IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-1 E-ISSN: 2347-2693

A Learning Automata Based Mechanism to Mitigate Energy Draining Data Flooding Attack in MANETs

Raman Preet[1*], Shaveta Rani[2], Paramjeet Singh[3]

[1*]Dept. of Applied Science (Computer Applications), I.K. Gujral Punjab Technical University, Kapurthala, India
[2]Dept. of CSE, Gaini Zail Singh Campus College of Engineering and Technology, Bathinda, India
[3]Dept. of CSE, Gaini Zail Singh Campus College of Engineering and Technology, Bathinda, India

**Corresponding Author: kohliramanpreet@yahoo.com*

Available online at: www.ijcseonline.org

Received: 06/Jan/2018, Revised: 10/Jan/2018, Accepted: 25/Jan/2018, Published: 31/Jan/2018

***Abstract*—**The inherent characteristics of mobile ad hoc networks make them susceptible to different types of malicious flooding attacks. Data flooding attack is one of them. Such flooding attacks deplete the network bandwidth and other precious resources to a large extent, creating barriers for future communication among legitimate nodes, paralyzing network operations and leading to Denial of Service (DoS) situation. Learning Automata theory has emerged as a useful tool for performing research activities targeting wireless mobile ad hoc networks. In this paper, we present LA-FIDS - a Learning Automata based Flooding Intrusion Detection System that mitigates the effect of data flooding attack in MANETs by detecting and isolating energy draining malicious node from the communication path. The proposed work is an effort to fill the gap mentioned F-IDS scheme, for not mitigating data flooding attack. The proposed mechanism is implemented in NS 2.35 and simulation results show a considerable improvement in network performance as compared to F-IDS scheme in term of various network performance metrics.

Keywords— MANETs, Flooding, Learning Automata, AODV, DoS, QoS

I. INTRODUCTION

1.1 Mobile Ad hoc Network (MANET)

With the increasing popularity of portable wireless devices, MANETs are presumed to be prevalent in coming years. Anticipating this fact, mobile ad hoc networks have drawn a lot a attention in recent years. Wireless technology is being explored to a large extent, to meet communication requirements in different scenarios. A Mobile Ad hoc Network (MANET) is a network, created temporarily among mobile wireless devices that establish connectivity with each other while they are on move without utilizing any kind of pre-established communication infrastructure or centralized controlling authority. Mobile ad hoc networks use wireless links to get the necessary connectivity among participating devices. Since these networks are devoid of any base/control station, participating nodes have to manage the networking operations on their own. Packets are routed via neighbourhood nodes instead of any base station. Therefore nodes not only act as normal hosts but also as routers, discovering, establishing routes and forwarding data for others [1-3]. Nodes work on mutual trust and cooperate with each other to carry out all necessary networking functionalities within their limited resources. Nodes have no restriction as far as their mobility is concerned. Complete liberty to move in any direction further makes the network topology highly dynamic [4-9].

These salient features of Mobile Ad hoc Networks (MANETs) make them a fascinating technology that could be used for achieving connectivity among mobile devices anywhere and anytime. But their inherent characteristics make them susceptible to a number of serious challenges. Open wireless medium, lack of fixed infrastructure, absence of concrete administrative support, unpredictable dynamic topology, constrained resources, limited shared bandwidth etc. pose a number of challenges towards its smooth deployment and conduct.

As the entire communication has to take place through an open and shared wireless medium, mobile ad hoc networks become most susceptible to large number of security menaces [10-14]. Denial of Service (DoS) attack [15] is one of the biggest challenge that could literally shatter the network operations by draining the energy of participating nodes. One way of launching DoS attack is by using control packet flooding or data packet flooding.

When malicious flooding is conducted via the transmission of control packets, used while discovering routes, maintaining routes or dissipating updations taking place in network topology like route request (RREQ), route reply (RREP), HELLO etc., it is termed as control packet flooding. On the other hand when an attacker transmits a large number of bogus or unwanted data packets to a target node in the network, it is termed as data flooding attack. Malicious flooding of any type, is a serious threat and must be avoided as it could make the network choked or congested with unwanted control or data packets. Abundant literature is available, dealing with the flooding threat caused due to control packets but only few techniques have been proposed to counter data flooding attack in mobile ad hoc networks. In this paper a learning automata based mechanism is proposed that mitigates data flooding attack in MANETs.

