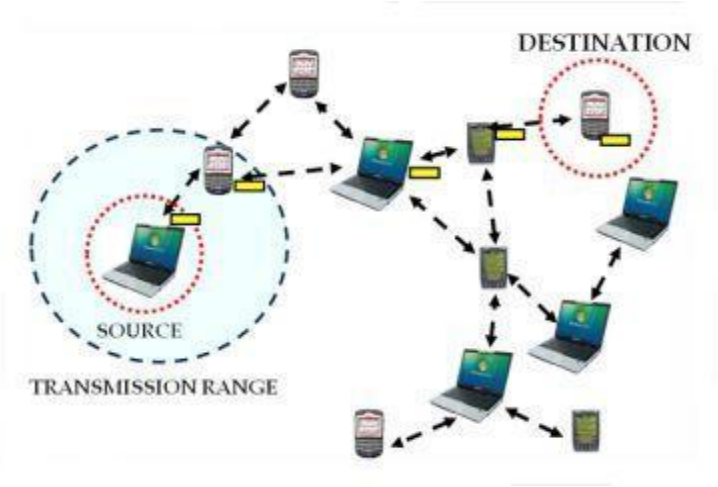

Fig.1. Mobile Ad hoc Network.

MANETs are vulnerable to a large extent as compared to wired networks due to mobile nodes. Due to these vulnerabilities, MANETs are more prone to malicious nodes. The Adhoc networks have various vulnerabilities like scalability, dynamic topology and infrastructure less networks, lack of centralized node, limited resources, and bandwidth constrained. The different attacks at the different layers in MANETs are:

- Black Hole Attack
- Selective Packet Drop Attack
- Flooding Attack
- Byzantine Attack
- Wormhole Attack
- Sybil Attack
- Hello Flood Attack
- Modification Attack

- Jellyfish Attack
- Replay Attack
- Selfish Attack
- Misrouting Attack

Out of various attacks in MANETs, Flooding attack is the most hazardous attack, which is responsible for reducing the network performance by consuming network resources.

1.1 Flooding Attack

This attack is very easy to implement in the network, but it is a most hazardous attack. This type of attack can be implemented by using an excess of route requests or by flooding large amount of data in the network. In this, malicious nodes flood excess of fake route requests in the network to decrease the performance of the network. In Flooding attack, the malicious nodes get into the network and set various paths with different nodes in the network. After establishing different paths in the network, these malicious nodes inject large amounts of RREQs packets for getting paths to different destination nodes. These large amounts of useless data packets congest the network. Due to this, the number of nodes other than the malicious nodes will be busy all of the time while receiving unwanted and useless data packets. The main aim of the flooding attack is to consume and exhaust the network resources. The routing operation is disrupted to a large extent by this attack. The flooding attack is used to degrade the performance of the network, so this attack is most hazardous attack. The RREQs flooding attack is shown in the figure2.

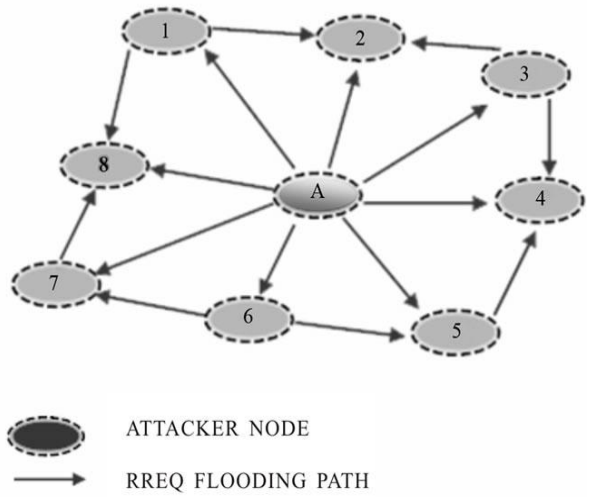

Fig. 2: Flooding Attack by Node A

2. RELATED WORK

The following section contains a comprehensive review of various approaches specially designed for prevention from flooding attack. The main objective of this study is to evaluate various shortcomings of existing techniques.

