Avoid Packet Replication Attack Based on Intrusion Detection and Defense Mechanism over MANET

, [1]Radhakrishnan S. R, [2]MuthuKumar. S
[1]PG Student, Dept of CSE, Sree Sowdambika College of Engineering, Tamilnadu, India.
[2]Assistant Professor, Dept of CSE, Sree Sowdambika College of Engineering, Tamilnadu, India.

***Abstract* - In the MANET, much more vulnerable attack is possible than a wired network. An Intrusion Detection System (IDS) for MANETs is designed to detect anomalous behavior and abuse. Swarm intelligence is a relatively novel field. It shows the desirable properties of being adaptive, scalable, and robust. The goal of this system framework is to detect and perform defense mechanism for packet replication attack and reduce the battery consumption energy of the node. The Packet Replication Attack is an internal attack which attack makes the situation repetitively transmit stale packets inside the network. The number of replication times is identified by the number of route entries for the destination, each and every data packet is individually identified with the tree-id provided by NS2 and the inordinate packets are discarded in the IP layer at the receiver. The battery consumption energy can be saved using the Mesh Network topology. The performance of the IDS is confirmed using the parameters like Throughput Average Packet Received Ratio, Average Packet Delivery Ratio and Average End to End Latency.**

Keywords – Mobile Ad hoc Networks (MANET), Attack, Intrusion Detection System, Swam intelligence, Packet Replication

I. INTRODUCTION

Recent researches in wireless communication and the smallness of computers have led to a new concept called the mobile ad hoc network (MANET), where two or more mobile Nodes can generate a temporary network without the use of any already presented network infrastructure or centralized administration. If the source and the destination mobile node are not within the communication range of each other, data packets are forwarded to the destination mobile host by relaying the transmission through other mobile hosts which exist between the two mobile hosts. Here no special infrastructure is needed, in various fields such as military and rescue affairs, many applications are expected to be developed for ad hoc networks. A mobile adhoc Network is a collection of autonomous nodes or terminals which communicate with each other by forming a multihop radio network.

Each device in a MANET is free to move independently in any direction. In contrast to the Cellular System there is no master slave relationship. If a network is a partitioned into two networks due to the migrations of mobile hosts in one of the partitions cannot access data items held by mobile hosts in one of the partitions cannot access data items held by mobile hosts in the other. Thus data accessibility in ad hoc networks is lower than that in conventional fixed networks. A possible and hopeful solution is the replication of data items at mobile hosts that are not the owner of the original data. Since mobile hosts generally have poor resources, it is usually not possible for them to have replicas of all data items in the network.

A. Wormhole Attack

In wormhole attack, a malicious node adversary receives packets at one location in the network and tunnels them to another location in the network, then that packets are resent into the network, this tunnel between two colluding attackers is called wormhole.

B. Black hole Attack

In this attack an attacker hears the request for routes in a flooding based protocol. In this attack the attacker receives the request for a route to the destination node, which creates a reply consisting of an extremely short route. If the malicious reply reaches the initiate node before the reply from the real node, a false route gets created. Once the malicious device able to insert itself between the communicating nodes, it is capable to do misbehavior action between them. Brief descriptions of such attacks are specified below.

C. Routing Table overflow

Incase of routing table overflow, the attacker establishes routes to nonexistent nodes. The goal is to create enough routes to avoid novel routes from being created or to overwhelm the protocol implementation. In proactive routing algorithms, it is necessary to discover routing information even before it is needed. In the reactive algorithms it is compulsory to find a route only when it is needed.

D. Routing Table poisoning

In routing table poisoning the compromised nodes there in the network send fabricated routing updates or modify genuine route updates packets sent to other approved nodes. Routing table poisoning might result in sub-optimal routing. Congestion in portion of the network, or even construct a few parts of the network inaccessible.

E. Packet replication Attack

A packet replication attack is an internal attack which the attacker belongs to the same network and attacks the recourse within the network. In the Packet Replication attack is perform the attacker replicates stale and sends them to trigger network. That result in loss of bandwidth of the network and also causes unnecessary confusion in the routing process.

F. Rushing Attack

On-demand routing protocol which use duplicate during the route innovation process are vulnerable to this attack. An attacker which receives a route request packet from the initiate node flood the packet rapidly throughput the network before further nodes which also receive the same route request packet can respond. Nodes that receive the lawful route request packet previously received through the attacker and hence discard those packets.

