Enhanced Intrusion Detection System for Mobile Ad-hoc Networks using Mobile Agents with no Manager

Taran Singh Bharati
Assistant Professor
Department of Computer Science
Jamia Millia Islamia
New Delhi, India

ABSTRACT
Now days everything is communicated via network because everybody is running a short of time. There are so many types of networks but in wireless network when data moves from one place to another, then it becomes susceptible to vulnerabilities. So there is need of secure transmission among the attackers. Here every layer activates the agents, it finally makes the positive rate. It is the decision agents, it finally makes the positive rate.

Keywords:
Mobile adhoc netwok, intrusion detection system, agent, consensus.

1. INTRODUCTION
Mobile adhoc networks are formed by mobile devices like laptop, cell phones and other electronic gadgets. They don’t use the fixed infrastructures. They are used specially when it is very much difficult to setup the network with fixed infrastructure like. Natural calamity, catastrophic situation, floods etc. Since these networks have no other support, hence they themselves communicate by their hand held devices. Here every communication is made in wireless open environment and everything is decided by making a consensus by passing through the messages. Intrusion detection system is a system they keeps an eye on every activity that is performed on the system. It checks whether there has been an intrusion into the system. Once there is an intrusion into the system this can collect our valuable information and can send it to its master. That latter can harm our organization. There are two types of security attacks. One is passive attack in which attacker is interested know about you messages only it is not able to modify our messages. A second type of attack is active and it is more dangerous because attacker is able to modify our messages also.

Basically there are two types of intrusion detection system:

Host based intrusion detections:
They are installed in the local host and they monitor the all local activities of the local system and ensure for any intrusion into the system. They apply many logics to identify the suspicious behaviour of the attacker i.e. anomaly, statistical techniques, threshold etc. Once they make sure that an intrusion has been made, they raise an alarm and all other nodes into the network. They have low false positive rate but they are not much effective.

Network based intrusion detection system:
They are installed in the routers or gateways where from all traffic passes. They inspect every message and check for the intrusion by applying its algorithms to detect intrusion into the system. These are effective but have more false positive rate. These intrusion detection systems for MANET can be implemented via mobile agents

2. RELATED WORK
Kun Xiao et al described a peer-to-peer intrusion detection system [1] based on two types of agents; voting agent used for voting on the decision and result agents that convey the decision or result about the intrusion attack into the system. It depicts that every node has three components. coordinator, controller, monitor, and executor. Coordinator coordinates the total process. Monitors monitor the local activities and if they found any undesirable activity, like file operations, privilege access they report to the controller of the node. Executor executes the work which comes from the controller. [2] Proposed that instead of installing agents on every host this will be installed at the head of the cluster so that memory and accessing time can be saved. Here each local node possesses the local data gathering, local detection, local response system, network joint detection, and network response. Here data is collected locally and monitored for intrusion at the local detection system and then local response policies are determined to inform inside the cluster. Joint intrusion detection is done when alone cluster head is not able to detect the intrusion. Barika et. al. [3] describes the advantages of Agents in intrusion detection system i.e. Autonomy, Mobility, Rationality Reactivity Inferential capability pro-activeness and social ability. This paper describes the sniffer agents that will sniff the network node to gather the information and if need arises then it leave host or duplicate itself. Total pre-treatment work is too large so it divides the work and at last it combines all works to give it to the next phase that is Analyser agents. This analyser here analyses the input for any intrusion by matching the already stored patterns. It declares an intrusion whenever there is an match. The last agent is the decision agents, it finally makes the decision and make all aware of its decision. Bernardes, Mauro Cesar, and Edson dos Santos Moreira [4] describes that all work intrusion detection will be done with the help of different agents. They described the modular approach for intrusion detection. They describe Reactive agents; Notifying agents, Decision making agents, and surveillance agents. Surveillance agents collects the information by patrolling the network and will send it to the decision making agents they analyse the data for the intrusion. This information is passed to the above layer that is Notification agents. On the basis of this information received from the previous layer this new information about the intrusion is sent to above layer that is reactive agents. This layer is made for taking a corrective or counter measure on the attack. Here every layer activates the agents to the layer of agents that above to them. In [5] watermarking and finger printing is used to check infringement in the activities of the attacker. A distributed cooperative intrusion detection with the help of mobile agents
is described in [6] by Dalila Boughaci et al. [7] describes the intrusion detection by using the tables for malicious activities and accordingly it acknowledges among the nodes into the network. [8] uses the autonomous agents for intrusion detection (AAFID). Detection system has, transceivers and monitors.

