International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-6, April 2020

Deployment and Selection of Monitoring Nodes for Detection of Selfish Attacks in MANET

R. Mangayarkarasi, R. Manikandan

Abstract: ***Since Mobile Ad hoc Network (MANET) has distributed network structure using wireless links, designing efficient security applications has become a critical need. Selfish nodes are nodes that refuse to forward the data from other nodes. The existence of selfish nodes will disturb the normal process of the network, and reduce the network performance. Intrusion Detection System (IDS) is a scheme for detecting any misbehaviors in the network operation by monitoring the traffic flow. Each monitoring node need to execute the IDS module. The common problems encountered by the monitoring nodes are energy depletion, link disconnection, mobility and coverage. Hence the selection of monitoring nodes plays an important role in IDS. This paper develops a technique for deployment and selection of monitoring nodes for detection of selfish attacks. In this technique, the whole network is virtually divided in smaller grid like zones. In each grid, the nodes with higher stability and better coverage are assigned a reward value. A cost metric is derived in terms of energy consumption and computational delay. Then the nodes with minimum cost and high reward are selected as monitoring nodes. By simulation results, it is shown that the proposed technique has reduced detection delay, energy consumption and detection overhead.***

Keywords: MANET; DoS; Selfish Attack; IDS; misbehavior

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is fundamentally a self-organizing network composed of plentiful nodules which are proficient of great flexibility and are associated to each other in a wireless method. In MANET, every mobile node is proficient of working as a router [1]. Since MANET has a distributed network structure using wireless links, several security threats are faced. As a result, designing efficient security applications has become a critical need in MANET [2][3]. Some of the control traffic attacks are Sybil attack, wormhole attack, rushing attack, etc [4]. Some of the major data traffic attacks are selective forwarding attack, blackhole attack, delaying and misrouting attack, etc [5]. One of the harmful attack is Denial of Service (DoS) attack. It exhausts the victim's network resources such as bandwidth, computing power, battery etc [6]. In Sybil attack, an attacker can create more than one identity on a single physical device in by launching a coordinated attack on the network [7]. Among these attacks, DoS, packet dropping attack and cheating attack are considered in this paper.

Revised Manuscript Received on March, 28 2020.
* Correspondence Author
R. Mangayarkarasi*, Assistant Professor, Department of Computer Science, Government Arts College, Trichy. E-mail: Mangayarkarasiphd@gmail.com
Dr. R. Manikandan, Associate Professor, Department of Computer Science and Engineering, Sengipatti, Thanjavur. E-mail: rmkmanikandan@yahoo.co.uk

Intrusion detection is described as a process of identifying any actions or series of actions which can affect the The selfish nodes are nodes that refuse to forward the data from other nodes. The existence of selfish nodes will disturb the normal process of the network, and reduce the network performance. confidentiality, integrity or availability of a network resource. Intrusion Detection System (IDS) is a scheme for detecting any misbehaviour in the network operation by monitoring the traffic flow [8]. In MANET, IDS should be developed in order to detect any active or passive attack and then respond to it by using appropriate defense scheme [9]. Each monitoring node need to execute the IDS module. Hence the selection of monitoring nodes plays an important role in IDS. The common problems encountered by the monitoring nodes are energy depletion, link disconnection, mobility and coverage. Hence this paper develops a technique for deployment and selection of monitoring nodes for detection of selfish attacks. The paper is organized as follows. In section 2, few of the existing works are discussed. Section 3 presents the detailed description of proposed methodology. In section 4, simulation results and analysis are described. Section 5 concludes the paper.

II. RELATED WORKS

Mustafa et al [9] have presented a distributed and cooperative mechanism for detecting routing attacks in MANETs. In this mechanism, both the neighbor nodes as well as remote node are taken into consideration, and then its direct as well as indirect network factors are monitored to develop behavior characteristics. The anomalous event is detected based on the routing delay time duration as well as packet count. But, gathering information related to the delay involved in packet transmission through all the paths will create high overhead. Also, only the forwarded packets and received packets are taken into consideration for developing the behavior metrics and all the remaining layer metrics are not considered. Balan et al [10] have proposed a Fuzzy based IDS to detect the malicious behaviour of nodes as well as to determine the attack type. This proposed technique is appropriate for mainly two kinds of attack: black hole attack and the gray hole attack. In this paper, just packet drop is considered as the major factor for detection of black hole nodes. However, precise result will not be attained from it since it will give rise to many false positive cases. Subha et al. [11] have presented a game theory based IDS mechanism that includes a cluster leader election procedure and a hybrid IDS. The hybrid IDS consists of a threshold based lightweight unit and also an anomaly based heavyweight unit.