G. Problem Identification

In this paper a swarm based well-organized distributed intrusion detection system for MANET is proposed. The Watchdog technique is the overhearing technique. In the watchdog mechanism identifies any fault nodes by promiscuously listening to the after that node in the packet's path using swarm agents. Each active node monitors its neighbor nodes within its transmission and collects the belief values from all the monitored nodes. If active node finds any node below a minimum trust threshold, then the node is noticeable as malicious.

The Pathrater isolate the misbehaving node from the network. In the Pathrater mechanism keep rate for every further node in the network it knows about. The Pathrater module uses the information generated by watchdog to choose the better route to deliver the packet. Thus in this paper, an efficient defense mechanism is proposed against packet replication attack in MANET

II. RELATED WORK

K.Ramanarayana and LillyKutty Jacob have proposed a lightweight solution for secure routing in integrated mobile ad hoc network (MANET) Internet. The proposed framework represented as bellowed:

Application of IBC to ad hoc networks for efficient key management and for the distribution of pair wise shared keys among the authenticated nodes; Providing protected Internet connectivity while the mobile node (MN) roams across different wireless domains operated by different agent and operators; and design of a lightweight secure ad hoc on demand distance vector routing protocol for intra-MANET routing which protect all the fields of the routing packet including hop count. Security and performance analysis prove that our proposed framework achieve excellent security while keep the overhead and latency minimal.

Wilson EO and Belknap Press and Wu SX and Banzhaf W. have proposed the Intrusion detection based upon computational intelligence is now attracting considerable interest from the research area. Characteristic of computational intelligence system, such as adaptation, fault resilience in the face of noisy information, fit the needs of building a good intrusion detection model. An overview of the research progress is provided in applying CI methods are provided in applying CI methods are provided to the problem of Intrusion detection.

Indirani and Dr. K.Selvakumar have proposed the malicious flooding attack is extremely dangerous. Also it may cause packet drop or modification of the routing message that will further result in network dysfunction. In the paper swarm based detection and defense technique for malicious attacks in mobile ad hoc networks (MANET) is proposed. In this technique the nodes with higher trust value, residual bandwidth and residual energy are elected as active nodes by using swarm intelligence based ant colony optimization. Each active node monitors its nearest nodes and estimates the trust value.

Zhou Lianying and Fengyu have proposed a swarm intelligence-based intrusion detection technique in order to reduce the misjudgment & misdetection and increase the real-time reply in the existing intrusion detection techniques.Seperating a huge and complicated intrusion detection system into server independent detection units with unique function so that the amount of detection data processing and the complexity of detection data processing and the complexity of detection data processing and the complexity of detection signature selecting ,which are the most important factors affecting the application performance of existing intrusion detection techniques, are reduced significally.

Zinal A and Maarof MA and Shamsuddin SM have proposed the existing IDS use all the features in network packet to evaluate and look for well-known intrusive pattern. Some of these features are unrelated and redundant. The disadvantage to this approach is a lengthy detection process. In a real time environment this may degrade the performance of AIDS.

Yang H and Luo H and Ye F and Lu S and Zhang L. have proposed fundamental security problem of protecting the multi-hop network connectivity between mobile nodes in a MANET is focused. The security issues related to this problem are identified and discussed the challenges in security issues related to this problem are identified and discussed the challenges in security design. and evaluate the state-of-the –art security proposals that protect the MANET link and network layer operations of delivering packets over the multi hop wireless channel. The Whole security solution should span both layers, and cover all three security mechanism of prevention, detection, and avoidance.

III. INTRUSION DETECTON TECHNIQUE OVER SWARM INTELLIGENCE

A. *Overview*

In this paper, a defense mechanism against malicious attacks is proposed in mobile ad hoc networks (MANET).In this technique; multiple paths are established between source and destination for data transmission using swarm intelligence of ant colony optimization. In the elected routes, the nodes with maximum trust value, residual bandwidth and residual energy are elected as active nodes by using ant agents. Every active node monitors its neighbor nodes within its transmission region and collects the trust of all monitored node. The active nodes adaptively change as per the trust thresholds.