1.2 Learning Automata

In learning automata theory, the component namely 'Automata' represents a machine that is capable of performing a finite number of actions where each selected action is assessed by an 'Environment'. It is called learning automata because it possess the ability to get feedback from the environment in which it is deployed and subsequently utilize the learning in improving the system by choosing the best action by following a reward and penalty system [16-19].

Formally, LA can be expressed as {Φ, α, β, F, h} where:

- Φ represents, a set of automata states. At any instant 'n', the state Φ (*n*) belongs to a finite set $\Phi=\{\Phi_1, \Phi_2, \ldots, \Phi_s\}$
- α is a set of action (output of automata), action of automata at instant n is α (*n*), and set of actions is $\alpha=\{\alpha_1,\alpha_2,\ldots, \alpha_1\}$
- β represents, a set of environment responses acting as inputs of automata. Input to automata at instant 'n' is β (*n*) and set of inputs is defined as $\beta = \{\beta_1, \beta_2,\ldots, \beta_m\}$.
- *F*: Φ × → Φ is the learning algorithm. *F* is a mapping current state and input to the next state. *F* can be defined as: Φ (*n* + 1) = *F* (Φ [*n*], β [*n*])
- *h*: Φ × β → α is the output function that maps current state and input to the current output. β (*n* = g (Φ ([*n*]) if output function replace by g: Φ → a.

Here
n depicts the iteration number.
$P_i(n)$ is action probability.

1.2 Motivation and contribution

The proposed scheme is an enhanced version of F-IDS (Flooding-Intrusion Detection System) scheme [20] which has a limitation of not mitigating data flooding attack in mobile ad hoc network. The proposed scheme LA-FIDS is employing theory of learning automata to detect and isolate malicious node causing data flooding from the data communication route. The proposed scheme is implemented in NS 2.35 and results achieved after simulation depict significant improvement in performance as compared to the F-IDS scheme in terms of parameters such as throughput, bandwidth wasted, energy remaining, packet delivery ratio and number of packets flooded.

1.3 Organisation of paper

In section II, we have given an overview of ad hoc flooding attacks, possible in MANETs. Section III discusses some of the existing schemes proposed for mitigating data flooding attacks in MANETs. In section IV, we describe the proposed mechanism - Learning Automata based Flooding Intrusion Detection System (LA-FIDS) in detail. In section V of this paper, we discuss the simulation results and evaluate the proposed scheme with F-IDS scheme. Section VI presents the conclusion and is later followed by references.

II. AD HOC FLOODING ATTACKS IN MANETS

MANETs are networks formed by mobile nodes without using any kind of fixed infrastructure. There is no administrative support from any base station or control station. Nodes utilize radio links to communicate in multi-hop fashion, managing activities, not only as an ordinary host but also as a router. To carry on the network operations, MANETs use flooding technique to undertake many of the network activities needed for establishing communication. Flooding could be termed as one of the most fundamental and frequently invoked function in wireless mobile ad hoc networks. It is employed by most of the popular standard routing protocols such as AODV [20], DSR [22], ZRP [23], LAR [24] etc. for disseminating information regarding route discoveries, route maintenance, routing errors, frequent topology changes etc. But an uncontrolled flooding could totally shatter the network operations. Therefore it is mandatory to employ efficient protocols that use flooding in an efficient manner without choking the network or compromising its performance.

Attackers generally exploit this flooding feature to bring down the network operations. The main objective behind any ad hoc flooding attacks is to push the network to a situation where nodes becomes incapable of providing mandatory services to legitimate nodes. Ad hoc flooding deplete the battery powers of nodes, exhaust their storage capacities and consume network bandwidth by congesting the network with unnecessary control or data packets, paralyzing any victim node and gradually the network. There could be multiple variations in the nature of ad hoc flooding attacks. But we have discussed only two types of flooding attacks namely

RREQ flooding attack and Data Flooding attack in this paper.