The lightweight unit is developed based on the Packet Forwarding Rate (PFR) factor. The normal network profile is developed based on the unsupervised association-rule mining technique and employed in the heavy weight module. In the Bayesian game model, the cluster leader is permitted to design its monitoring technique. Imani et al. [12] have presented a combined technique for misuse detection along with the anomaly detection to examine the network and determine the kind of attack. In this technique, the combination issue is resolved by employing the partially observed Markov decision process (POMDP). Whenever the known attack probability is greater, the misuse detection scheme is used. The anomaly detection scheme is used, whenever the unknown attack probability is greater and crosses the threshold value.

Vali et al. [13] have suggested a Cross-layer centered dispersed and supportive IDS by means of Dempster-Shafer indication philosophy. The network action is frequently observed by the indigenous discovery engine. It activates the IDS whenever any malicious behavior is seen. But, just the packet dropping attack is taken into consideration in this paper.

III. PROPOSED SOLUTION

3.1 overview

In this technique, the whole network is virtually divided in smaller grid like zones. The entire nodules in every lattice are inspected and the nodules with advanced steadiness and better coverage are assigned a reward value. A cost metric is derived in terms of energy consumption and computational delay. Then the nodes with minimum cost and high reward are selected as monitoring nodes.

3.2 node stability

For foreseeing the forthcoming state of the network, the flexibility is assessed which is well-defined as follows.

$$S_i = \frac{1}{\Delta t}\left|Davg_i(t) - Davg_i(t+\Delta t)\right| \quad (1)$$

$$Davg_i = \frac{1}{n}\sum_{j=1}^{n} D_{(i,j)}(t) \quad (2)$$

$$D_{(i,j)} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (3)$$

Where Si signifies the comparative rapidity of the nodules

Davgi(t) signifies the average expanse amongst the nodule i and its adjacent at period t.

n is the number of adjacent nodule i

D(i,j)(t) is the expanse amongst nodule i and nodule j.

x and y signify the synchronizes of the nodule.

Dependability of a wireless association is able to be dignified by means of LET which is a location centered layer metric. The movement factors of two adjacent nodules are vital for open space broadcast. Hence, in MANETs, global positioning system (GPS) is desirable by every nodule. The period for which these two nodules are associated is evaluated by means of the movement factors of two nodules. Here it is presumed that nodules have equivalent broadcast radius y with particular locations *(m1, n1)* and *(m2, n2).* The rapidity along the directions *d1* and *d2* are signified as s1 and s*2*. The succeeding equation offers the LET calculation.

$$LET = \frac{-(pq+rs) + \sqrt{(p^2+r^2)y^2 - (ps-qr)^2}}{(p^2+r^2)} \quad (4)$$

p = s1cos*d1* – s2 cos*d2*
q = m1-m2
r = s1sin*d1*-s2sin*d2*
s = n1 –n2 [9]

3.3 ENERGY CONSUMPTION

Let E_i be the preliminary energy of a nodule

After the time period t, the energy spent by the nodule (E (t)) is provided by means of succeeding equation [4]

$$E(t) = n_{tx} * \varepsilon + n_{rx} * \delta \quad (5)$$

where n_{tx} and n_{rx} are the number of data packages transferred and obtained by the nodule after time t.

ε and δ are coefficients in the series (0,1)

3.4 Cost of a Node

Let dc_i be the computation delay of node N_i .

Then the cost of a node is computed in terms of energy consumption and computational delay as

$$C_i = E_i + dc_i \quad (6)$$

where C_i and E_i are the cost and energy consumption of node Ni.

3.5 Reward of a Node

Primarily the entire nodules of the network are allotted a recompense value RW, universally.

3.6 Deployment of Monitoring Nodes

The entire nodules in MANET are inspected and the nodules with advanced steadiness and remaining energy are nominated and are denoted as Monitoring nodules (MNs). These MNs will further be responsible for monitoring the network within its transmission range and determining the trust value of these surrounding nodes, in order to ensure the authenticity of these nodes. The process of selecting the MNs is described in algorithm 1.