B. Intrusion Detection System

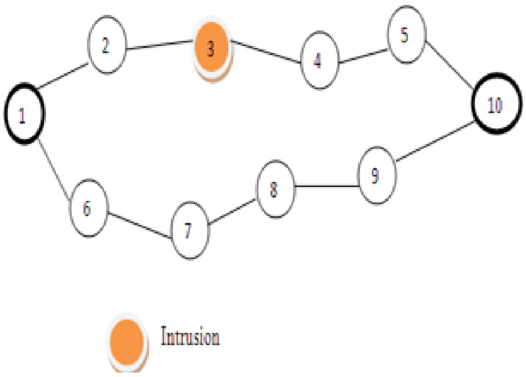

Figure 2: Intrusion Detection

In this paper a detection based security scheme is provided for Mobile Adhoc network (MANET).Although MANET has low computation and communication capacity, they specific properties such as their constant neighborhood information that permit for detection of anomalies in the networking nodes. In many attacks against Mobile adhoc networks, initially attacker is to make itself as a legitimate node within the network.

C .Ids Techniques for MANET

A selfish node wants to protect its own resource when using the services of others and generating their resources when using the service of their resources. There are two approaches for dealing with their selfish nodes. The first one gives a motivation for participating in the network function. The second approach detects and excludes misbehaving nodes. Most existing systems belong to the second type.

The watchdog/Pathrater is a solution to be the problem of selfish or fake nodes in MANET. The watchdog techniques notice the misbehaving nodes and the Pathrater, to take action against the intrusion by isolating the selfish or misbehavior node from the network operation.

Watchdog runs on each and every node. When node forwards a packet, the watchdog module verifies that the next node in the path also forward the packet. In the watchdog technique which listening and monitor the next node's after the transmissions. If the next node does not forwards the packet, then it is considered to be misbehaving and is reported to all nodes.

This is done by sending an alarm message to the further nodes on its friends list. When those nodes get the alarm message, they evaluate it and modify the reputation of the accused node only if the alarm is entirely trusted other same node was accused by partially trusted nodes.

C1. Watchdog module:

If the Watchdog module that detected the misbehaving node is not in the similar node that is acting as source node for the packets, then it sends a message to the source identifying the misbehaving or selfish node. The Pathrater module uses the information generated by Watchdog to select a better available route to deliver the packets, avoiding the misbehaving or selfish nodes.

The Watchdog technique identifies some misbehaving nodes by promiscuously monitoring to the next node in the packet's path. If dropped more than packets dropped occur across the predefined threshold value, which is notified. discovery a misbehaving node along the selected path.

The Watchdog module was implemented by maintaining a buffer of recently send packets as well as comparing every overhead packet with the packet in the buffer to observe if there is a match.

C2. The Pathrater

After the Watchdog detects the malicious node the Pathrater module then neglect the corresponding route from the route cache and try to determine if there is another route obtainable to other destination by looking in its cache table. If suppose route is not available, then the Pathrater broadcast a Route Request get a novel route to reach the destination.

C3. Swarm Intelligence:

Swarm intelligence is the decentralized and self organizing system. Each and every node take the decision its own to transmit the packet while finds the malicious node in the network. The main advantage of this technique does not wait for source node to retransmit. This methodology is used to avoid unnecessary and repeated transmission in the network.

IV. PROPOSED SYSTEM

Swarm intelligence is the self organizing technique. Each and every node has highly utilized in this methodology. Using the swarm intelligence the battery consumption or energy of the node becomes low. Due to the energy loss the attacker can easily compromise that node and to perform the misbehaving action through that node.

While the node forward the packet in some delay which node may be become the malicious node. This delay node identifies and recovered in the routing path by using the Mesh network.

In mesh network each device communicates its routing information to every device connects itself. All nodes have the recently updated routing information about the network. According to that information each node can passed the data to the valid nearest node not for the all nearest node. Due to this methodology battery consumption power of the each node can be saved.

V. PERFORMANCE METRICS

The performance is evaluated according to the following metrics:

1. *Average packet Delivery* Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
2. *Average end to end Delay*: It is the total time delay taken by the nodes to transmit the data to the receiver
3. *Average Packet Received:* It is the average number of packets dropped by the misbehaving nodes
4. *Energy Consumption:* It represents the energy of the node for transmission.

