Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks

G. Indirani
Assistant Professor
Department of Computer Science and Engineering
Annamalai University, Annamalai nagar- 608002

K.Selvakumar
Phd,Associate Professor
Department of Computer Science and Engineering,
Annamalai University, Annamalai nagar- 608002

ABSTRACT
In mobile ad hoc networks (MANETs), the malicious flooding attack is very hazardous since it not only clogs the victim node but also the entire network. Also it may cause packet drops or alteration of the routing message that will further result in network dysfunctioning. In this paper, we propose 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 neighbour 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. By simulation results, we show that the proposed approach reduces overhead.

Keywords
Mobile ad hoc Networks (MANET), Attacks, Swarm Based Detection, Defense Technique

1. INTRODUCTION
1.1Mobile Ad Hoc Networks (MANET)
A set of wireless communication nodes performing self-configuration in a dynamic mode for formation of network excluding fixed infrastructure or centralized supervision is termed as mobile ad hoc network (MANET). Often, there may be random changes in the network topology as nodes are mobile. In addition to the role of router, the nodes also play the role of end host. The routing protocol in such a network is an authority to determine the routes and offering communication among end points via intermediate nodes. The MANET is well-liked and attractive since they offer good communication in the changing infrastructure for the applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. [1]
The weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [6]

1.2 Attacks in MANET
The MANETs are more susceptible to security attacks rather than wired networks. Due to the facts such as restricted protection of every individual node, uneven behaviour of connectivity, deficit of certification authority, centralized monitoring or administration, security is complicated aspect to be maintained in these networks. In such a wireless network, attacks can enter from all possible way and focus at any node. Hence each node is priorly ready for facing attacks straightly or in a roundabout way. Especially, compromised node attack within the network is critical and the method of identifying it is very complicated. [2]
The mobile ad hoc networks are subject to two types of attacks that include active and passive attacks which are described below.

1.2.1 Active Attacks
An active attack obliterates the data exchanged in the network that distracts the regular functioning of the network. It constitutes two categories such as internal and external attack.

- The compromised nodes within the network executes internal attacks
- The compromised nodes which are away from the network executes external attacks

The following are some of the attacks in particular to active attacks.

- **Wormhole Attack**

The malicious node upon receiving the data packets at one location channels the packet to another location and finally re-transmits the packet into the network. The channel existing among the two colluding attackers is termed as wormhole. This utilizes either a wired link between colluding attackers or a long range wireless links.

- **Black Hole Attack**

The attacker node that wants to interrupt node packets utilizes the routing protocol to establish the false fact that it has shortest path to the node. This is termed as black hole attack. When the malicious nodes are present between the communicating nodes, it performs any sort of action with those packets that crosses them.

- **Byzantine Attack**

The individual or group of compromised nodes function together resulting in routing loops, packet forwarding through non-optimal paths and packet dropping using selective approach which is turn results in routing services degradation. It is very complicated to identify these type of attack and it is termed as Byzantine attack.

- **Information Disclosure**

There is a possibility that compromised node discloses the secure or main information to malicious nodes in the network. This activity results in exposure of secure information related to network topology, geographic location or best possible routes of the approved nodes in the network.

- **Resource Consumption Attack**

In resource consumption attack, an attacker attempts to consume limited availability of resources such as battery power, bandwidth and computational power of other nodes in the network. The various forms of attacks include needless requests for routes,

repeated production of beacon packets or forwarding worn-out packets to nodes.

1.2.2 Passive Attacks

This type of attack intrudes the data exchanged within the network without modifying it such that the regular behaviour of the network is not affected. This type of attack is complicated to identify as the normal operation of the network is not affected. [2] [4]

There is an attack which is specific to the passive attack whose brief description about it is given below:

- **Snooping**

Snooping refers to the illicit use of another person's data. This may refer to watching e-mail informally that is displayed on another's computer screen or observing other people typing. Also more complicated snooping involves a software program to examine the process of a computer or network device. [5]

1.3 Defense Mechanism in MANET

The defense mechanism for distributed denial of service (DDoS) involves the following three actions

(i) Attack detection
(ii) Attacking source detection
(iii) Filtering the distrustful packets by controlling the attacking traffic.