Geetha K. et al. [1] in their work proposed a technique for preventing the MANETs from flooding attack by using the game theory approach. This approach also prevents the network from malicious nodes, which are responsible for unnecessary delays. By using this approach, performance of the network is enhanced in the terms of packet delay and throughput. Javad M. et al. [2] used a balance index concept for protecting vehicular networks against RREQ flooding attack. The proposed mechanism is known as Balanced AODV. In this approach concept of standard deviation is used for detecting abnormal behavior of malicious nodes in the network. In this method, a node is declared as malicious is it deviates from the predefined threshold. The simulation of the proposed approach represents the improved performance of the VANET in the terms of false positive rate and overhead. Song, J. et al. [3] in their article provides a novel filtering scheme for preventing MANET against RREQ flooding attack. In this mechanism, two different threshold values are used to detect malicious nodes. The threshold values represent the maximum limit of RREQs which can be used for declaring a node as malicious node. Anchit B. et al. [4] presented the analysis of various bot flooding attacks. These bot flooding attacks lead to Distributed Denial of Services (DDOS). In this work, denial of service attacks are analyzed by using user datagram protocol. The simulation results show the performance of the network with and without denial of service attacks. Zhi A. [5] et al. in their work utilized the Route Request Flooding Defense mechanism for mitigating the problem of Route Request Flooding Attack (RRFA). The simulation results show increased packet delivery ratio by reducing Packet delay and overhead.

Sui A. et al. [6] have proposed an effective mechanism for mitigating flooding attack MANET. In this approach, each node in the network is set into some upper route request limit based on the predefined threshold values. If the route request increased from this predefined value, then route requesting node is treated as malicious node and is isolated from the network. The route overhead is reduced by using this approach. Bandyopadhyay et al. [7] provide the study of performance degradation due to presence of flooding attack nodes in the MANET. The whole simulation is done for AODV routing protocol. The results show the degradation in the performance of the network in the terms of packet loss, overhead and bandwidth. Patidar D. et al. [8] provides A Hybrid Approach for Dynamic Intrusion Detection, Enhancement of Performance and Security in MANET. A hybrid approach is given for intrusion detection by removing malicious nodes during the route discovery process. The proposed approach increases the network performance in terms of PDR, throughput, and end to end delay and security also. Chaudhary A. et al. [9] have provide a fuzzy logic based intrusion

detection system for preventing Adhoc network from RREQ flooding attack. This detection mechanism works on the basis of Sugeno-type fuzzy inference system for detecting malicious nodes in the network. The performance of the MANET is increased in the terms of low false positive rates and high true positive rates. Choudhury et al. [10] introduced a reputation based approach for mitigating flooding attack in MANET. In this technique, behavior of each node is observed periodically. If at any time, route requests increased from the predefined limit, then it is declared as malicious node. Cervera et al. [11] demonstrated a novel multipath routing approach to detect a flooding attack in MANETs. This mechanism is used in OLSR protocol to reduce the impact of flooding attack in the network. The simulation results show the improved performance of the MANET.

Verma S. et al. [12] in their paper discussed the technique for investigating the impact of flooding attack on the Quality of services in the network. The various results shown the drastic effect of malicious nodes on the performance of the network. Sukiswo et al. [13] in their work provide a new Ad Hoc On-demand Multipath Distance Vector protocol for tackling with various categories of flooding attack. The simulation results prove the improved performance of the network in the terms of Throughput, Delay, and Packet Delivery Ratio. Kumar S. et al. [14] in their paper discussed the effects of various attacks on the performance of MANETs. The various effects of the malicious nodes on the network are measured under different metrics. The major related issues are also discussed in this survey. Jiang F. et al. [15] proposed a power saving technique for mitigating flooding attack in MANET. A Petri net based model is used to design the new intrusion detection system. The simulation results represent the improved performance of the Adhoc network. Jung J. et al. [16] in their paper provide a new mechanism for tackling with route request flooding attacks in the network. This mechanism is based on Forward Packet Recovery and Backward Packet Recovery methods. In this approach, route request and compensation packets are adjusted dynamically. Laeeq K. [17] et al. have utilized the RFAP (Route Request Flooding Attack Prevention) scheme for preventing the MANETs from flooding attack nodes. This approach protects the MANETs under the AODV protocol. This approach isolates the malicious nodes in a more reliable manner as compared to other approaches. Patel M. [18] et al. in their paper demonstrated a new approach based on AODV protocol metrics for preventing the network against flooding attacks. In this approach, various metrics are used for detecting the malicious nodes in the network. Rmayti et al. [19] in their paper utilized the statistical approach for defending MANETs against RREQ flooding attacks. The simulation results clearly depict that flooding attacks can be effectively detected with low false alarms. Sawant K. et al. [20] introduced a threshold-based mechanism for effectively detecting the presence of DOS flooding attack in the Adhoc network.

