Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

PERFORMANCE OF SWARM BASED INTRUSION DETECTION SYSTEM USING VARIOUS MOBILITY MODELS IN MANET

G. Indirani
Assistant Professor
Department of CSE.,
Annamalai University,
Annamalai nagar- 608002 , India.

K.Selvakumar
Associate Professor
Department of CSE.
Annamalai University,
Annamalainagar-608002, India.

Abstract— In mobile ad hoc network (MANET), the process of intrusion detection is difficult due to the features of the MANET such as dynamic topology, limited transmission range, mobility, etc. The movement of nodes plays the major role. In this paper, Swarm based Intrusion detection is created using various mobility models in MANET. The various mobility models used are Random waypoint mobility model, Random walk mobility model and Random direction mobility models. Here the nodes with highest trust value and residual bandwidth are selected as active nodes using the swarm agents. Every active node examines its neighbour nodes within its radio transmission range and gathers the trust value from all monitored nodes. The active nodes will always be changing as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. When the source receives alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. By simulation results we show that the Swarm based intrusion detection using random direction mobility model is producing better results while varying the attackers and speed. So the mobility model plays a major role during the intrusion detection.

Keywords— MANET, SBDT, RANDOM WAYPOINT MOBILITY MODEL, RANDOM WALK MOBILITY MODEL, RANDOM DIRECTION MOBILITY MODEL

I. INTRODUCTION

A. MOBILE AD-HOC NETWORKS (MANETS)

A mobile ad hoc network is a collection of wireless mobile nodes which can have communication among themselves without any centralized monitoring and control. A manet is a temporarily formed network having the dynamic topology. It is a self-configured network. Here each mobile node acts as a router or host. Here the routes required for communication between the source and destination is achieved through the routing protocols. The manet can be used in many applications such as rescue operations, tactical operations, environmental monitoring, conferences, connecting soldiers in battlefields and social or business application such as public and personal area networks.[1] the weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [2].

B. GENERAL ATTACKS IN MANET

The MANETs are highly affected by the security attacks than the wired networks[3]. Since the MANET nodes have restricted protection, dynamic behaviour of connectivity, no centralized administration, the security maintenance is difficult. The attacks in MANET can enter either from inside the network or from outside. Detection of attacks from inside the network are difficult and also destructive. The MANET attacks are classified as active and passive attacks which are described below.

1) Active attacks: An active attack causes various levels of damage to the network depending on the type of attack. It is further classified into two categories of attacks such as internal and external attacks.

- The internal attacks are performed by the valid nodes that belong to the network.
- The external attacks are performed by the nodes that are not part of the network.

Wormhole attack, black hole attack, Byzantine attack, information disclosure and resource consumption attack are some of the examples of active attacks.

2) Passive attacks: In this attack, the attacker does not interrupt the normal operation of the network but indirectly obtains the data exchanged in the network without changing it. This type of attack is difficult to identify as the normal operation of the network is not affected [3] [4]. Snooping is a type of passive attack which uses another person's data illegally. That is watching e-mail informally that is displayed on another's computer screen or observing other people typing or employing a software program to examine the process of a computer or network device [4].

C. Swarm based Intrusion detection[SBDT][1]

Here, the active nodes are selected by using the swarm intelligence based ant colony optimization. The active nodes are selected based on the parameters namely the node with highest trust value and residual bandwidth. This is done to perform the process of intrusion detection. Every active node examines its neighbor nodes within its transmission range and collects the trust values from all those nodes. Every active node changes adaptively as per the trust thresholds. Then the collaborate exchange of the trust values will occur among the active nodes. After the exchange process, if any particular node's trust value is found to be below minimum threshold, then that node is identified as malicious. Upon detecting malicious node, the active node sends an alert message to the source node. The source then deploys a defense mechanism to filter the malicious nodes from the networks [2].

D. Mobility models

Here three mobility modes are used namely Random waypoint mobility model, Random walk mobility model and Random direction mobility model. Mobility models play a major role in the performance of SBDT.