1.3.1 Necessity of Defense Mechanism in MANET

- During route discovery process in AODV protocol, the malicious flooding attacker floods the route request packets through the victim node symbolizing as setting up a path.
- Following the path establishment, the attacker floods data packets through the victim node for paralyzing the node. As the packet size of these data packets is much larger than the route request packet, the victim nodes gets congested easily.
- The attackers consume the battery power of the victim node thus separating them from the network. Hence the malicious flooding attack leads to denial of service (DoS) attack on the victim node. Thus there is a worsening in the act of processing the valid packets at the victim node.
- As the malicious flooding attack congests the victim node as well as the entire network, it is very harmful to the mobile ad hoc network. Also it is very difficult to avoid this attack when it is caused by the multiple attackers. [11]
- The flooding and packet dropping attacks preventing the network service availability results in ineffective secure routing. [13]
- A malicious node can manipulate routing messages and also causes packet drops selectively which may result in network dysfunctioning. [14]
- The general form of security violation is the DDoS attack where the attackers floods huge incoming packets over the victim nodes. [12]
- Generally in wireless networks, attackers introduce the false packets effortlessly imitating another sender which is termed as spoofing attack. [15]

In order to overcome all these issues, it is necessary to develop a defense mechanism against malicious flooding attacks.

1.4 Problem Identification

In paper [7], a swarm based efficient distributed intrusion detection system for MANET is proposed. This technique involves selection of nodes with maximum trust values, residual bandwidth and residual energy using swarm agents. Each active node monitors its neighbour nodes within its transmission and collects the trust values from all the 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 need to be deployed to filter the corresponding malicious attack for MANET.

Thus in this paper, we propose an efficient defense mechanism against malicious attack in MANET.

2. RELATED WORKS

Quan Jia et al [8] have proposed a novel capability based secure communication mechanism called CapMan. This technique mitigates denial of service attacks on MANETs by regulating end-to-end traffic communicated over multiple paths. Also it empowers individual nodes to maintain global flow state which in turn enables them to both setup and enforce bandwidth limits in a distributed fashion.

S.Venkatasubramanian and N.P.Gopalan [10] have proposed a distributed defense technique to mitigate the DoS attacks. The technique for monitoring the node selection is designed that detects all affected packets while selecting the monitoring nodes so as to cover the entire network. Following the estimation of the short-lived flows, when the total traffic load exceeds the threshold, an attack is detected and the attacker is added into a local blacklist. The monitoring nodes sends the Blacklisted nodes to the master node and the attacker will be alerted via the notification message to make the nodes aware of the attacker.

HyoJin Kim et al [11] have proposed a novel defense mechanism against malicious flooding attacks, performed by collaborative attackers. The various attacks have been categorized as per the possible malicious flooding attacks. They defend against the malicious flooding attacks, collaboratively conducted by flooding nodes using RREQ packet, data packets, or both. The effect of packet delivery ratio with the increase in the number of malicious node is not considered in this approach.

Rizwan Khan, and A. K. Vatsa [16] have proposed the detection and control mechanism for DDoS attacks over reputation and score based MANET. The architecture worked in three phases. In first phase, the cluster creation and cluster head selection is performed based on reputation. The second phase involves the detection strategies of DDoS attacks such as message bombing and cache poisoning. In the third phase, a control frame packet format is demonstrated that defends the DDoS attacks. The issues such as mobility and scalability are not considered in this work that degrades the QoS and performance of the network.

