Power-Aware Hybrid Intrusion Detection in Wireless Adhoc Networks using Mobile Agents

Praveen Kumar Madala
PG Scholar, Dept of CSE
Saveetha Engineering College, Chennai,
Tamil Nadu, India,

G. Nagappan
Associate Professor, Dept of CSE
Saveetha Engineering College, Chennai,
Tamil Nadu, India

ABSTRACT
Power-aware hybrid intrusion detection in wireless ad hoc networks using mobile agents (PHIDS) describes design and implementation of an energy conscious anomaly based co operative intrusion detection system for wireless ad hoc networks based on mobile agent technology. This paper addresses the above stated issue by (1) Applying mobile agent technology to minimize network load, conserving bandwidth and to improve reactivity. (2)Minimize energy consumption of network monitoring nodes by using power metric node selection algorithm.(3) It integrates both host based and network based intrusion detection system. IBM's Aglet is used as the base agent architecture to create mobile agents such as monitoring agent, decision-making agent and action agent. Host based intrusion detection system take care of local intrusion detection on each node. Network based intrusion detection system take care of cooperative intrusion detection at network level.

Keywords – Agent based architecture, intrusion detection, and wireless ad-hoc networks.

1. INTRODUCTION
Wireless ad hoc networks are autonomous nodes that communicate with each other in a decentralized manner through multi hop radio network. Wireless nodes form a dynamic network topology and communicate with each other directly without wireless access point. Wireless networks are particularly vulnerable to intrusions, as they operate in open medium, and use cooperative strategies for network communication. Wireless transmissions are subject to eavesdropping and signal jamming. Physical security of each node is important to maintain integral security of the entire network.

Intrusion detection is one of the key techniques behind protecting a network against intruders. An intrusion detection system tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network. An IDS is a defense system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security. IDS may work on a host level and network level to detect intrusions. An intrusion detection system (IDS) is the software and hardware installed to allow intrusion detection. The IDS are described through three fundamental components. Information source: It represents the source of information and events to be analyzed by the IDS to look for eventual intrusion. It can be either the network traffic or the system logs. Analysis method: It defines the method used to analyze the events produced by the information source and to decide whether there is intrusion or not. There are basically two approaches: Misuse detection and Anomaly detection. Response to intrusions: this component indicates whether the IDS takes actions gains intrusions (active IDS) or remains passive, it just report the intrusion (passive IDS).

2. RELATED WORKS
Recently a lot of research activities have been devoted to the issue of securing wireless ad hoc networks, but the research is still at its early stage. Srinivasan presented a power aware hybrid intrusion detection system using hybrid agents for highly mobile ad hoc network. Power level metric is used to determine the duration for which a particular node can support a network-monitoring node [1]. The research efforts generally fall into four categories: secure routing, trust and key management, service availability protection, and intrusion detection. Intrusion detection is suggested as a complementary mechanism when all other intrusion prevention approaches failed and the attackers can successfully access the network [3]. Hongmei and Roger presented an agent based co operative anomaly detection scheme for securing wireless ad hoc networks. It considered energy-efficiency issue by implementing the function of intrusion detection in a cooperative fashion, rather than a fully distributed manner. It made use of unsupervised intrusion detection mode which is efficient in dealing with a large amount of network data and shortage of purely labeled datasets in real ad hoc network environments. It can be applied to any routing protocol, any attack types, and any clustering protocols with appropriate feature selection [3]. Consequently in addition to the normal traditional IDS capabilities, some extra features have to be possessed for IDS to suit wireless ad hoc networks [6]. Due to the structural and behavioral differences between wired and wireless mobile networks, make existing IDS designs are inapplicable to the wireless networks [13].

Albers presented local intrusion detection on each node of the ad hoc network using mobile agents. In order to make local intrusions a global concern, the local intrusion detection System existing on different nodes collaborate. Architecture uses SNMP and Management Information Base of SNMP. It does not consider compromised nodes broadcasting false intrusion related information to the network. Security of the agent platform is not addressed [14].