E. Problem identification

Swarm based Intrusion detection technique (SBIDT) performs well when compared with DTMF [1]. Now in this work the performance of swarm based Intrusion detection system is created using three mobility models for the various routing attacks.

II. LITERATURE REVIEW

Indirani G and K. Selvakumar [1] have discussed the technique in which, the swarm agents are utilized to select the nodes with highest trust value, residual bandwidth and residual energy as active nodes. Each active node monitors its neighbor nodes within its transmission range and collects the trust value from all monitored nodes. The active nodes adaptively changes as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. When the source receives alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. Indirani G and K. Selvakumar [2] have proposed a swarm based detection and defense technique for malicious attacks in mobile ad hoc networks (MANET). In this technique, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using swarm intelligence based ant colony optimization. Each active node monitors its neighbor nodes and estimates the trust value. If the active node finds any node below a minimum trust threshold, then the node is marked as malicious and an alert message is sent to the source node. When the source node wants to forward the data packet to destination, it discards the malicious nodes in that path and bypasses the data through other nodes in alternate path. It also performs the certificate revocation process for the malicious nodes.

S Gowrishankar, T G Basavaraju and Subir Kumar Sarkar[6] have studied the effects of various random mobility models on the performance of AODV. Here three mobility models are used namely Random Waypoint, Random Walk with Reflections and Random Walk with Wrapping. Experimental results illustrate that performance of the routing protocol varies across different parameters like number of nodes, packet delivery ratio and end to end delay.

Patrick Tague et al [8] investigate a class of coordinated jamming attacks in which multiple jammers collaboratively apply knowledge about the network layer functionality to efficiently reduce the throughput of network traffic. They show how a constrained optimization framework can be used to characterize coordinated jamming attacks and allow the impact of the attack to be quantified from the perspective of the network. Using this network-centric interpretation of jamming attacks, a network designer can attain a greater understanding of the potential threat of jamming. To illustrate their approach, they propose and evaluate a variety of metrics to model the attack impact, serving both as adversarial objective functions and as network evaluation metrics. Wenkai Wang et al [9] has proposed cross layer attacks and defending the cross layer attacks in cognitive radios. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. However, the attackers do not necessarily restrict themselves within the boundaries of network layers. In this paper, they design cross-layer attack strategies that can largely increase the attackers' power or reducing their risk of being detected. As a case study, we investigate the coordinated report-false-sensing data attack (PHY layer) and small-back-off-window attack (MAC layer). Furthermore, they propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion. Lei Guang et al [5] demonstrate a new class of protocol-compliant exploits that initiates at the MAC layer but targets ad hoc on-demand routing mechanisms. A misbehaved node implementing this type of attacks completely follows the specifications of IEEE802.11 standard and the existing on-demand routing protocols. However, it can cause routing shortcut attacks or detour attacks. They discuss the exploits against two on-demand routing protocols: AODV and DSR. They evaluate the impact of such attacks on the network performance and propose Prevention from Shortcut Attack and Detour Attack (PSD) to mitigate their impacts.

III. PROPOSED SOLUTION

A.Overview

In this paper, the performance of swarm based intrusion detection system itself is examined under 3 mobility conditions for the various routing attacks in MANET.

B. SWARM BASED NODE MONITORING STRAREGY[1] AND PARAMETERS FOR ACTIVE NODES SELECTION

The parameters used to select the active nodes are residual bandwidth and trust which is described in the following sections.

1) Residual bandwidth calculation

The residual bandwidth is calculated using the local bandwidth and the minimum bandwidth among the neighboring nodes. The difference between the local bandwidth BWloc and Bwmin is the residual bandwidth.