Hai Vu et al [17] have proposed a framework to detect wormhole attacks in wireless networks (Wormeros). This framework includes two phases such as suspicion and confirmation. The first phase utilizes local information existing at the time of regular operation of wireless nodes. In the second phase, only when a wormhole attack is suspected, advanced techniques are applied. This reveals that there will be no necessity for the wireless nodes

to waste computation and communication resource when there are no wormholes in the network.

Chaorong Peng and Chang Wen Chen [18] proposed an algorithm to enhance the defense against malicious attack (IDMA) based on Assignment Router Identify Protocol (ARIP) protocol. In the ARIP protocol, they designed the ARIP architecture based on the new Identity instead of the vulnerable IP addresses to provide the required security that is embedded seamlessly into the overall network architecture. The proposed protocol is aimed to minimize the costs of network monitoring and provide a degree of defense against malicious nodes attack.

3. SWARM BASED DETECTION TECHNIQUE FOR MALICIOUS ATTACK

3.1 Overview

In this paper, we propose a defense mechanism against malicious attacks in mobile ad hoc networks (MANET). In this technique, multiple paths are established among source and destination for data transmission using swarm intelligence of ant colony optimization. In the selected routes, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using ant agents. Each active node monitors its neighbour 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. Upon detecting malicious node, the active node sends an alert message to the source node. When the source node wants to forward the data packet to D, it discards the malicious nodes in that path and bypasses the data through other nodes in alternate selected path towards D and performs the certificate revocation process for defending against the malicious nodes.

3.2 Intrusion Detection Technique

Let S and D represent the source and destination respectively

Initially multiple paths are established among S and D for data transmission using the swarm intelligence of ant colony optimization. In the selected route, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes. The swarm intelligence based ant colony optimization is utilized for selecting the active nodes (NA). Each NA monitors the trust values of its neighbouring nodes within its transmission range. The NA collects the trust values from the monitored nodes and exchanges the collected information with its neighbour NAs. After the information exchange, NA verifies the trust value of each monitored node. If the trust value of a particular node is below a minimum trust threshold, it notifies the malicious node detection. After the detection of malicious nodes, the NA sends the alert message (MA) to S. Similarly, all the NAs perform the trust message exchange technique and upon intrusion detection forwards the MA towards the S. S stores the path number and node ID details in which the malicious node is detected in its routing table. As the threshold levels of the trust value keeping varying, the nodes also keep changing from their active states in the adaptive manner. [7]

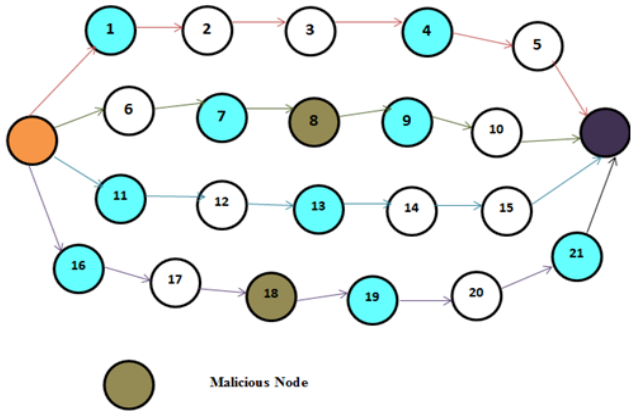

Figure 1: Intrusion Detection

4. DEFENSE MECHANISM FOR MALICIOUS ATTACKS

When the source node wants to forward the data packet to D, it discards the malicious nodes in the path and bypasses the data through other nodes in alternate selected path towards D (shown in figure 2) and source performs the key revocation process for defending against the malicious nodes (explained in 4.3)