Yu J. et al. [21] provide the C 4.5 algorithm for detecting and preventing from flooding attack in MANETs. This algorithm uses the SNMP MIB (Simple Network Management Protocol & Management Information Base) information. The various types of flooding attacks are detected by using data mining approach. After depth analysis of these attacks, the particular attack is detected by the proposed algorithm. Neetu Singh et al. [22] used the distributive approach for protecting the MANETs against flooding attacks. This technique is used to detect new type of attack which is known as AHFA (Adhoc Flooding Attack). This mechanism is based on threshold values. In this technique, all of the nodes can detect the trust value of all of the neighboring nodes based on the threshold values. The results show that the distributive approach can effectively detect the malicious nodes by improving the performance of the network. Srinivasa et al. [23] introduce a new hierarchical cluster based mechanism for avoiding flooding attack in a wireless network. This technique is used to improve the performance of MANET in terms of Packet Delivery Ratio and routing overhead. This mechanism is unique in the terms of adaptability and route security. In this technique, each node is capable of detecting malicious nodes in the network.

3. RESEARCH GAPS

- The most of the past research work is based on preventing the MANETs from flooding attack by using the distributive approach, but very less work is done on the basis of threshold values.
- The lot of previous work has also been done on the basis of game theory, trust, and filtering based schemes, but the design of an efficient approach still remains a challenge.
- There is a research gap for finding an efficient statistical based approach to preventing the MANETs from flooding attack under the AODV protocol.

The efficient technique for preventing MANETs from flooding attack has not been accounted so far according to the authors' knowledge.

4. PROPOSED APPROACH

In order to protect the MANET from flooding attacker malicious nodes, we have proposed a new statistical based approach. In SAODV, dispersion is used as a statistical factor in finding the node which is disrupting the network by an excess of Route Requests (RREQs). For calculating dispersion, the mean deviation of all of the RREQs made by different nodes in the network is calculated. This algorithm is very useful for detecting and preventing the MANETs under the AODV protocol. This mechanism is based on the statistical threshold value (STV). This threshold value is further depends

upon mean of the RREQs made by various nodes in the network and mean deviation of all of these RREQs from the mean. In this algorithm, if there are 'n' nodes in the network and then x_i will represent the number of RREQs by the particular node 'i' in the network where i= 1,2,3,…… n. The mean of all of the RREQs made by 'n' different nodes is calculated as

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

After calculating the mean, the next step is to calculate the mean deviation of RREQs made by each node in the network. This mean deviation (Dispersion) for all of the nodes from $x_1, x_2, x_3, x_4, \ldots\ldots\ldots\ldots x_n$ is calculated as

$$Mean\ Deviation\ of\ Route\ Requests\ (MDRREQ) = \frac{\sum_{i=1}^{n} |x_i - MRREQ|}{n} \ldots\ldots\ldots\ldots (2)$$

The next step after calculating the dispersion is to define some threshold value for detecting flooding attacker malicious node in the network. This value is termed as Statistical Threshold Value (STV) and will be obtained from mean and dispersion value as

$$STV = 2 * \sum_{i=1}^{n} \frac{x_i}{n} * \frac{\sum_{i=1}^{n} \frac{x_i}{n}}{\frac{\sum_{i=1}^{n} |x_i - MRREQ|}{n} + 1} \ldots\ldots\ldots\ldots (3)$$