2.1 Route Request (RREQ) Flooding Attack

RREQ flooding attack is a control packet flooding attack. Most of the standard routing protocols have set a limit on the number of route requests a node can send per unit time. Attacker nodes bypass this limit and flood the network with more than required RREQ control packets, making the network congested with bogus RREQs. The nodes end up creating overflow in their routing tables by innocently processing bogus RREQs. As a result nodes fail to entertain genuine route requests [25] [26] and legitimate nodes fail to use the network for valid communication causing denial of service (DoS) attack.

2.2 Data Flooding Attack

It has been discovered that MANETs are vulnerable to malicious flooding attacks because of their inherent features and attackers could very well exploit these features to paralyze network operations either by maliciously introducing RREQ flooding or data flooding. But still majority of efforts have been exercised, mitigating RREQ flooding and comparatively lesser number efforts have been put towards providing protect from data flooding attacks [25][26]. Due this fact, comparatively little literature is available on data flooding attacks.

As MANETs are devoid of fixed communication infrastructure, a multi-hop path needs to be constructed from source to the destination by the nodes themselves for communicating with each other. Similarly, for performing data flooding attack, the attacker node setups a path to the target node before forwarding bogus data packets in large numbers to it. The target node keeps on processing the incoming data packets innocently, unaware of the attack, exhausting its battery power. Data flooding attack turns out to be more disastrous due to larger size of data packets. A data packet is generally of 1 Kbytes or 512 bytes in size in comparison to 24 bytes of RREQ packet [27]. These excessive data packets, create congestion in the network, deplete the available bandwidth and other resources to a larger extent, creating barriers for future communication among legitimate nodes, paralyzing network operations and leading to denial of service attack [13]. Thus MANETs need to have measures to intelligently detect and mitigate data flooding attacks. In this paper we have proposed a scheme to counter data flooding attack using learning automata theory.

III. RELATED WORK

Authors in [13] propose a system namely Flooding Attack prevention (FAP), a defence mechanism for route request or data flooding attacks. The scheme is employing a path cut-off mechanism to safe guard against data flooding attacks. As per this scheme when a victim node comes to know that it has been made a target for imposing data flooding attack, it may cut-off the communication route. In the present time, when everyone is in a hurry, people want to get access to their required data in no time. People around the world are using the latest electronic devices to get data packets in the form of burst traffic [28] to save their precious time. In view of this it is observed that FAP is not using any mechanism to differentiate between burst traffic and attack traffic. It recognises a data attack by simply comparing the data traffic with a threshold value which will wrongly interpret a burst traffic with a data flooding attack and will definitely degrade the throughput of burst traffic.

In [29], authors have proposed PDM, a novel period-based defence mechanism for mitigating the effect of data flooding attacks while taking due care of the burst traffic. PDM is working on periods and is handling data floods by means of a blacklist, allowing high data traffic to flow at high rate for the entire duration. Authors have carried a comparison between the performances of standard AODV routing protocol with that of PDM scheme and notified that PDM outperforms between the two as standard AODV fails to process packets due to resource exhaustion in the presence of burst traffic.

Authors in [30] are using a firewall that is dynamically configurable to detect the intruder, source of data flooding. The firewall has filters to resist data flooding. The scheme is using a firewall table, a reject list and a black list. Firewall table is keeping a record of data flows while reject list is maintaining entries of suspicious nodes. An intruder once detected, is restricted by the firewall for a specified time. Once a node is blacklisted, this information is exchange with other nodes. The scheme is programmed with a fixed threshold value of 80 packets for a normal user. On each entry in reject list threshold value is decremented by 5 data packets.

In [31], a dynamic method is adopted to locate a less congested path for performing data transfer in malicious data flooding scenarios. In this scheme every host investigates possible misbehaviour of its neighbours. Whenever network congestion is detected, the sending nodes decrease their respective data transmitting rates. Thereafter if the channel still remains congested, the destination concludes that some of the sending nodes have not reduced their transmission speeds. To curb the situation, a comparison between the current and the previous sending rates is carried on. If both the transmission rates happen to be same, the sender is taken up as an attacker and an alternative path is opted for completing the data transfer, isolating the attacker. Selfish path selection mechanism is utilized to select an alternative

path. Possible drawback of this approach could be due to path oscillations.