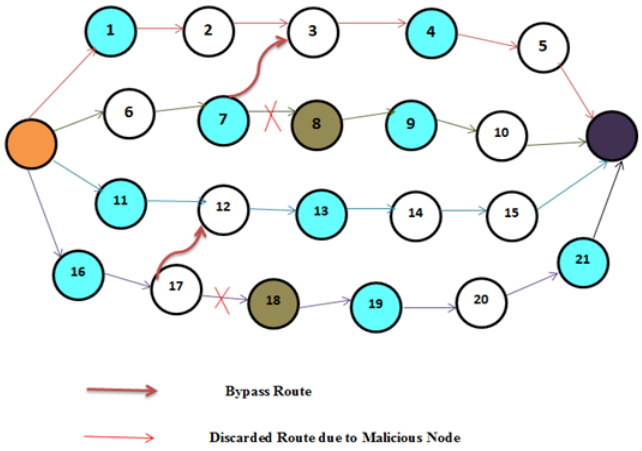

Figure 2: Bypass Routing

An example of intrusion detection is illustrated in Figure 1

In path 1, active node NA_4 monitors N_3, N_8, and N_5. It collects the trust information from all these nodes and exchanges the gathered information with NA_9. From the exchanged information, it is found that trust value of N_8 is below a minimum threshold. This reveals that N8 is a malicious node. Then NA_4 sends an alert message (MA) to source node S about the malicious node. S stores path number (path 2) and node ID of N_8 in its routing table. When S forwards the data through path 2, it discards N_8 and uses N_3 in path 1 as alternate node to proceed with DP forwarding towards D using bypass routing technique.

Similarly in path 3, NA_{13} monitors the N_{12}, N_{14}, N_{17}, and N_{18}. It collects the trust information from all these nodes and exchanges the gathered information with NA_{19}. It is found that trust value of N_{18} is below a minimum threshold. This means that N_{18} is a malicious node. Then NA_{13} sends an alert message (MA) to S regarding malicious node. S stores path number (path 2) and node ID of N_8 in its routing table. When S forwards the data through

path 4, it discards N_{18} and uses N_{12} in path 3 as alternate node to proceed with DP forwarding towards D using bypass routing technique.
The active node keeps changing adaptively as per the threshold levels of trust value.

4.1 Proactive Secret Sharing Technique

The threshold cryptography helps in sharing the secret among the nodes. A proactive secret sharing technique (PSS) can be employed along with the threshold cryptographic technique in order to make the sharing scheme more secured. This scheme permits refreshment of all shares by generating a new set of shares for a similar secret key from the old shares exclusive of renovating the secret key.
Let K represent the secret key and k_{i1}, k_{i2}…., k_{in} represents the sub-key. Let the node N_i hold the key.
The Proactive secret sharing technique can be described using the following steps.

1) N_i randomly generates its sub-keys $k_{i1}, k_{i2}, ..., k_{in}$
2) Every sub-key k_{ij} (b=1, 2,…, n) is distributed to node N_j through secure link.
3) When N_j receives the sub-keys $k_{1j}, k_{2j}, ..., k_{nj}$, it calculates a new key from the received sub-keys and old keys using the following equation.

$$k_j^{'} = k_j + \sum_{i=1}^{n} k_{ij} \quad (1)$$

4) 4) Each new key (k1',k2'……kn') is sharing of the secret key K, since $\sum_{j=1}^{n} k_{ij} = 0, \forall i \in \{1,...., n\}$.

4.2 Certificate Renewal Process

Each node deployed in the network holds a certificate signed by the secret key K that contains the fields such as Node ID, signature period, and expiration period (using equation (1)). Also each node holds a certificate revocation list (CRL) based on certificate revocation mechanism and each CRL is associated with the soft-state timer. As nodes are certified, a malicious node has no possibility to reveal the certificate of any other nodes.

$$\text{Node n} \leftarrow K[ID, t_s, t_e] \quad (1)$$

In prior to the expiry of the current certificate, each node looks for its neighbours within two-hop distance for certificate renewal (CR). The steps involved in the CR are as follows.