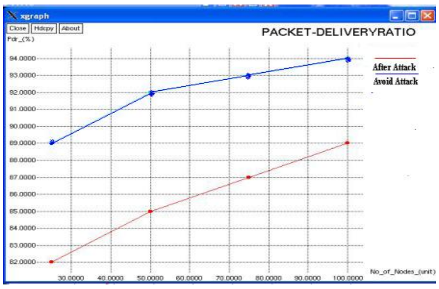

Figure 3: Node vs. Packet Delivery Ratio

In this X-graph the performance evaluated based on the Packet delivery ratio. Here the X axis consider as the No of Nodes and Y axis consider as the packet delivery ratio in percentage. Here the performance evaluated should be different by the two lines.

When the watchdog technique used the packet delivery is very low which should be represented in the red line. Watchdog technique every node listening the neighboring node whether the packet are transmitted. If anyone node does not forward the packet at properly. Then the selfish node is there. Then isolate the attack using the Pathrater technique. Using Swarm intelligence each node identifies the alternate path itself. After implementing the watchdog and swarm intelligence technique, the Packet delivery ratio is increased slightly this is represented in the blue line.

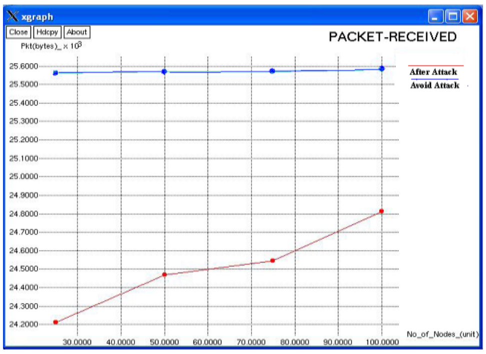

Figure 4: Node vs. Packet Received Ratio

In this x graph the performance evaluated based on the packet received ratio. Here the x axis considers as the no of nodes and Y axis consider as the packet received ratio in percentage. Before the attack the successive received packet ratio is very low.

The watchdog module was implemented by maintaining a buffer of recently sent packet and comparing each overhead packet with the packet in the buffer. to see if there is a match. In the catch buffer the same packets is forward at respectively. Then malicious attack is there. After ignore the malicious attack by using the watchdog and swarm intelligence technique. The packet Received ratio is increased slightly.

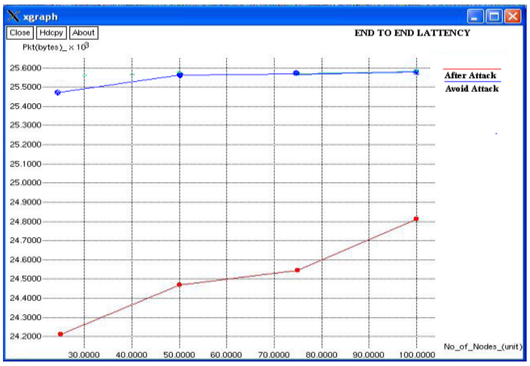

Figure 5: Node vs. Delay

In this x graph the performance evaluated based on the packet delivery ratio, Here the X axis consider as the No of the modes and Y axis consider as the packet delay ratio in percentage

Watchdog technique detects malicious misbehavior by promiscuously listening to its next hop's transmission. Which means Each and Every node in the network listening the neighbor nodes whether packet properly forward to its neighbor. If intruder present in the network they compromise the nearest node in the network performs the malicious action through this node. The compromised node forward and received the packet in some delay. In the Swarm intelligence technique calculates the timestamp value transmission between the various nodes, based on the timestamp value delay should be identified. After implementing the swarm intelligence technique the performance ratio is increased slightly.

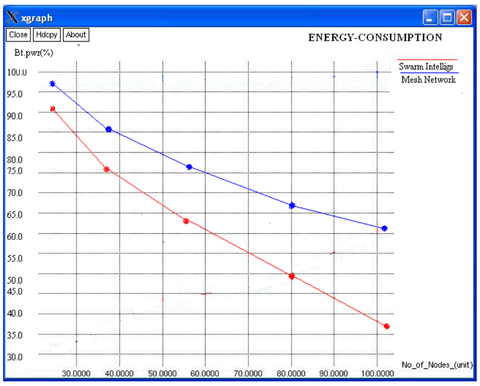

Figure 6: Node vs. Energy Consumption

In this x graph the performance evaluated based on the Energy Consumption ratio. Here the X axis Consider as the no of nodes and Y axis consider as the Battery consumption in percentage.