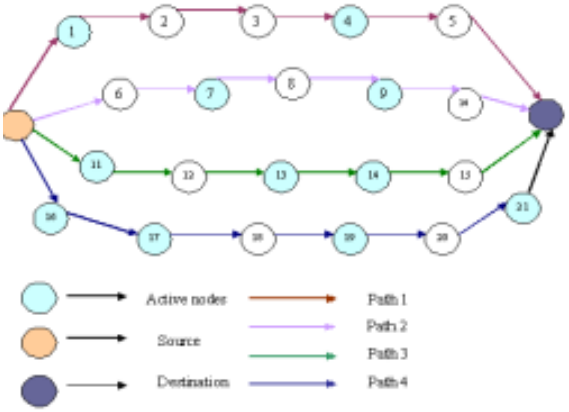

Fig. 1: Swarm based Active nodes selection

2)Trust value (T)

The trust values of the nodes can be estimated from the forwarding behavior of the intermediate nodes. The trust value of a node is decremented if the node does not forward sufficient number of packets or the forwarding delay is high or malicious packets are injected.The active nodes are adaptively changed depending on the above 3 factors.

TABLE-I: HEADER FIELDS ANT AGENTS USED BY SBDTS

Node ID	Seq. no.	Resi. Band Width	Trust

C. Selection of the active nodes

Swarm intelligence technique based on ant colony optimization (ACO) is used for selecting active nodes. The forward ant agent (FA) establishes the pheromone track to the source node (S), while backward ant agent (BA) establishes the pheromone track to the destination (D).

The header of the ant agents (SBDTs) include the fields which are illustrated in table 1. The procedure for selecting the active nodes is given in following algorithm.

Algorithm :

1) Here three SBDTs are created namely SBDT-RWP, SBDT-RWK and SBDT-RD.
2) In each SBDT, the FA is launched in S and it traverses through all intermediate nodes along the path towards D.
3) FA on reaching every node, computes the parameters residual bandwidth and trust(as explained in section 3.2.1.1, 3.2.1.2), and updates its header with the information about the node (as per fig 1).
4) With the gathered information from all the hops, FA reaches D.
5) When FA reaches D, D generates BA and transfers all the information of FA into BA. The BA takes the same path as that of its corresponding FA, but in the reverse direction.
6) The BA updates the header field at the neighboring nodes for all the entries related to the FAs destination node.
7) The BA upon reaching the source delivers the status of all the nodes. The source then selects the nodes with the maximum trust value and residual bandwidth as the active nodes. (shown in fig 1)
8) The steps from 3 to 7 are performed for all three SBDTs mentioned in step 1.
9) Then the performance analysis is performed using the above three SBDTs.

D. Data transmission through secure channel

In each SBDT, the source node selects the path to the destination such that it contains only the valid nodes. Thereby, our technique provides defense against routing layer attacks.

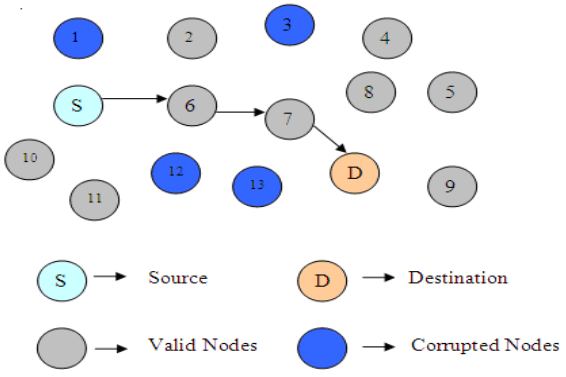

Figure-2 Secure Data transmission

IV. SIMULATION RESULTS

A.Simulation model and parameters

Here the Network Simulator Version-2 (NS2) is used [14] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol is used. It has the functionality to notify the network layer about link breakage.

In this simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The numbers of nodes are set to 100. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and
parameters are summarized in table 2.

B.Performance metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average-end-to-end Delay: It is the total time delay taken by the nodes to transmit the data to the receiver.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

TABLE –II. SIMULATION SETTINGS

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10,20,30,40 and 50 m/s
No. Of Attackers	1,2,3,4 and 5.

C. Results

1) Based on Speed

In the first experiment, the number of nodes are set to 100. The speed of the nodes are varied as 10,20,30,40 and 50 in all the three mobility model based SBDTs.