- The node that needs CR broadcasts a certificate renewal request (CR_{req}) packet to its neighbours that include current certificate and time stamp (TS).
- A node upon receiving CR_{req} packet from its neighbours extracts the certificate from the packet and compares it with the CRL. i.e. verifying whether the certificate has previously been revoked.
- On comparison, if the certificate is valid, then a new certificate is constructed similar to the older one that holds the equivalent time stamp as that in CR_{req} packet. On the other hand, if CR_{req} has revoked certificates, then it is dropped.
- Then the new certificate is signed with its own private key (k_{pr}) and the certificate reply packet CR_{rep} encapsulates by this partially signed certificate is unicasted back to the node from which it received C_{Rreq}.
- When the requested node receives CR_{rep} packets from its different neighbours, it gathers all the partially signed certificates into a single certificate signed with k_{pr}.

4.3 Certificate Revocation Process

When a malicious node is detected, MA is sent to S by the active nodes (explained in section 3.4). When S receives a multiple MA for the same node, it performs the following actions.

- Generates the certificate revocation (C_{rev}) notification.
- Signs the C_{rev} using its own share of $k_{pr.}$
- Broadcasts C_{rev} to other nodes.
- The certificate revocation process is initiated.

When a node receives a C_{rev} packet, it verifies whether the packet is signed and also whether the revoked certificate is already in the CRL. If C_{rev} packets are not signed by the k_{pr} or contain certificates on CRL, then it is dropped. Otherwise node adds the revoked certificate is added to its own CRL and re-broadcasts the C_{rev} packet. This process allows every node to add the revoked certificate into its CRL. As only nodes with valid certificates can take part in the network operations, this certificate revocation mechanism guarantees that a malicious node is isolated following its detection. Also to make sure that a malicious node should not renew its certificate, a revoked certificate has to be kept in CRL until it expires, after which it can be deleted.

5. SIMULATION RESULTS

5.1 Simulation Model and Parameters

We use Network Simulator Version-2 (NS2) [22] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.
In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We have varied the number of nodes as 20, 40, 60, 80 and 100. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1

Table 1. Simulation Settings

No. of Nodes	20, 40, 60, 80 and 100.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
No. Of Attackers	1,2,3,4 and 5.
Initial Energy	10.5 J
Transmission Power	0.660
Receiving Power	0.395
Idle Power	0.035

5.2 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.

Avg-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.

We compare our Swarm Based Detection and Defense Technique (SBDT) with the CAPMAN [8].

5.3 Results

A. Based On Attackers

In the first experiment, we vary the number of attackers as 1, 2, 3, 4 and 5 in a 100 node network.