2.1 IDS architecture for wireless ad hoc network

An anomaly detection architecture that was proposed in [12] is shown in Fig. 1. In this scheme every node in the MANET participates in intrusion detection and response. Every node is responsible for detecting signs of intrusion locally and independently by monitoring activities such as user and system activities and the communication activities within the radio range, but neighboring nodes can collaboratively investigate over a broader range.

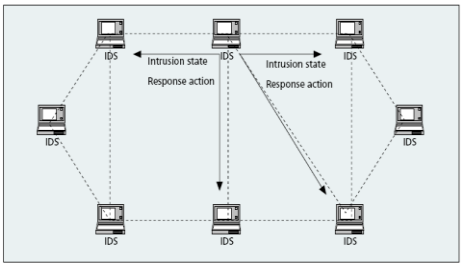

Fig 1: IDS architecture for a wireless ad hoc network.

This activity normally occurs at the following two locations:

1. Host – Host based IDS

2. Network – Network based IDS

Finally, many intrusion detection systems incorporate multiple features into a single system. These systems are known as hybrid systems. These hybrid intrusion detection systems having their architecture based on agents which travel throughout the network, provide a comprehensive solution.

2.1.1 Host based intrusion detection

Host based intrusion detection system take care of local intrusion detection attempts on each node. The host monitoring module includes user level and system level monitoring modules.

2.1.2 Network-based intrusion detection

Network based intrusion detection system detects intrusion attempts at network level. The cluster head has packet monitoring agent, decision making agent and action agent to perform network monitoring of packets within the communication range. The modules of the network based intrusion detection system

2.1.3 Hybrid Intrusion Detection System

This paper describes integrates both host based and network based intrusion detection system to provide a robust system which takes care of entire ad hoc wireless network.

In a proper IDS implementation, it would be Advantageous to fully integrate the network intrusion detection system, such that it would filter alerts and notifications in an identical manner to the host-based Portion of the system, controlled from the same central. In doing so, this provides a convenient means of managing and reacting to misuse using both types of intrusion detection.

2.1.4 Power-aware Design

Power-aware design and evaluation of network protocols requires knowledge of the energy consumption behavior of actual wireless interfaces. Wireless devices must depend on battery power. It is important to minimize their energy consumption and so it becomes essential for each of the active nodes to be aware of the available power. The energy consumption of the network interface can be significant, especially for smaller devices. We believe that energy-aware design and evaluation of network protocols for the ad hoc networking environment requires practical knowledge of the energy consumption behavior of actual wireless devices.

2.2 IDS Architecture

In the fig 2 shows the modular architecture was mainly three types of agents: Action, Decision making and monitoring agents. The IDS we consider is built on a mobile agent framework as in. It is a non-monolithic system and employs several sensor agents that perform certain functions, such as:

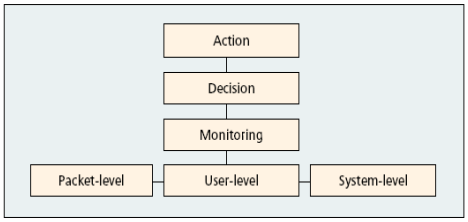

Fig 2: IDS architecture

Host monitoring: Every node on the mobile ad hoc network is monitored internally by a host-monitoring agent. It includes monitoring system-level and user-level activities.

Network monitoring: Only certain nodes have sensor agents for network packet monitoring, in order to preserve total computational power and battery power of nodes.

Decision-making: Every node decides on its intrusion threat level on a host-level basis. Certain nodes collect intrusion information and make collective decisions about network level intrusions using fuzzy logic controller.

Action: Every node has an action agent responsible for resolving intrusion situation on a host and network.

2.3 Agent mobility

This module is used to check agent mobility. As the physical network arrangement changes, cluster membership is dynamically updated. The network monitoring agents are dispatched to new cluster head.

3. IMPLEMENTATION

3.1 Cluster head selection

Cluster head take care of network monitoring. The cluster heads are identified by two techniques based on

1) Connectivity index

2) Power aware node selection algorithm.

The first method considers number of reachable nodes is the basis for cluster head selection. The node with highest connectivity is selected as cluster head. In second method power level of the nodes is considered for cluster head selection in order to minimize energy consumption.

3.1.1 Connectivity index Method

Step1. Hop Selection Step: based on security requirements, a certain number of hops are selected for network monitoring node. Selection of this number greatly affects the network monitoring range.