The STV is the threshold value, which is used to detect the malicious node in the network. As $x_1, x_2, x_3, x_4, \ldots\ldots\ldots\ldots x_n$ represent the total number of route requests made by different n nodes in the network, Now check for each x_i where i=1, 2, 3,…….. n whether $x_i > STV$ or not. If value of $x_i > STV$ is true, then it means the node $'i'$ is sending fake route requests in the network to decrease the performance. After detecting this node as malicious node, a message will be broadcasted on the network to isolate this node from the network. This process is repeated for each node in the network, which is sending route requests to some destination. In this way, malicious nodes are effectively isolated from the MANET. The algorithm for the proposed statistical and threshold based approach is represented as:

Algorithm 1

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 Mean Deviation of the RREQs by the various nodes requesting route in the network for calculating the dispersion

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

Step 5: Calculate Statistical Threshold Value (STV) as

$$STV = 2 * \sum_{i=1}^{n} \frac{x_i}{n} * \frac{\sum_{i=1}^{n} \frac{x_i}{n}}{\frac{\sum_{i=1}^{n}|x_i - MRREQ|}{n} + 1}$$

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 RREQ from the node i, declare this node as 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 dispersion is calculated on the basis of 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 method used for detecting flooding attacker malicious node in MANET.

5. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

For checking the performance of the proposed approach, we simulate the approach by using AODV protocol in the NS 2.3 simulator. The different parameters used for simulation are represented in the Table 1.

Table 1: List of various Parameters

Parameter	Value
Simulator	NS 2.3
Protocol	AODV
Number of Nodes	11
Transmission Range (Meters)	250
Size of Packet (Bytes)	512
MAC Layer	IEEE 802.11
Area of Simulation (Meters)	800 by 800
Simulation Time (Seconds)	60
Channel Type	Wireless
Traffic Pattern	Constant Bit Rate (CBR)

In this simulation, the proposed statistical technique is used for detecting and preventing flooding attack in MANET. After implementation of the proposed technique, the performance of Adhoc network is measured under various parameters. The results clearly represent the improved performance of network after removing flooding attacker nodes.