IV. METHODOLOGY

For mitigating the impact of malicious data flooding attack, a modified mechanism based on Learning Automata is proposed called as Learning Automata- Flooding Intrusion Detection System (LA-FIDS), which comprises three separate phases. These phases are termed by their functionalities namely - dynamic threshold calculation phase, confirmation phase and prevention phase. First two phases will be part of the LA component and last phase will be executed by the routing component.

During the first phase, a dynamic threshold value is calculated. The second phase is responsible for identifying a node for its trustworthiness. A node is recognised to be malicious after getting conformation from F-IDS nodes and by assigning penalty points.

The F-IDS nodes play a special role in the network. All F-IDS nodes are put in sniff mode for keeping a watch on the behaviour of the nodes in their neighbourhood during the data transmission phase. Each F-IDS node records the number of data packets forwarded by the intermediate nodes during a pre-set time period (T). This value will act as the input parameter for enabling the LA component of the F-IDS nodes to decide for the authenticity of the nodes.
At the end of the time-period (T), the F-IDS nodes calculate data packets forwarded by the nodes per unit time. They calculate the average, variance and standard deviation for the data packets forwarded using the equations (1) to (3) respectively.

$$A = \sum_{i=1}^{n} DP_i \quad (1)$$

$$v = \sum_{i=1}^{n} \frac{(DP_i - A)^2}{n} \quad (2)$$

$$T = \sqrt{v} \quad (3)$$

Where,
n indicates the number of nodes
DP_i represents the number of data packets forwarded by node $_i$
A represents the average
V is the variance
T is the standard deviation

The calculated standard deviation will be taken as the final threshold value. If the total number of data packet of any node is found greater than the threshold value, the F-IDS node will assign penalty points to the node implying malicious (M) node. In the alternate case, it will assign the reward points, implying a trusted node. This marks the end of confirmation phase.

In the prevention phase, the F-IDS nodes forward an ALERT packet to the source node to notify about the identity of the malicious node, so that source node can change the data transmission path.

V. RESULTS & DISCUSSION

NS-2.35 was used to simulate the schemes with parameters as mentioned in table 1 below.

Figure 1 presents the network animator screenshot of F-IDS scheme simulation, where attacker node 23 is flooding the network, leading to packet dropping and congestion in the network.

Figure 2 is the network animator screenshot of the proposed LA-FIDS scheme displaying the new path (shown in cyan colour) taken by the source node for forwarding data, after the attacker causing data flooding is detected and isolated.

Table 1: Simulation Parameters

Parameter	Value
Channel	Wireless
Mac	802.11
Propagation Model	Two Ray Ground
Antenna	Omni-Directional
Initial Energy	100 Joules
Number of nodes	60
Traffic Type	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Connection Type	UDP
Protocol	AODV

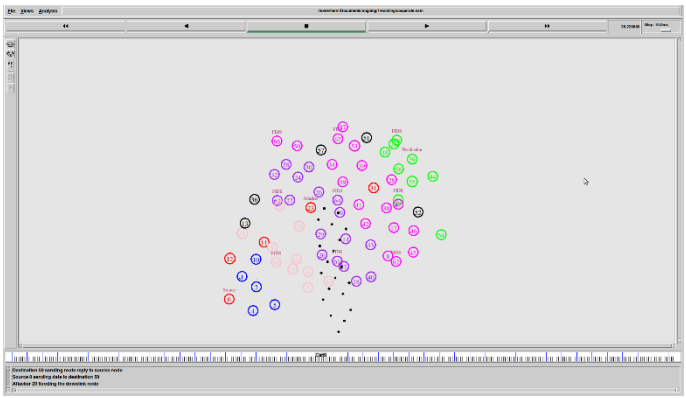

Figure 1: Attacker node 23 flooding the network in F-IDS scheme, leading to packet dropping and congestion.