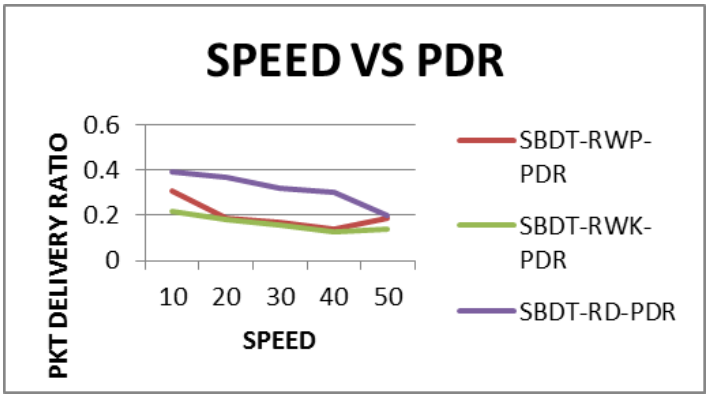

Figure 3:Speed Vs Pkt Delivery Ratio

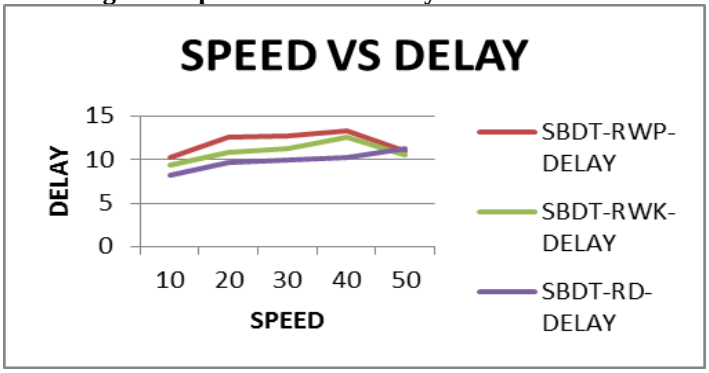

Figure 4: Speed Vs Delay

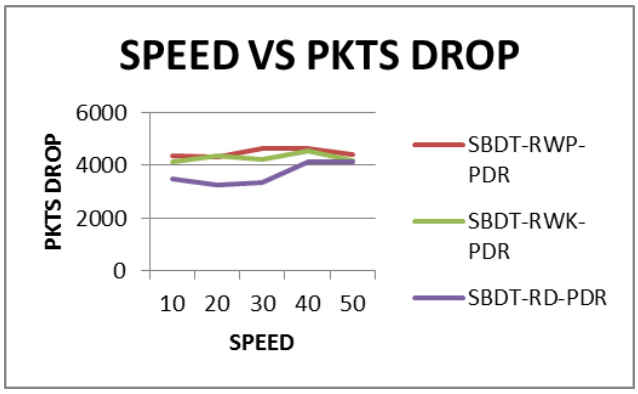

Figure 5: Speed Vs PktsDrop

From figure 3, we can see that the packet delivery ratio of SBDT-RD is higher than the other two mobility model based SBDT techniques.
From figure 4, we can see that the delay of SBDT-RD is less than the other two SBDT based techniques.
From figure 5, we can see that the packets drop of SBDT-RD is lower than the other two SBDT based techniques.
2). Based on attackers
In the second experiment, the number of nodes are set to 100 and the attackers varied as 1,2,3,4 and 5. But the maximum speed of the nodes is set to 10m/sec in all the three mobility model based SBDTs.