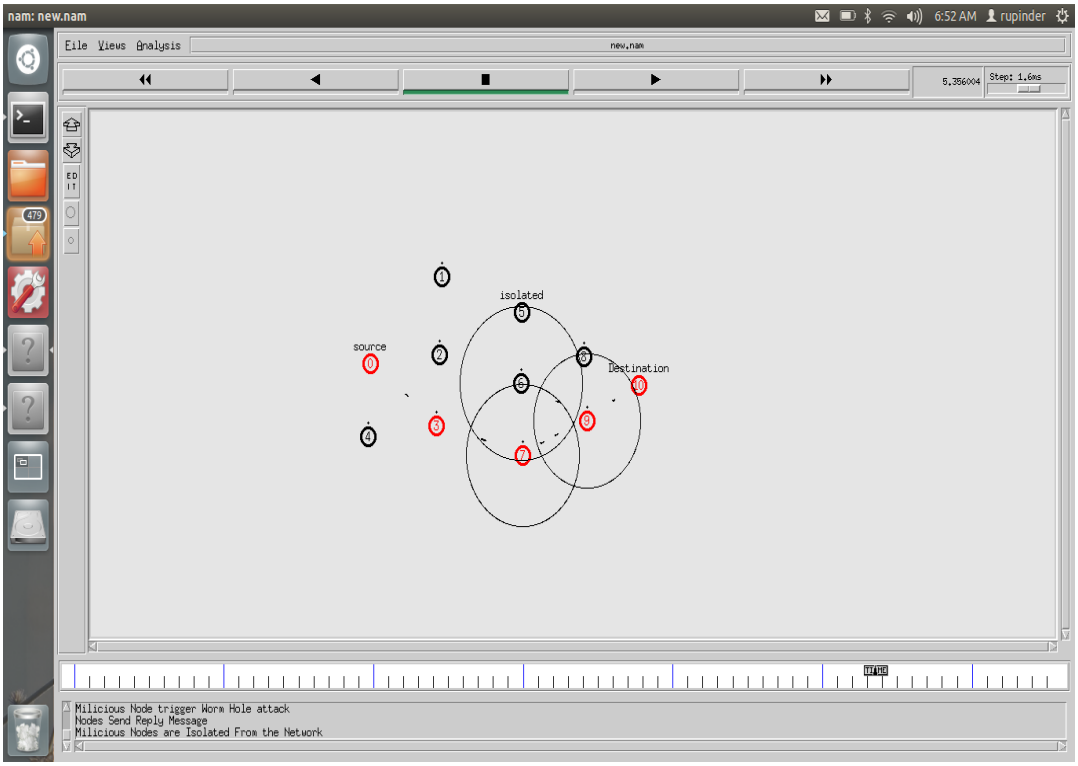

Fig. 3: Isolation of the RREQs flooding attacker node in MANETs

5.1 Packet Delivery Ratio (PDR)

The packet delivery ratio is the ratio of the packets received at the destination to the packets produced at the source node. The Packet delivery ratio can be calculated as:

$$\text{PDR} = \frac{\text{Packets reached at the destination}}{\text{packets produced at the source}} * 100 \ldots\ldots\ldots (4)$$

The following figure 4 represents the improved performance of the MANET after isolation of flooding attacker nodes.

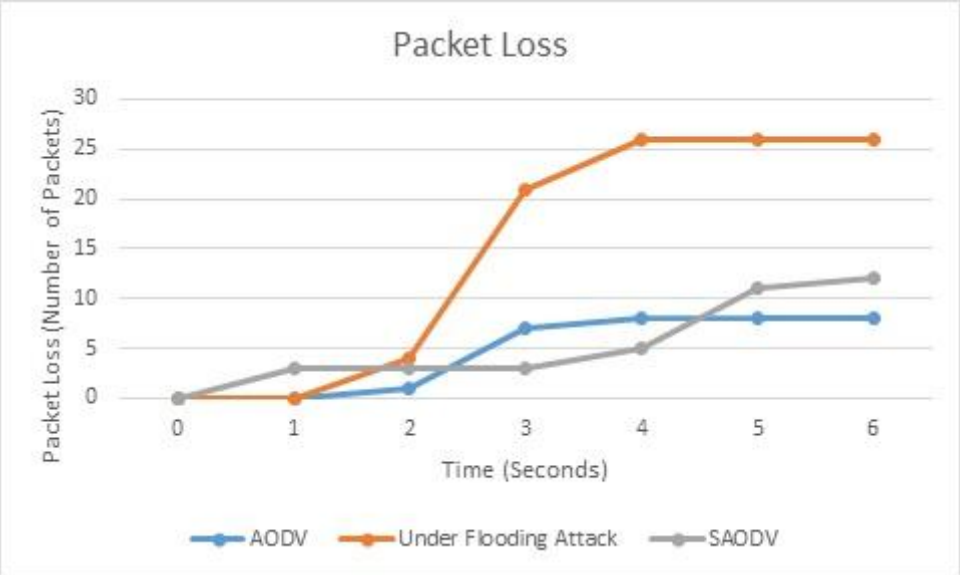

Fig. 4: Improvement of Packet Loss parameter after implementing SAODV

5.2 Throughput

The throughput is the main parameter for estimating the performance of any network. It is measured as the rate of the delivered packets per unit of time. The following figure 5 represents the improved throughput of the MANET after the isolation of malicious nodes.