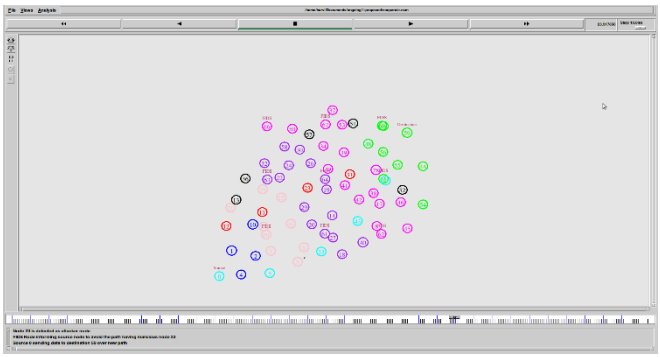

Figure 2: Source node forwards data over new path (in cyan colour) in the proposed scheme- LA-FIDS

After analysing the simulation results, we found that the proposed scheme LA-FIDS outperforms the F-IDS (with data flooding) scheme in terms of following metrics.

5.1 Remaining Energy

This is the perfect measure for the lifetime of the network. Since this work is related to energy draining malicious nodes in the network, therefore, the improvement in this parameter for the proposed scheme adequately showcases the outperformance of the proposed scheme. Under the influence of attacker, the average energy remaining in the network for F-IDS scheme was 86.46 Joules. The proposed scheme shows the value of remaining energy at 87.82 Joules as shown in figure 3. The reason behind less energy consumption for the proposed scheme was that the malicious node was detected and the flooding gets avoided. The malicious node thus cannot consume much energy of the network.

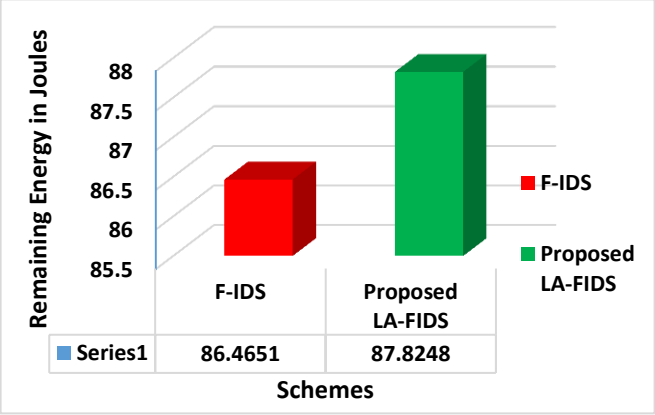

Figure 3: Remaining Energy in Joules

5.2 Throughput

It represents amount of data received at the destination node per unit of time. When the network was under influence of data flooding malicious node, the value of throughput for F-IDS scheme was around 1003.52 Kbps and for the proposed scheme LA-FIDS, the value of throughput was around 1257.47 Kbps as shown in figure 4. The reason behind this is that the existing scheme does not combats flooding of the data packets, which leads to more consumption of the bandwidth of the links between the nodes. This consequently leads to decrease in throughput. However, the throughput for the proposed scheme was more than the existing F-IDS scheme as it shields against the data flooding malicious node.

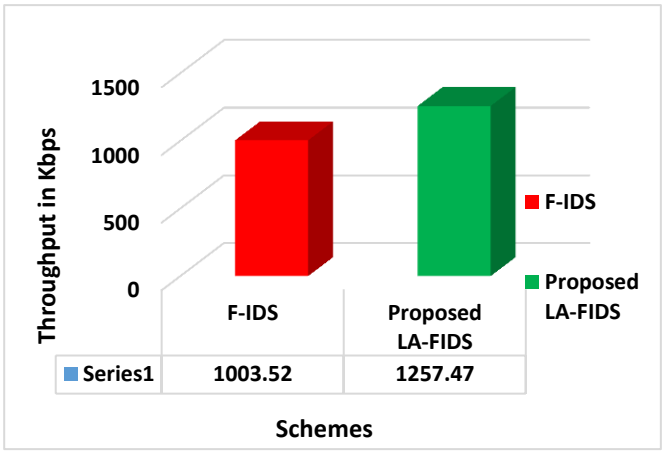

Figure 4: Throughput in Kbps

5.3 Packet Delivery Ratio (PDR)

PDR suggests the percentage of packets sent that got dropped in the network. This parameter was calculated for the entire network, i.e. during the RREQ phase as well as during the data transmission phase. It was 0.83 for the F-IDS under data flooding attack and 0.96 for the proposed LA-FIDS scheme. The reason for the dropping values of PDR was increase in the amount of congestion caused by the malicious nodes. This exhausts the links between the nodes resulting in packet drops and hence decrease in PDR values. Simulations carried by us gave 0.835443 PDR for F-IDS and 0.962526 for the proposed LA-FIDS scheme shown in figure 5.