3. PROPOSED WORK

In our proposed model of intrusion detection in mobile adhoc networks, a network is made by a collection of mobile nodes of devices which can move over the time like laptops, cell phones, pagers etc. Here all nodes interact and cooperate each other by exchanging messages, for any consensus about the occurrence of intrusion into the network. Since this kind of mobile network has no special fixed infrastructure so there are so many problems which are faced in making of consensus about an intrusion. Here we assume there is set of agents which are installed at many places like local host and at coordinator. They collect information at their disposal, communicate among themselves and to the coordinator by secure message passing only. Our method uses the following main steps to decide if there is an intrusion attack into the mobile adhoc network.

![Network node](image)

**Figure 1: Nodes in network connected together in a single hop**

1. At a time only one node’s agent can initiate the process of intrusion detection. Before initiating this node checks whether or not any other node has initiated and its work has not accomplished. If no other node’s works is in pending, this current node can initiate the process.

2. It sends a message to all other agents which are connected to it in a single hop.

3. Every agent at node receives the information from all the nodes’ agents which are connected to it in a single hop and some nodes may be faulty also.

4. Here polling or decision algorithm is used to decide whether or not there is an intrusion into our mobile adhoc network. The following tasks are performed:

   - If some nodes are failed or selfish, then we enforce fault tolerance consensus protocol.
   - Fault tolerance method
   - Majority protocol
   - Voting

Total system can be depicted pictorially as follows:

![Proposed model architecture](image)

**Figure 2: Proposed model architecture**

5. This decision is acknowledged to all other nodes’ agents into the system. That can be made by using cryptosystems; Encryption and messages authentication methods i.e. MAC (messages authentication Code), Hash function, Digital Signature algorithm and other authentication protocols.

**Performance:** Our model can be analysed in following manner.

**Distributed Mutual Exclusion algorithm:** There are two types of mutual algorithm for achieving mutual exclusion in distributed environment; token based and non-token based algorithms. Here Raymond’s Tree Based Algorithm is used because it token based algorithm and its performance is better that all other algorithms for the same and its performance is measured by following parameters. Suppose T is the average message delay and E is the average execution time of the CS.

- **Response time:** time duration for which a node has to wait for its critical section execution (CS).
- **Synchronous Delay:** the time between the next node enters the CS and the time last node exits the CS.
- **Messages:** The messages which are needed to reach the mutual exclusion.

- Resp. time (in low load): \( T \log N \) + E
- Synch. Delay: \( T \log (N/2) \)
- Messages (high load): \( \log(N) \)
- Messages (low load): 4
Algorithm for Consensus about the intrusion having some faulty nodes:
Here Dolve et al.’s algorithm is used to tolerate faulty nodes. Which works on the basis of HIGH witnesses and LOW witnesses received from other nodes about the (non)faulty nodes. Assume that there are n nodes into the network and out of them m nodes are faulty.

- Here algorithm reaches on consensus after 2m+3 rounds

Apart from above analysis this proposed method provides the following characteristics:

- Initiator node Failure Tolerance: failure of individual nodes and initiator will not down the system
- Robustness of insertions and deletion of nodes.
- Transparent to location of failure of nodes and location of initiator.

4. CONCLUSIONS

This paper proposed a new and improved intrusion detection system for mobile ad hoc networks. It will be more profound for the failure and fault tolerance due to the failure of its node as well as a failure of initiator itself. Because when one node’s agent or initiator fails, then their works will be taken over by other nodes’ agents or other initiator without letting know other nodes’ agents about the failure into the system. That is why our model is transparent to failure also. In earlier models a separate human manager was needed but here this proposed model won’t require any manager kind of thing. Here system itself is able to perform its all required works.

5. ACKNOWLEDGEMENT

I would like to acknowledge my supervisor Dr. Rajendra Kumar and my family for their constant support and inspiration which they offered me time to time for this work.

6. REFERENCES