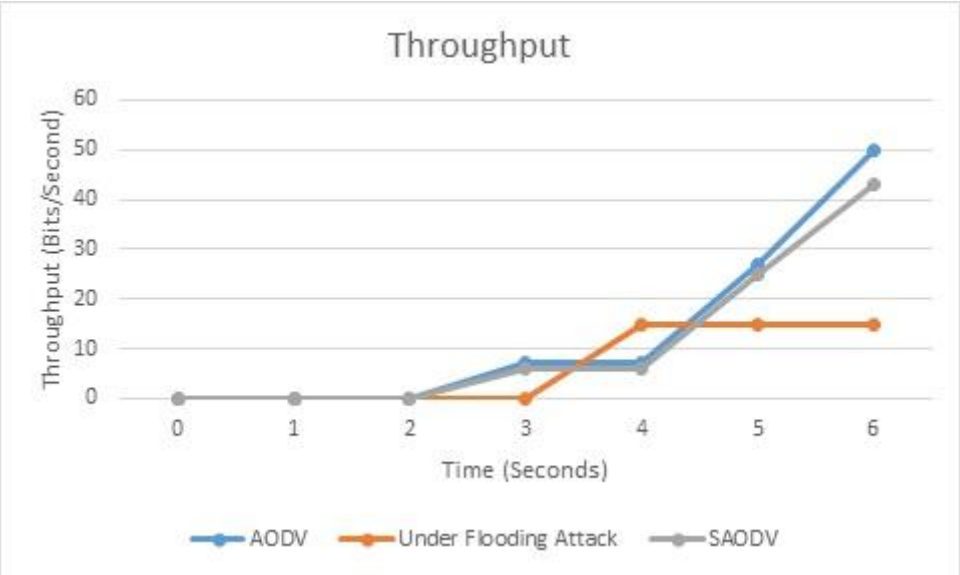

Fig. 5: Improvement of Throughput after implementing SAODV

5.3 Overhead

It is the extra time required by the network for delivering the data packets from source node to the destination node. The figure 6 clearly depicts the decreased overhead after implementing the proposed approach.

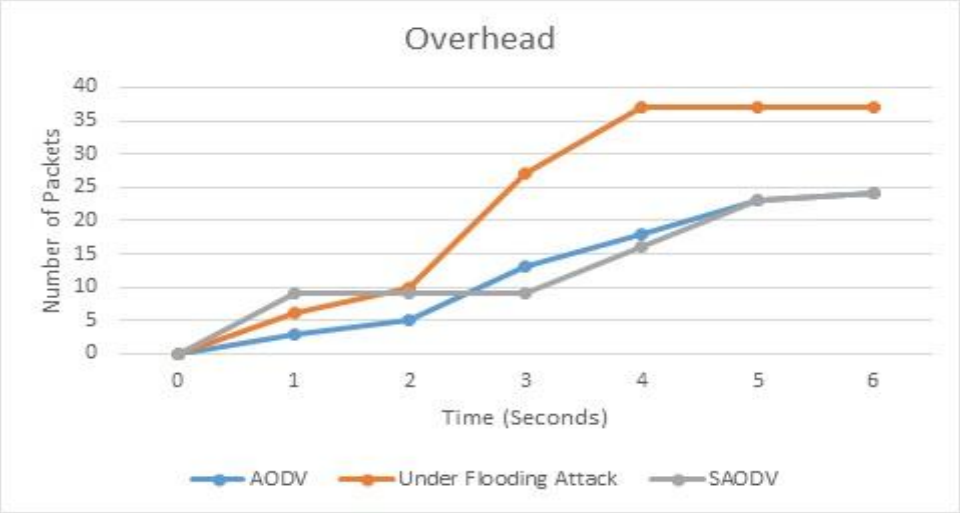

Fig. 6: Improvement of Overhead after implementing SAODV

5.4 End-to-End Delay

It is measured as the total time consumed between the data packet created at the source node to the arrival of data packet at the destination node. The following figure 7 represents the improved performance of the network in the terms of end-to-end delay.

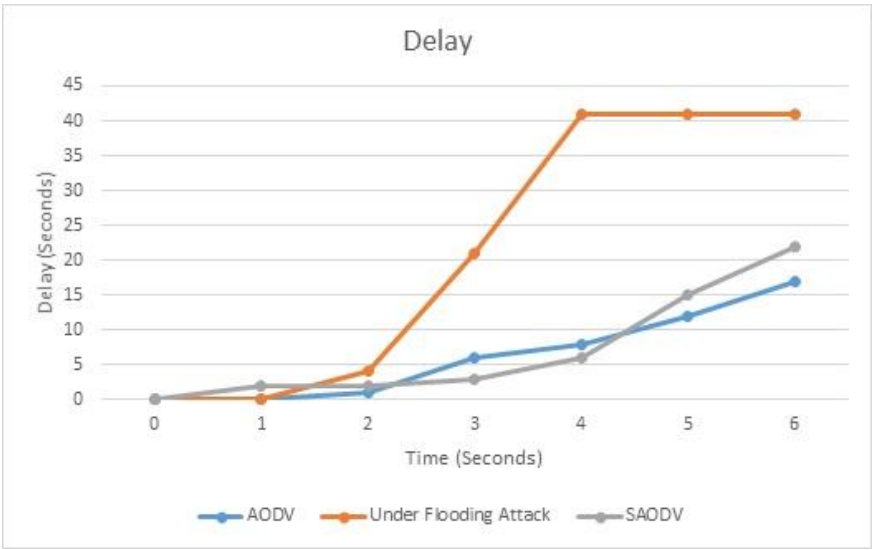

Fig. 7: Improvement of End-to-End Delay after implementing SAODV

The various experiments shown above for different parameters represent the improved performance of the MANET.