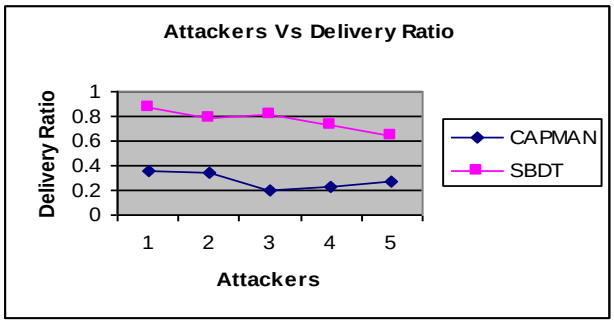

Figure 3: Attackers Vs Delivery Ratio

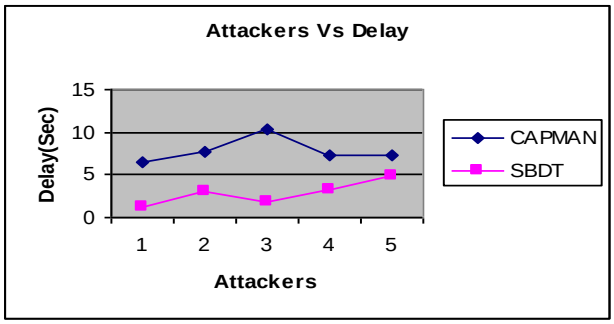

Figure 4: Attackers Vs Delay

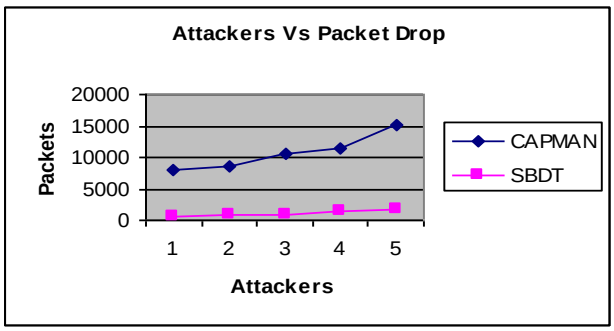

Figure 5: Attackers Vs Drop

From figure 3, we can see that our proposed SBDT achieves high delivery ratio than the existing CAPMAN technique.

From figure 4, we can see that out proposed SBDT has less delay than the existing CAPMAN technique.

From figure 5, we can see that out proposed SBDT has less packet drop than the existing CAPMAN technique.

Detection Accuracy

We measure the false detection ratio and detection accuracy in terms of percentage. Figure 6 shows the false detection percentage is considerably less for SBDT, when compared with CAPMAN. Also from figure 8, we can see that the detection accuracy for SBDT is slightly more than that of CAPMAN.

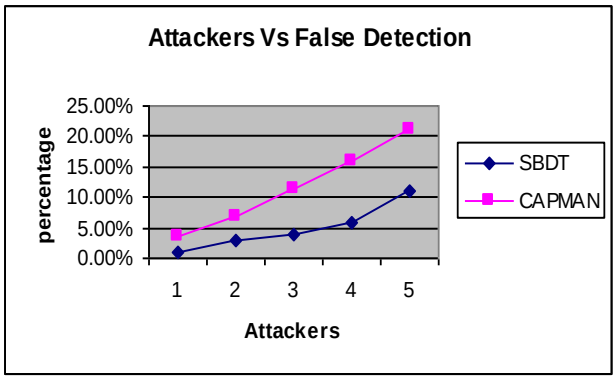

Figure 6: Attackers Vs False Detection Percentage

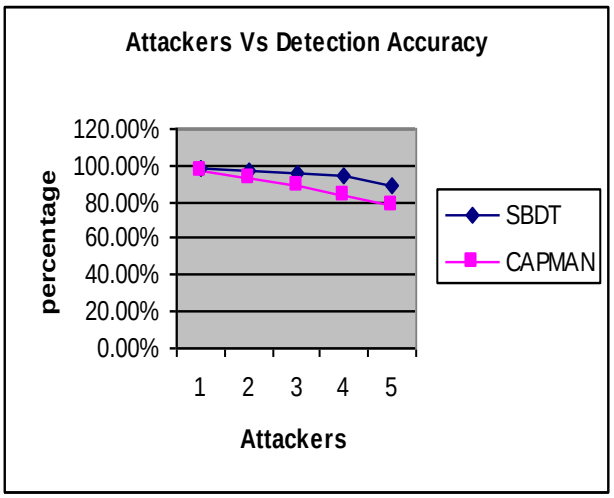

Figure 7: Attackers Vs Percentage of Detection Accuracy

B. Based on Nodes

In the second experiment we vary the number of nodes as 20, 40, 60, 80 and 100 keeping the number of attackers as 4.