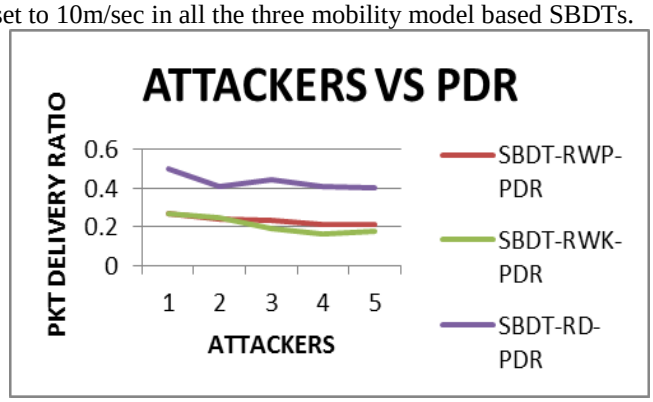

Figure 6: Attackers Vs Delivery Ratio

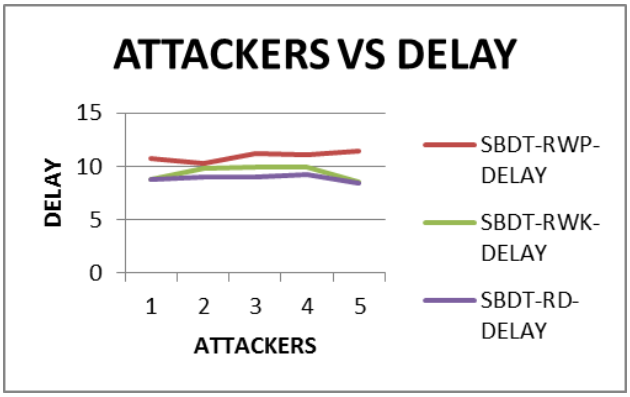

Figure 7: Attackers Vs Delay

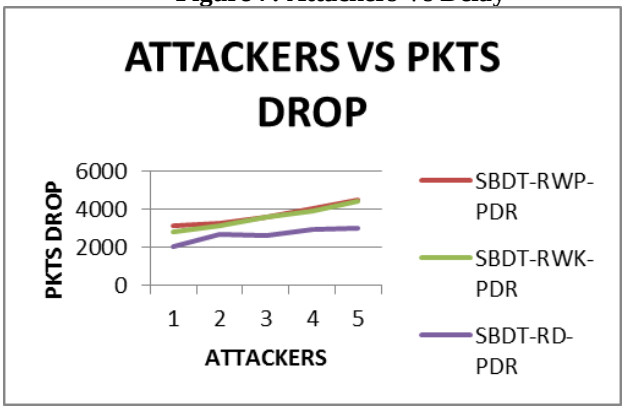

Figure 8: Attackers Vs Pkts Drop

From figure 6, we can see that the packet delivery ratio of SBDT-RD is higher than the other two SBDT based techniques.
From figure 7, we can see that the delay of SBDT-RD is less than the other two SBDT based techniques.
From figure 8, we can see that the packets drop of SBDT-RD is lower than the other two SBDT based techniques.

V. CONCLUSION

In this paper, performance of swarm based intrusion detection system is examined under 3 mobility models by varying the speed and attackers in MANET. All the three SBDTs use the forward and backward ants to select the active nodes (valid nodes) for data transmission. Here two experiments were conducted by varying the speed and the attackers. In both the experiments the performance of SBDT-RD mobility was found to be better than the other two SBDT based mobility models.

REFERENCES

[1] G.Indirani and K.Selvakumar, "A Swarm Based Efficient Distributed Intrusion Detection System for Mobile Ad hoc Networks MANET)",International Journal of Parallel, Emergent and distributed systems(Accepted),2013
[2] G.Indirani and K.Selvakumar, "Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks", International Journal of Computer Applications (0975 – 8887),Volume 50– No.19, July 2012
[3] Sureyya Mutlu, Guray Yilmaz, "A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs", IARIA Seventh International Conference on Networking and Service, 2011
[3] N.Shanthi, DR.LGanesan and DR.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad Hoc Network", Journal of Theoretical and Applied Information Technology, 2009
[4] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS), 2009.
[5] Lei Guang, Chadi Assi, and Abderrahim Benslimane, "Interlayer Attacks in Mobile Ad Hoc Networks", Springer, Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science Volume 4325, pp 436-448 , 2006.
[6] S Gowrishankar, T G Basavaraju and Subir Kumar Sarkar, "Effect of Random Mobility Models Pattern in Mobile Ad hoc Networks",IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, June 2007.
[7] Network Simulator:http://www.isi.edu/nsnam/ns