Step2. Let c_i be the- Number of established connections (reachable nodes from node i at the time of cluster setup), N be the total no of nodes in the entire network, each node sends its c_i value to all its reachable neighbors.

Step3. Upon receiving $c_j$values from its neighbors$j$, where $j \neq i \; \forall \; i = 1..N$, node i sums up the total as s_i (connectivity index) as equation 1, which upon completion is broadcast to all nodes

$$s_i - c_i + \sum_j c_j \qquad (1)$$

Step4. Each node then has to vote to select cluster head. Every node sends a vote packet to the node it selects based on highest connectivity index received as result of a broadcast in step (3). If a node receives a vote from a node with equal s_i value, it doesn't send a vote to the source node. In case of two nodes have equal s_i values and send votes to each other simultaneously, the node with the largest total of s_i values sends a "discard vote" message to the other node. This will ensure that the minimal number of nodes is selected for hosting packet-monitoring agent.

Step5. Each node that received at least one vote is selected as cluster head to perform network monitoring of packets.

3.1.2 Power aware Node Selection

This power aware node selection algorithm considers tree structure, in which monitoring node as the root and the nodes being monitored as its children. The root along with its child nodes contribute to individual clusters. This algorithm uses power level metric to identify candidate nodes which can be selected as cluster head to perform network monitoring. When there is drain in power levels take place at the monitors, any other child node with higher battery power for monitoring can take charge of that cluster.

3.2 Power Loss Availability for Network Monitoring Estimate

The calculation of $PLANE$ (Power Loss/ Availability for Network Monitoring Estimate) involves calculating the duration for which the node can continue to support a network monitoring along with its normal operations as shown in equation 2. $PLANE$ is directly related to the wireless protocol used, mean number of wireless links for a specific node, average node maintenance energy consumption, and the battery power remaining.

$$PLANE = BPR/TEC_{nm} \qquad (2)$$

BPR Is Total Battery Power Remaining at the instant of node selection and TEC_{nm} is Total Energy Consumption with network monitoring node processes running. In this absence of network monitoring we assume $PLANE$ as $PLANE'$ shown in equation3.

$$PLANE' = BPR/TEC \qquad (3)$$

TEC Is Total energy consumption before the node is selected for network monitoring.

3.3 Calculation of PLANE Threshold

Node should have enough battery power to compete to become a network monitoring node. The threshold value is computed by equation 5.

$$\nabla d = {PLANE_{max} - PLANE_{min}}/{2} \qquad (4)$$

$$Threshold = PLANE_{max} - \nabla d \qquad (5)$$

Where ∇d the mean deviation is is value, $PLANE_{max}$ and $PLANE_{min}$ are the highest and the lowest values for the $PLANE$ metric.

An Example

Consider an ad hoc network with 8(A, B, C, D, E, F, G, H) and their values are 4,5,6,7,8,9,10,11 nodes and their $PLANE$ values as shown in Fig 3

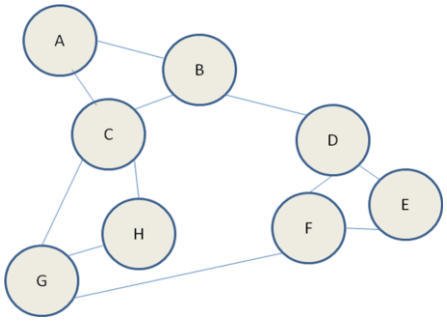

Fig 3: An example network

Node A: 8.2 Node D: 6.3 Node G: 9.0
Node B: 8.5 Node E: 8.1 Node H: 7.1
Node C: 5.4 Nodes F: 7.6

Nodes are represented by circles and are numbered to uniquely identify them in the network. As shown in Fig 3 and 4, the node selection algorithm mentioned above considers the power availability of each node in the network. The nodes in the working set {B, E, and G} are the monitors and they form the cluster heads. The dotted lines represent the monitoring function that they perform using agents. In Figure 4, node B is the monitor, detecting

intrusions over A and C, thus forming a cluster represented by the circle.