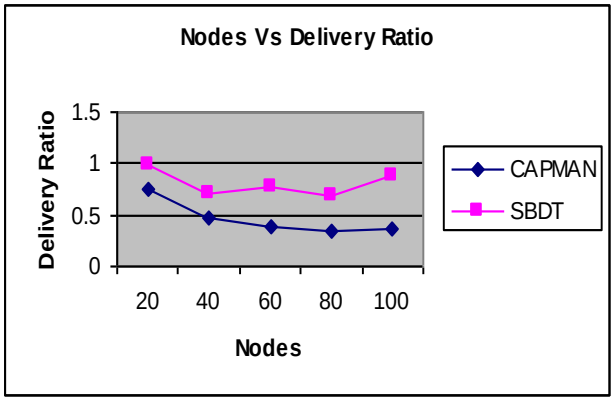

Figure 8: Nodes Vs Delivery Ratio

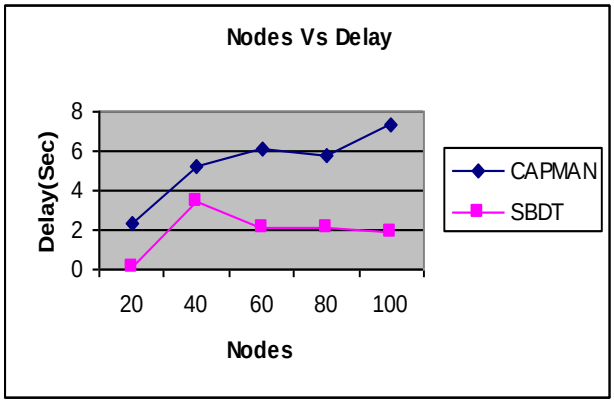

Figure 9: Nodes Vs Delay

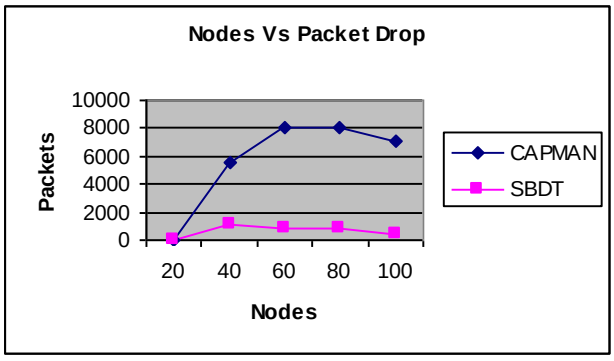

Figure 10: Nodes Vs Drop

From figure 8, we can see that our proposed SBDT achieves high delivery ratio than the existing CAPMAN technique.

From figure 9, we can see that out proposed SBDT has less delay than the existing CAPMAN technique.

From figure 10, we can see that out proposed SBDT has less packet drop than the existing CAPMAN technique.

6. CONCLUSION

In this paper, we have proposed a swarm based detection and defense technique for malicious attacks in mobile ad hoc networks (MANET). In this technique, multiple paths are established among source and destination for data transmission. In the selected routes, 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 neighbour 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. Upon detecting malicious node, the active node sends an alert message to the source node. When the source node wants to forward the data packet to D, it discards the malicious nodes in that path and bypasses the data through other nodes in alternate selected path towards D and performs the certificate revocation process for defending against the malicious nodes. By simulation results, we have shown that the proposed approach accurately detects the attacks and minimizes the packet drops due to attacks.

7. REFERENCES

[1] Sevil Sen, and John A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks", Proceedings of the second ACM conference on Wireless network security (WiSec '09).

[2] Sureyya Mutlu, and Guray Yilmaz, " A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs", The Seventh International Conference on Networking and Services(ICNS), pp 292 to 298, 2011

[3] Sumitra Menaria, Prof Sharada Valiveti, and Dr K Kotecha, "Comparative study of Distributed Intrusion Detection in Ad-hoc Networks", International Journal of Computer Applications, Volume 8– No.9, October 2010.

[4] N.Shanthi, Dr.L.Ganesan, and Dr.K.Ramar, " Study of different attacks on multicast mobile ad hoc networks", Journal of Theoretical and Applied Information Technology, 2005-2009

[5] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265 pp 245-74.

[6] S. Mangai, and A.Tamilarasi, "An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System in Mobile Ad Hoc Networks", Journal of Computer Science., pp 505-511, 2011.