Algorithm - Deploying and Selecting MNs_

Notations	Definition
$G_1, G_2, \ldots G_k$	Virtual grids
$MN_1, MN_2, \ldots MN_k$	Monitoring nodes
D_{im}	Node density of each grid G_i
Average $\{D_{im}\}$	Average node density all grids
Rw_i	Reward value of MN_i.

Retrieval Number: D6704049420/2020©BEIESP
DOI: 10.35940/ijeat.D6704.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C_i Cost of MN_i
inc Increment counter for reward and cost
d_i delay of MN_i
$MinE_r$ Minimum threshold value for residual energy
MinLET Minimum threshold value for LET
$Ne(MN_j)$ Nearest neighbor of MN_j

---

1. Split the network effectively into k smaller grids $G_1, G_2, \ldots G_k$
2. For each G_i, i=1,2…k.
3. Choose any $MN_j \in G_i$
4. Estimate D_{im} of G_i
5. Estimate C_i
6. If D_{im} > Average $\{N_{im}\}$ and LET (MN_j) > MinLET then
7. $Rw_i = Rw_i + inc$
8. If C_i = Minimum(C_i) and Rw_i = Maximum(R_i) , then
9. MN_j is selected
10. Else
11. Choose $Ne(MN_j)$
12. Repeat from step 4.
13. End if
14. Else
15. Find $G_k = G_i \cup G_{i+1}$
16. Repeat from step 3.
17. End if
18. End For

In this algorithm, the whole network is virtually divided in smaller grid like zones for convenience. Initially, one node N_j is randomly selected in each zone. It estimates node density of its zone. The decision for a node to act as a MN will be on the basis of the high dense zone. If the node density of that zone is more than the average value, the selected node will be further checked for LET and residual energy. If both are higher than the minimum threshold values, then the node N_j is selected as MN. Otherwise, the nearest neighbor node of Nj is considered and checked for stability and energy conditions. This process is continued until a node from the same zone, satisfying the conditions is found. On the other hand, if the node density is less, the next zone will be merged to form a new larger zone, and the process is repeated.

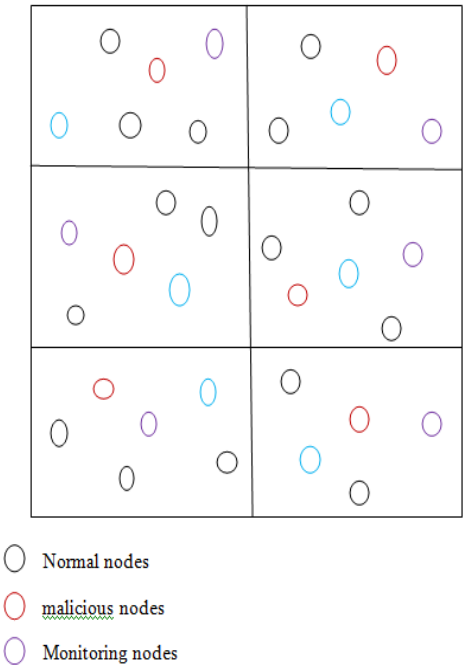

Figure 1 Deployment of MNs

Figure 1 shows the network partitioned into zones. Each zone can be considered as a cluster and every node within the cluster is under the coverage range of the MN. So, whenever a intruder or a new connection enters into the cluster, it is monitored by the MN.

IV. SIMULATION RESULTS

4.1 Simulation Parameters

The proposed DSMN technique is simulated in NS2 and is compared with the RTBD [14] technique. The performance of both these techniques is evaluated in terms of packet delivery ratio, average residual energy, end-to-end delay, and detection overhead.
Table 1 shows the settings and parameters used in our simulation

Table 1 Simulation parameters

Network Size	60 to 140 nodes
Size of the Area	1000 X 1000 m
MAC Protocol	IEEE 802.11
Traffic Model	Constant Bit Rate
Number of Attackers	1 to 5
Propagation Model	Two Ray Ground
Antenna Model	Omni Antenna
Initial Energy	15 Joules
Tx Power	0.8 watts
Rx Power	0.5 watts

4.2 Threat Model

We take into consideration a MANET milieu in which both an outward challenger (outsiders) and inside (prevailing members) challenger, bout the multicast congestion. The deliberated bouts are DoS and package plummeting bouts.

4.3 Results & Analysis

Varying the nodes with 5% of attackers

In order to analyze the effect of attackers over the network size, the number of nodes is varied as 50,75,100,125 and 150 with 5% of the nodes as attackers.