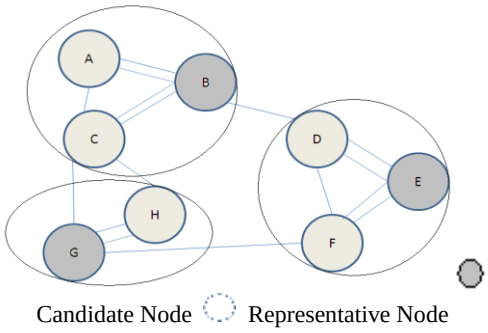

Fig 4: Example 1 with WS = {B, E, G} final selection

Step 8 of the algorithm proves to provide an energy efficient solution whenever one or two clusters actively participate in transmitting, receiving and routing. Variation in power levels take place much more in those nodes than those of any other clusters. It is sufficient enough to change the monitoring node only in those clusters instead of troubling the whole setup. Supposing cluster 1 with root B is constantly participating in routing, the power level will significantly decrease in B, since it has to monitor the packets transmitted across it and its children for intrusions. At one point of time the BPR of node B may drop below that of node A.

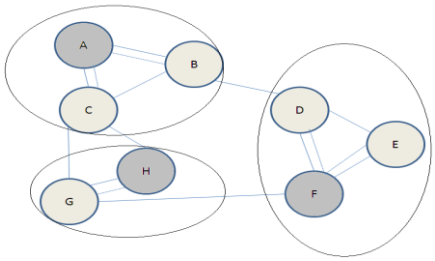

Fig 5: Example 1 with WS = {A, F, H} with cluster 1 re-established

At this point, the re-arrangement within the cluster takes place, with node A becoming the root i.e. the monitor and node B and C become its children. This is explained diagrammatically in Fig5.On constant participation in the network activities, if all the nodes in a particular cluster lose their power below the threshold, then a re-run of the entire node selection algorithm needs to be done. Also, since a new node can enter anytime into the existing network, the node selection algorithm should be re-run to find out the network monitors. As shown in Fig 6, if a new node enters the network it is monitored temporarily by the nearest cluster head.

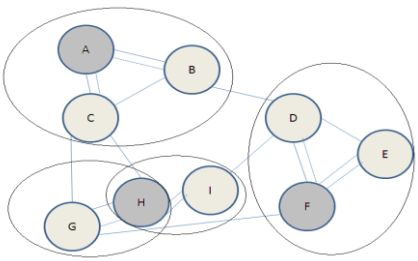

Fig 6: Example 1 with WS = {A, F, H} with new node I

Since the new node may have a higher $PLANE$ value than the existing roots it may replace them on subsequent re-run of the node selection algorithm.

3.3 Power aware node selection algorithm

Step1: Set $PLANE$ threshold: Set a constraint on the $PLANE$ value (threshold value) of nodes which can compete to become a network monitoring node.

Step2: $PLANE$ Calculation and $PLANE$ Ordered List (POL): Arrange the different nodes in the order of increasing values of $PLANE$ which satisfy $PLANE$ constraint.

Step3: Hop Radius: Initially set the hop radius to one and increment hop radius for each insufficient node selection. Selection of this number greatly affects the network monitoring range.

Step4: Expand Working Set of Nodes (WS): Consider node selection incrementally, initially from the first node, (node with highest$PLANE$), to finally the set of all nodes in the network, incrementing the set of nodes under consideration by one node each time. The working set is expanded only if the addition leads to increase in number of represented nodes.

Step5: Voting: Each node has to vote to select cluster head. The nodes considered for cluster head selection are member of the working set.

Step6: Check acceptability of nodes: If all links/nodes are not represented by the set of nodes covered by the voting scheme, then expand the working set and repeat the process from step4. If working set equals the $PLANE$ ordered list, then increment the hop radius and repeat from step3. It is suggested that increment in hop radius effectively increases the amount of processing per monitoring node.

Step7: Cluster Setup: Set individual clusters with the nodes in the working set as roots and the nodes being monitored by them as their child nodes.

Step8: Re-run: Changes in power levels of the root nodes in each cluster will be signaled to their child nodes and the vote count as in step5 takes place within the cluster to elect a new monitoring node.