6. CONCLUSION AND FUTURE WORK

In this paper, a mechanism SAODV is presented for preventing the MANETs against RREQ flooding attacker nodes. The approach used for detecting and preventing the network from malicious nodes is more efficient because it depends upon the behavior of each node in the network. The main feature of this technique is that it is the combination of statistical methods along with the threshold values. The threshold values are defined on the basis of mean and mean deviation as statistical factors. The SAODV technique is the best technique for resolving inherent vulnerability against RREQ flooding attack. The simulation results proved that the proposed technique is optimal in the case of various parameters like Throughput, End-to- End Delay, Overhead and Packet Delivery Ratio. The SAODV technique is responsible for destroying the effect of the RREQ flooding attack in MANETs. In future, this technique can be extended by using data mining techniques for some other attacks in MANET.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

Conflicts of Interest

The authors declare no conflicts of interest.

REFERENCES

[1] 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.

[2] Faghihniya, M., Hosseini, S., Tahmasebi, M., “Security upgrade against RREQ flooding attack by using balance index on the vehicular ad hoc network”, Journal of Wireless Network, pp. 1-12, 2016.

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

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

[5] Eu, Z., Seah, G., "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", International Conference on Information Networking, Springer, pp. 327-336, 2006.

[6] Sui, A., Guo, D., Zhao, D., "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Information Networking. Advances in Data Communications and Wireless Networks, Springer, pp. 327-336, 2006.

[7] Bandyopadhyay, A., Vuppala, S., Choudhury, P., "A Simulation Analysis of Flooding Attack in MANET using NS-3", 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, IEEE, 2011.

[8] 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.

[9] Chaudhary, A., Kumar, A., "A Novel Intrusion Detection System for Ad Hoc Flooding Attack Using Fuzzy Logic in Mobile AdHoc Networks", "IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)", 2014.

[10] Choudhury, P., Nandi, S., Pal, A., Narayan, C., "Mitigating Route Request Flooding Attack in MANET using Node Reputation", IEEE 10th International Conference on Industrial Informatics, 2012.

[11] 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.

[12] Verma, S., Patel, R., Lenka, S., "Investigating Variable Time Flood Request Impact Over QOS In MANET", 3rd International Conference on Recent Trends in Computing, Procedia Computer Science, Elsevier, Vol. 57, 2015.

[13] 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.

[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] 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.

[16] Jung, J., Kim, Y., Kim, I., "ASTRAL: An Adaptive, Efficient, and Reliable Flooding Mechanism for MANET", Proceedings of the ACM Symposium on Applied Computing, pp. 731-732, 2010.

[17] Laeeq, K., "RFAP, A Preventive Measure against Route Request Flooding Attack in MANETs", 15th International Multitopic Conference (INMIC), IEEE, 2012.

[18] Patel, M., Sharma, S., Sharan, D., "Detection and Prevention of Flooding Attack Using SVM", "International Conference on Communication Systems and Network Technologies", IEEE, 2013.

[19] Rmayti, M., Begrichey, Y., Khatouny, R., Khoukhi, L., Gaiti, D., "Flooding Attacks Detection in MANETs", "International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)", 2015.

[20] Sawant, K., Rawat, M., Jain, A., "Implementation of Energy Aware Secure Routing Protocol over Flooding Environment in MANET", IEEE International Conference on Computer, Communication, and Control, 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. Shweta Yadav, "Flooding Attacks Prevention in MANET", "International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Volume 1, Issue 3, ISSN 2249-6343.

[23] D. Srinivasa Rao, Dr. P.V. Nageswara Rao, "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network", "International Journal of Applied Engineering Research", Volume 11, 2016, ISSN 0973-4562.