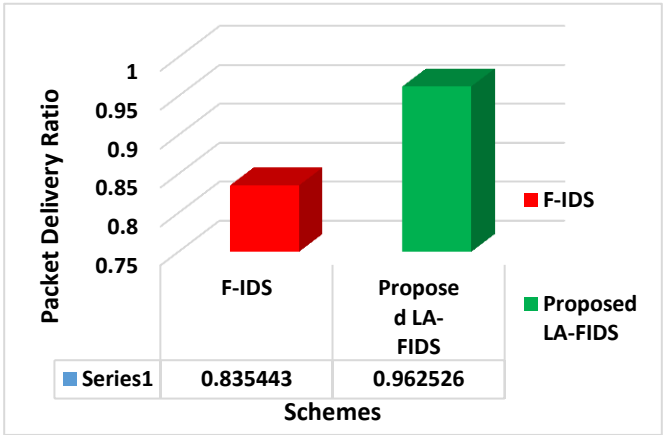

Figure 5: Packet delivery ratio

5.4 Bandwidth Wasted

Since malicious nodes, which flood the network affect bandwidth of the links in addition to energy of the nodes, therefore this parameter was analysed for both the schemes. The proposed scheme LA-FIDS allows the nodes to detect the malicious node and existing scheme is sans any such mechanism. Thus, it results in more Bandwidth wasted /consumed for the existing F-IDS scheme. The results obtained for this parameter for the schemes F-IDS and proposed LA-FIDS are shown in figure 6.

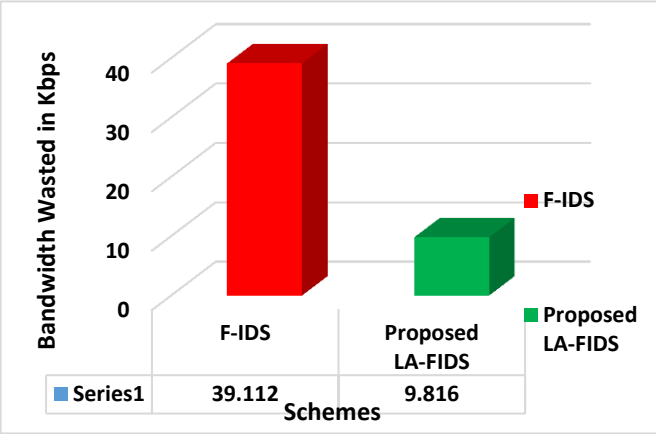

Figure 6: Bandwidth Wasted in Kbps

5.5 Number of Packets Flooded

This shows the impact of the attackers over the network. The higher value of this parameter is obvious for the F-IDS scheme, which does not has any mechanism in place for the detection of data flooding attacker. However, the proposed scheme LA-FIDS shows lesser number of packets flooded in the network as compared to F-IDS scheme as it detects the attacker. Thereby, the source node would avoid the path having the attacker node in it. As shown in figure 7, number of packets flooded in the network were 4889 in case of F-IDS scheme and only 1227 in the proposed LA-FIDS scheme.