3.4 Host monitoring

Every node on the mobile ad hoc network has local detection agents, consists of monitoring agent, decision making agent and action agent. Host monitoring agent monitors user level and system level activities for anomaly detection. Monitoring agent looks for suspicious activity on the host node, such as unusual process memory allocations, CPU activity, I/O activity, user operations (invalid login attempt). If an anomaly is detected the decision making agent decides the threat level and commands the action agent to terminate suspicious process or lock out the user.

3.5 Network monitoring

In this network monitoring creates packet monitoring agent to capture and examine individual packets. Packet

monitoring agent resides on the cluster head to monitor packets within the communication range.

Types of Attacks handled

Packet Dropping: Dropping of packets by compromised nodes.

Spoofing attack: Changing the source IP address by attackers.

SYN Flood Attack: Overloading the network by numerous connection requests.

3.6 Decision making

In this decision making phase creates decision making agent to take decision about the anomalous activity identified by packet monitoring agent. It uses rule based fuzzy system to identify the threat level. It confirms the type of intrusion detected and makes a collaborative decision with other hosts.

3.7 Action

In this phase creates an action agent which takes necessary action when an intrusion attempt is detected. It takes the counter measure to inhibit intrusion.

4. PERFORMANCE EVALUATIONS

Packet dropping attack has five threat levels such as low, low-medium, and medium, medium high and high as shown in the table 1.

Table 1 packet dropping levels

Threat Level	Packet Dropping
Low	< = 10%
Low-Medium	>10% <=30%
Medium	>30 % <=50%
Medium-High	>50 % <=70%
High	>70%

Packet dropping levels are shown in graph in figure 7.

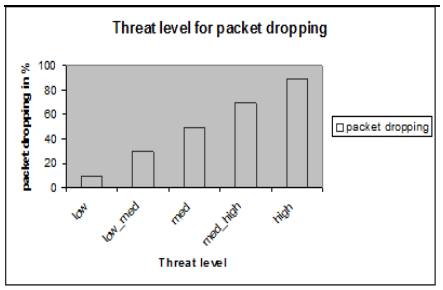

Fig 7: Threat Level for Packet dropping

The packet dropping under normal condition and dropping by intruder own in Fig 8. Under normal condition the packet dropping percentage is usually less than 30%. When the packet dropping rate is greater than 50% the decision making agent alerts the action agent to take counter measure about intrusion attempt. The use of fuzzy logic reduces the rate of false positive rate.

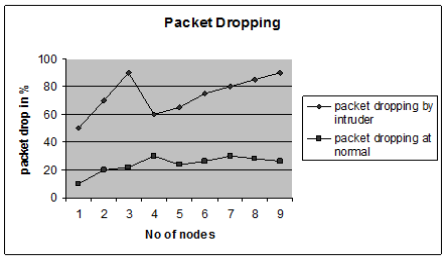

Fig 8: Packet dropping

Power aware node selection algorithm results in improved performance when the number of nodes increases in a particular cluster or among the clusters as shown in Figure 9.

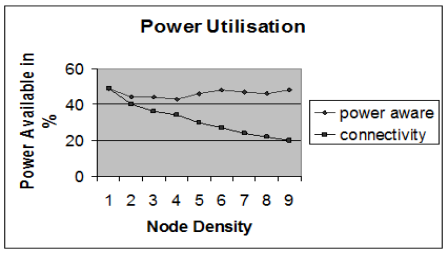

Fig 9: Power Utilization

Node density refers to the number of nodes per unit area. The utilization of power for network monitoring is better in case of power aware node selection algorithm than connectivity index method. The power available for network monitoring in case of connectivity index method shows gradual decrease. When the node density increases the utilization of power for network monitoring is improved by 20 percent. Power aware method determines the duration for which a node can serve as network monitoring node. It considers tree structure, in which network monitoring node as the root and the nodes being monitored as its children. The root along with its child nodes contribute to individual clusters. When there is drain in power levels take place at the cluster head, any other child node with higher battery power for monitoring can take charge of that cluster.

5. CONCLUSION

This paper describes design and implementation of an energy conscious anomaly based co operative intrusion detection system for wireless ad hoc networks using mobile agent technology. The developed system has two subsystems, host based and network based intrusion detection system. IBM's Aglet is used as the base agent architecture to create mobile agents for intrusion detection task. Three major agent categories used are namely monitoring agent, decision making agent and action agent.