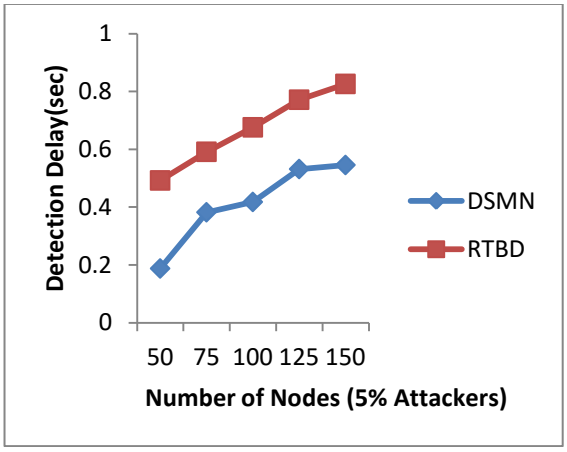

Figure 2 Detection Delay for 5% of attackers

The result of detection delay of DSMN and RTBD techniques is presented in Figure 2.As the nodes are increased, the delay of DSMN increases from 0.18 seconds to 0.54 seconds whereas the detection delay of RTBD increases from 0.49 to 0.82 seconds. Since the attacks are detected quickly by collaborative detection of monitoring nodes, the detection delay of DSMN is 40% lesser than RTBD.

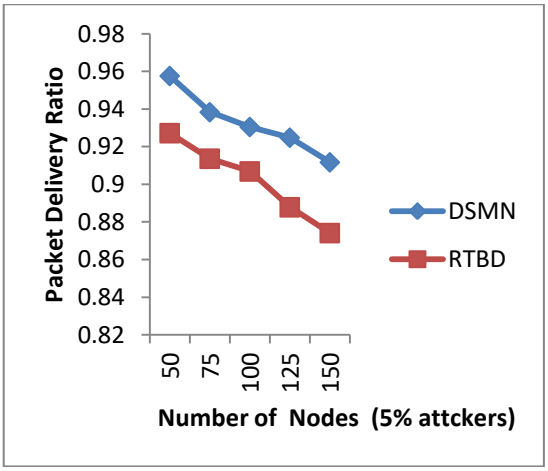

Figure 3 Packet delivery ratio for 5% of attackers

The result of packet delivery ratio of DSMN and RTBD techniques is presented in Figure 3. As the nodes are increased, the delivery ratio of RTBD decreases from 0.95 to 0.91 and the delivery ratio of RTBD decreases from 0.92 to 0.87. As DSMN detects attacks on both network and MAC layers, the delivery ratio of DSMN is 3% higher than RTBD.

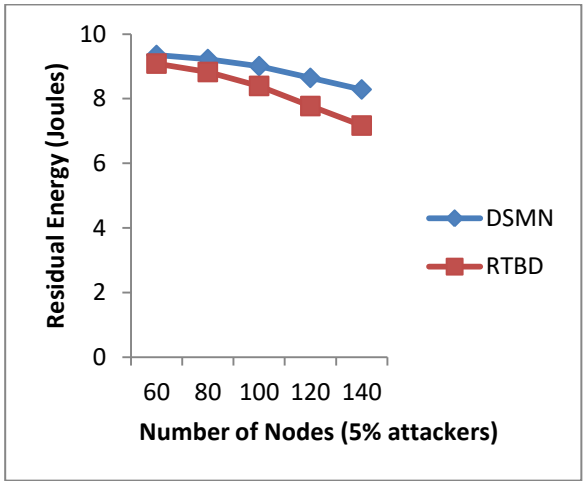

Figure 4 Residual Energy for 5% of attackers

The residual energy of DSMN and RTBD techniques is shown in Figure.4. As the nodes are increased, the residual energy of DSMN decreases from 9.3 to 8.2 joules and residual energy of RTBD decreases from 9.0 to 7.1 joules. Since DSMN aims to detect attacks on energy depletion, it has 7.5% higher residual energy than RTBD.