[7] G.Indirani, and Dr.K.Selvakumar ,"A Swarm Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)"

[8] Quan Jia, Kun Sun, and Angelos Stavrou, " CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET", Proceedings of 20th international conference on computer communications and networks (ICCCN), pp 1 – 6, 2011

[9] Alicherry, M, Keromytis, A.D, Stavrou. A, "Evaluating a collaborative defense architecture for MANETs", IEEE International conference on internet multimedia services architecture and applications (IMSAA), pp 1 – 6, 2009.

[10] S.Venkatasubramanian, and N.P.Gopalan, "A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET", International Journal of Computer Applications (IJCA), pp 7-11, 2011.

[11] HyoJin Kim, Ramachandra Bhargav Chitti, and JooSeok Song,"Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[12] Hwee-Xian Tan, and Winston K. G. Seah, "Framework for Statistical Filtering Against DDoS Attacks in MANETs", 2nd international conference on embedded software and systems, pp 8, 2005.

[13] Venkatesan Balakrishnan, Vijay Varadharajan, and Udaya Kiran Tupakula, "Fellowship: Defense against Flooding and Packet Drop Attacks in MANET", IEEE /IFIP Network Operations and Management Symposium (NOMS), pp 1-4, 2006.

[14] Wei Yu, Yan Sun, and K. J. Ray Liu, "HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks", Proceedings: 24th annual joint conference of the IEEE computer and communications societies (INFOCOM), pp 1252 – 1261, vol. 2, 2005.

[15] Hu, Y-C, Perrig, A.; Johnson, D.B., " Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", 22nd Annual Joint Conference of the IEEE Computer and Communications (INFOCOM), pp 1976 - 1986 vol.3, 2003

[16] Rizwan Khan, and A. K. Vatsa, "Detection and Control of DDOS Attacks over Reputation and Score Based MANET", Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 11, October 2011.

[17] Hai Vu, Ajay Kulkarni, Kamil Sarac, and Neeraj Mittal, " WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks", Proceeding of the Third International Conference on Wireless Algorithms, Systems, and Applications (WASA), 2008

[18] C. W. Chen, "IDMA: improving the defense against malicious attack for ad hoc networks based on ARIP," Proceedings of SPIE Defense and Security Symposium Conference on "Mobile Multimedia/Image Processing, Security, and Applications, March 2008, Orlando, USA

[19] Vinay Rishiwal, S. Verma, and S. K. Bajpai, "QoS Based Power Aware Routing in MANETs", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009.

[20] Tolba, F.D. Magoni, D. Lorenz, P, "Connectivity, Energy and Mobility Driven Clustering Algorithm for Mobile Ad Hoc Networks", IEEE Global Telecommunications Conference (GLOBECOM), pp 2786-2790, 2007.

[21] Yaling Yang, and Kravets, R, "Contention-Aware Admission Control for Ad Hoc Networks",IEEE Transactions on mobile computing", pp 363-377, Vol 4, issue 4, 2005.

8. AUTHOR'S PROFILE

Mrs. G. Indirani received B.E degree in Computer Science and Engineering from Annamalai University in 1995. She received M.E., degree in Computer Science and Engineering from Annamalai University, Annamalainagar in the year 2007. She has been with Annamalai University, since 2000. She is doing her Ph.D in Computer Science and Engineering at Annamalai University. She published 2 papers in international conferences and journals. She is the author of the book namely, "Data Structures using C", Tata McGrawHill Publishers in the year 2008. Her research interest includes Computer Networks, Mobile Ad hoc Networks and Network Simulator.

Dr. K. Selvakumar received B.E degree in Electronics and Communication Engineering from Kongu Engineering College in the Year 1989. He received M.E degree in Communication Systems from Regional Engineering College in the year 1997. He has been with Annamalai University, since 1999. He completed his Ph.D., degree in Computer Science and Engineering at Annamalai University, in the year 2008. He published 30 papers in international conferences and journals. His research interest includes Computer Networks, Cryptography and Network Security, Wireless Networks, Mobile Adhoc Networks and Network Simulator.