Host based intrusion detection system take care of local intrusion detection on each node. The host monitoring agent monitors user level and system level activities for anomaly detection. Network based intrusion detection system takes care of co operative intrusion detection at network level. The cluster heads are identified by two techniques based on i) connectivity index ii) power aware selection algorithm. The first method considers number of reachable nodes is the basis for cluster head selection. The node with highest connectivity is selected as cluster head. In second method power level of the nodes is considered for cluster head selection in order to minimize energy consumption. Power aware node selection

algorithm results in improved performance when the number of nodes increases in a particular cluster or among the clusters. The utilization of power for network monitoring is better in case of power aware method.

6. FUTURE WORK

In present work the mobile agents are used to detect attacks on the network level. The mobile agent itself is the target of the attackers. In future, security for the mobile agent can be considered. The agent can be further improved by including learning algorithms to detect and prevent multiple attacks.

7. REFERENCES

[1] T.Srinivasan, V. Mahadevan, A. Meyyappan, A.Manikandan, M.Nivedita, N.Pavithra, "Hybrid Agents for Power Aware Intrusion Detection in Highly Mobile Ad-hoc networks", International Conference on Systems and Network Communication (ICSNC'06) October 2006.

[2] Zeng-Quan Wang, Hui-Qiang Wang, Qian Zhao, Rui-Jie Zhang , " Research on Intrusion Detection System", Proceedings of the 5th International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[3] Hongmei Deng, Roger Xu, Jason Li, Frank Zhang, Renato Levy, Wenke Lee, "Agent - based Cooperative Anomaly Detection for wireless Ad Hoc Networks", Proceedings of the 12th International Conference on Parallel and Distributed Systems (ICPADS'06). 12-15 July 2006, Volume: 1, pp. 613620.

[4] Dalia Boughaci, Habiba drias, Ahmed Bendib, Youcef Bouznit and Belaid Benhamou, "A Distributed Intrusion Detection Framework based on Autonomous and Mobile Agents", Proceedings of the International Conference on Dependability of Computer Systems (DEPCOS RELCOMEX'06) pp 248-255 May 2006.

[5] T. Srinivasan, Vivek Vijaykumar, R. Chandrasekhar, "An auction based task allocation scheme for power–aware intrusion detection in wireless ad- hoc networks", International Conference on Wireless and optimal communication networks, 11-13 April 2006.

[6] Abdulrahman Hijazi, Nidal Nasser, "Using mobile agents for intrusion detection in wireless ad hoc networks", Wireless and Optical Communications Networks WOCN 2005, Second IFIP International Conference on 6-8 March 2005, pp 362-366.

[7] Abdelhamid Belmekki, Abdellatif Mezrioui, "Using active agent for intrusion detection and management" Proceedings of the 2005 International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'05).

[8] Islam M. Hegazy, Hassam M. Faheem, Taha Al-Arif, Tawfik Ahmed, "Evaluating how well agent-based IDS perform", IEEE Potentials, May2005.

[9] Noria Foukia, "IDReAM: Intrusion detection and response executed with agent mobility architecture and implementation", AAMAS'05, July 25-29, 2005, Utrecht, Netherlands. ACM.

[10] Mishra, A. Nadkarni, K., Patcha, A., "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications Volume: 11, Issue: 1, 2004, pp 48-60.

[11] Yan Xia, Ren-Fa li, Ken- Li Li, " Intrusion detection using mobile agent in ad hoc networks", Proceedings of the Third International Conference on Machine Learning and Cybernetics, Shanghai, 26-29 August 2004.

[12] Y.Zhang, W.Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM *J. Wireless Net.* vol. 9, no. 5, Sept. 2003, pp. 545–56.

[13] O.Kachirski, R. Guha, "Intrusion detection using mobile agents in wireless ad hoc networks", Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN'02), July 10-12, 2002, pp.153-58.

[14] P.Albers "Security in Ad hoc Networks: a General Intrusion Detection Architecture Enhancing Trust based Approaches", First International Workshop on Wireless Information System, Spain Apr 3-6 2002.