Each node energy capacity should reduce after the packet transaction performed. Using the Mesh network topology in network the node energy
Consumption ratio should be increased lightly, which should be represented in blue line.

VI. CONCLUSION

In this paper, a swarm based detection and defense technique is proposed for packet replication attacks in mobile ad hoc networks (MANET). The watchdog module was implementing for maintaining a buffer of recently sent packets as well as comparing every overhead packet with the packet in the buffer to see if there is equal. After the watchdog module detects the malicious node or fake node. The Pathrater module then deletes the corresponding route from the route cache and tries to determine if there is another route available to the destination by looking in its cache table. If new route is not available, Pathrater will broadcast a Route Request to obtain a new route to the destination.

Using the swarm intelligence the battery consumption or energy of the node becomes low. In mesh network each device communicates its routing information to every device connects itself. Based on this information each node can pass the data to valid nearest node not for the all node. Due to this methodology battery consumption power of the each node can be saved. By simulation results, it results, it is shown that our technique detects the packet replication attack, avoids the packet replication and also reduces the battery consumption during the transmission.

REFERENCES

1. Bonabeau, E., Dorigo. M., Theraulaz, G: Swarm Intelligence: FroNatural to Artificial Systems, Oxford University Press, New York (1999)
2. G.Indirani, and Dr.K.Selvakumar,"Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks" International Journal of Computer Applications (075-8887) Volume50-No.19,July 2012.
3. K. Ramanarayana and LillyKutty Jacob."Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet". Third International workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Pages 19-24, 2007.
4. L. Buttyan, J.P, Hubaux. "Stimulating Cooperation in Self organizing Mobile Ad Hoc Networks", ACM Journal for Mobile Network(MONET),special issue on Mobile Ad Hoc Networks,2003,pp 57-592.
5. Lippmann R, Haaines JW, Fried JD, Korba J, Das K. The 1999 DARPA off-line intrusion detection evaluation Computer Networks intrusion detection and prevention systems (IDPS).Technical report. NIST: National Institute of Standards and Technology.U.S Department of Commerce: 2007.
6. L. Zhou and Z.J. Haas. "Securing Ad Hoc Networks", IEEE Network Magazine, Volume .13, no.6, Pages 24-30, December 1999.
7. Rajagopalan, S., Shen, C,-C.: ANSI: A Swarm Intelligence-based Unicast Routing Protocol for Hybrid Ad hoc Networks. Journal of Systems Architecture, Special Issue on Nature Inspired Applied Syatems, 485-504(2006).
8. Wang J,Hong X,Ren R,Li T.A real-time intrusion detection system based on PSO-SVM.In: Proceedings' of the International workshop on Information Security and Application 2009 (IWISA 2009).p.319-321
9. Wang Q, Megalooikomnu V. A clustering algorithm for intrusion detection. In: Proceeding of the SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005.p31-38.
10. Wedde H.F., Farooq, M: A Comprehensive Review of Nature Inspired Routing Algorithms for Fixed Telecommunication Networks. Journal of Systems Architecture. Special Issue on Nature Inspired Applied Systems, 461-484(2006).
11. Williamson M. biologically inspired approach to computer security. Technical Report. Bristol: HP Laboratories; 2002.
12. Wilson EO. Sociobiology: the new synthesis. Belknap Press; 1975.Wu Sx, Banzhaf W. The use of Computational intelligence in intrusion detection systems: are views. Applied Soft Computing 2010 ;(1):1-35.
13. Xiao L, Shoa Z, Liu G.K-means algorithm based on particle swarm intelligence algorithm for anomaly intrusion detection In: Proceedings of the Sixth World Congress on Intelligent Control and Automation 2006 (WCICA2006).p584-5858.
14. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile adhoc networks: challenges and solution. IEEE Wireless Communication 2004; 11(1):38-47.
15. Yang S, Wang M, Licheng J. A quantum particle swarm optimization. In: Proceeding of the congress on Evolutionary Computation 2004(CEC2004).p.320-324.
16. Zhou Lianying and Liu Fengyu a Swam intelligence based intrusion detection technique. IJCSNS International Journal of Computer Science and Network Security 2006; 6(7):146-50.
17. Znial A, Maarof MA, Shamsuddin SM. Feature selection using rough dpso in anomaly intrusion detection, In: Proceedings of the Conference on Computational Science and its Application (ICCSA)2007.p.512-524.