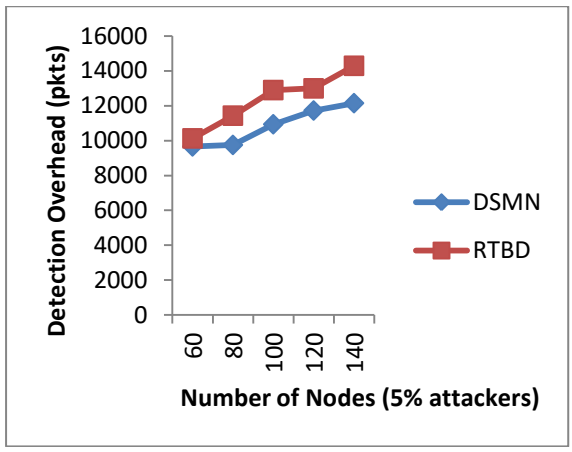

Figure 5 Detection Overhead for 5% of attackers

The detection overhead of DSMN and RTBD techniques is shows in Figure 5. As the nodes are increased, the overhead of DSMN increases from 9664 to 12144 packets and overhead of RTBD increases from 10125 to 14285 packets. Since the stable and energy efficient nodes are selected for monitoring, the frequency of changing the monitoring node is less. Hence the detection overhead of DSMN is 11% less when compared to RTBD.

V. CONCLUSION

This paper develops a technique for deployment and selection of monitoring nodes for detection of selfish attacks. In this technique, the whole network is virtually divided in smaller grid like zones. In each grid, the nodes with higher stability and better coverage are assigned a reward value. A cost metric is derived in terms of energy consumption and computational delay.

Retrieval Number: D6704049420/2020©BEIESP
DOI: 10.35940/ijeat.D6704.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Then the nodes with minimum cost and high reward are selected as monitoring nodes. By simulation results it has been shown that the proposed DSMN technique has reduced detection delay, energy consumption and detection overhead.

REFERENCES

1. Usha G, M. Rajesh Babu, S. Saravana Kumar,(2016), "Dynamic anomaly detection using cross layer security in MANET", *Computers and Electrical Engineering*, Elsevier, 1–11.
2. Javidi M.M and Laya Aliahmadipour,(2015),"Game Theory Approaches in Taxonomy of Intrusion Detection for MANETs",*Computer Engineering and Applications* Vol. 4, No. 1.
3. Amiria E., Hassan Keshavarz, Hossein Heidari, Esmaeil Mohamadi, Hossein Moradzadeh,(2014), "Intrusion Detection Systems in MANET: A Review",*Procedia - Social and Behavioral Sciences*, 129, 453 – 459.
4. Khan M.S and Noor M. Khan,(2016), "Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks",*Journal of Sensors,Hindawi Publishing Corporation*, Article ID 9783072, 9 pages
5. Behzad S.S.J.,(2015), "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", *International Journal of Computer Science and Network Security*,44, VOL.15 No.3.
6. .Sari A.,(2014),"Security Approaches in IEEE 802.11 MANET", *Int. J. Communications, Network and System Sciences*,7, 365-372
7. Abbas S., Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, (2013),"Lightweight Sybil Attack Detection in MANETs", *IEEE SYSTEMS JOURNAL*, VOL. 7, NO. 2.
8. Abdalla A.M, Imane A. Saroit, Amira Kotb, Ali H. Afsari,(2011),"Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol",*Procedia Computer Science* 3,115–121
9. Mustafa H, Yan Xiong, Khalid Elaalim,(2014), "Distributed and Cooperative Anomaly Detection Scheme for Mobile Ad Hoc Networks", *Journal of Computer and Communications*, 2, 1-10
10. Balan V.E, Priyan M K, Gokulnath C, Prof.Usha Devi G,(2015), "Fuzzy Based Intrusion Detection Systems in MANET", *Procedia Computer Science*, 50, 109 – 114
11. Subba B., Santosh Biswas, Sushanta Karmakar,(2016),"Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation",*Engineering Science and Technology, an International Journal, Elsevier*, 19,782–799
12. Imani M, Mohammad Ebrahim Rajabi, Mahdi Taheri, and Majid Naderi,(2015),"A Novel Approach to Combine Misuse Detection and Anomaly Detection Using POMDP in Mobile Ad-Hoc Networks",*International Journal of Information and Electronics Engineering*, Vol. 5, No. 4.
13. Vali Y.S And T.R.Rangaswamy,(2017),"An Efficient Cross-Layer Based Intrusion Detection System For Mobile Ad Hoc Networks", *Journal of Theoretical and Applied Information Technology*,Vol.95. No.1
14. Subramaniyan S., William Johnson and Karthikeyan Subramaniyan,(2014), "A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique", *EURASIP Journal on Wireless Communications and Networking*, 2014:s205