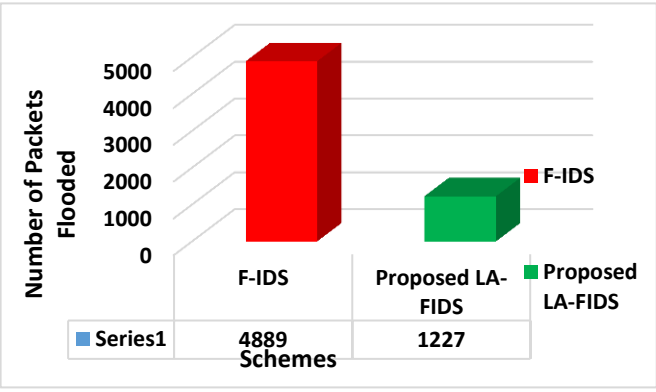

Figure 7: Number of Packets Flooded

VI. Conclusion

Mobile ad hoc networks possess features that throw a number of challenges towards their successful deployment. Handling flooding attack is one such serious challenge. Malicious flooding could be introduced by attackers through control packets as well as via data packets. Data flooding attack, if not handled, can easily result into denial of service attack. Current literature is abundantly full of detection and preventive measures handling RREQ flooding attack but, very few techniques have been proposed to mitigate data packet flooding attack in MANETs. In this paper, we have proposed a Learning Automata based Flooding Intrusion Detection System (LA-FIDS) that mitigate the effect of data flooding in MANETs. In the proposed scheme, F-IDS nodes are employed, operating in the sniff mode to monitor the behaviour of nodes in their neighbourhood during the data transmission phase. The learning made by F-IDS nodes help in distinguishing legitimate nodes from misbehaving node. This information is then effectively utilized to isolate malicious node from the data transmission path. The proposed scheme is an enhanced version of F-IDS scheme. The simulation results show that the proposed LA-FIDS scheme improves the network performance in terms of PDR, throughput, bandwidth wasted, remaining energy and number of data packets flooded when compared to F-IDS. In future, the work can be extended to mitigate the effect of control packet flooding in mobile ad hoc networks.

REFERENCES

[1] J. Sun, "Mobile Ad hoc Networking: A Essential Technology for Pervasive Computing", In the Proceedings of International Conference on Info-tech and Info-net (ICII) Vol, 3 Beijing, pp. 316-321, 2001.

[2] M. S. Alkatheiri, J. Liu, A. R. Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs", In the Proceedings of IEEE 13th International Conference on Communication Technology (ICII), pp. 614-618, 2011.

[3] A. Mishra, R. Jaiswal, S. Sharma "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network", In the Proceedings of 3rd IEEE International Conference - Advance Computing Conference (IACC), pp. 499-504 2013.

[4] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Internet Request for comment RFC 2501, Jan 1999.

[5] R. Ramanathan, J. Redi , "A brief overview of ad hoc networks: challenges and directions", IEEE Communication Magazine, pp. 20-22, 2002

[6] B. Wu, J. Chen, Wu, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security, Springer US, pp. 103-135, 2007.

[7] M. O. Pervaiz, M. Cardei and J. Wu, "Routing Security in Ad hoc Wireless Networks", Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL 33431, pp. 117-142, June 2010.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of Routing Attacks in Mobile Ad hoc

Networks", In the Proceedings of Wireless Communications, IEEE Issue 5, pp. 85-91, 2007.
[9] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29, 2008.
[10] M. Al-Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad hoc Networks", In the 42nd Annual Southeast Regional Conference ACM (ACMSE 2004), pp. 96-97, 2004.
[11] Y.C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, 2006.
[12] Y.C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad hoc Network Routing Protocols," In the 2nd ACM Workshop on Wireless Security, pp. 30-40, 2003.
[13] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad hoc Networks", International Conference on Information Technology: Coding and Computing 2005 (ITCC 2005), vol. 2, pp. 657-662, 2005.
[14] B. Sharma, "Pragmatic Analysis of Energy Conservation in MANETs", International Journal of Computer Science and Engineering, Vol- 3 Issue -5, pp. 227-230, 2015.
[15] J. Mirkovic and P. Reiher, "A taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM Comput. Commun. Review, 34(2), pp.39–53, 2004.
[16] K. S. Narendra, M. Thathachar, "Learning Automata an Introduction", Prentice-Hall, New York, 1989.
[17] P. Nicopolitidis, G.I. Papadimitriou, P. Sarigiannidis, M. S. Obaidat and A. S. Pomportsis, "Adaptive Wireless Networks Using learning Automata", IEEE Wireless Communications, 2014.
[18] S. Misra, P.V. Krishna, A. Bhiwal, A. S. Chawla, B. E. Wolfinger and C. Lee, "A Learning Automata-based Fault-tolerant routing Algorithm for Mobile Ad hoc Networks", Springer –The Journal of Supercomputing, Volume 62 issue 1, pp. 4-23, 2012.
[19] S. Jagannathan, M. J. Zawodniok, "Dynamic Channel Allocation in Wireless Networks using Adaptive Learning Automata", International Journal of Wireless Information Networks, Volume 18, Issue 4, pp. 295-308, 2011.
[20] S. Gurung, S. Chauhan, "A Novel Approach for Mitigating Route Request Flooding Attack in MANET", Wired Networks 2017, pp. 1–16, 2017.
[21] C. E. Perkins, "Ad Hoc On-Demand Distance Vector (AODV) Routing," INTERNET DRAFT - Mobile Ad hoc NETworking (MONET) Working group of the Internet Engineering Task Force (IETF), 1997.
[22] D. B. Johnson, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Springer- Mobile Computing, pp. 153-181. Kluwer Academic Publishers, Dordrecht, Netherlands, 1996.
[23] Z. J. Haas and M. R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", INTERNET DRAFT - Mobile Ad hoc NETworking (MONET) Working group of the Internet Engineering Task Force (IETF), 1997.
[24] Y. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", Springer –Wireless Networks, pp. 307-321, 2000.
[25] S. Desilva and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad hoc networks," IEEE Wireless Communications and Networking Conference (WCNC) USA, vol. 4, pp. 2112-536, 2005.
[26] S. Li, Q. Liu, H. Chen, and M. Tan, "A New Method to Resist Flooding Attacks in Ad Hoc Networks," In the Proceedings of IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1-4, 2006.
[27] K.A. Khan, T. Suzuki, M. Kobayashi, W. Takita, and K. Yamazaki, "Packet Size based Routing for stable data delivery in Mobile Ad-hoc Networks," IEICE Transactions on Communications, vol. E91-B, no. 7, pp. 2244-2254, 2008.
[28] X. Yang, Y. Shi, M. Zeng, and R. Zhao, "A Novel Method of Network Burst Traffic Real-time prediction based on decomposition," International Conference on Networking (ICN), Lecture Notes in Computer Science, vol. 3420, pp. 784793, 2005.
[29] H. Kim, R. B. Chitti and J. Song, "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Consumer Electronics , pp. 579-582, 2010.
[30] S. Akram, I. Zubair, M.H. Islam, "Fully Distributed Dynamically Configurable firewall to Resist DOS", In the Proceedings of IEEE International Conference. on Networked Digital Technologies, pp. 547-549, 2009
[31] M. Bahl, R. Bhoomarker, S. Zafar, "Distributed Detection of packet flooding in Infrastructure-less Wireless Network- An adaptive approach", In the Proceedings of IEEE International Conference on Advances in Engineering & Technology (ICAETR), pp. 1-4, 2014

Authors Profile

Raman Preet is a research scholar at department of Appied Science- Computer Applications, I.K. Gujral Punjab Technical University, Jalandhar. She has nine years of teaching experience. Her research interests are wireless networks, natural language processing and image processing.

Shaveta Rani received her B. Tech. in Computer Science and Engineering from PTU, Jalandhar and M. S. in Software Systems from BITS, Pilani. She did Ph.D. in Computer Science and Engineering from BITS, Pilani, in 2009. She is working in Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab since August 1998. There are 50 research papers to her credit out of which 11 research papers in International refereed Journals, 12 publications in International refereed Conference proceedings, rest are in National Conferences. She has guided 25 M.Tech and 04 PhD thesis. Her research interest includes Computer Networks, Image Processing, Optical Networks.

Paramjeet Singh received his B. Tech. in Computer Science and Engineering from PTU, Jalandhar and M. S. in Software Systems from BITS, Pilani. He did Ph.D. in Computer Science and Engineering from BITS, Pilani. He is working in Giani Zail Singh College of Engineering and Technology Bathinda since September 1998. There are 51 research papers to his credit out of which 11 research papers in International refereed Journals, 12 publications in International refereed Conference proceedings, rest are in National Conferences. He has guided 30 MTech. and 04 PhD thesis. His research interest includes Computer Networks, Computer Graphics, and Software Engineering.

