Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks

Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris
Department of Informatics, University of Piraeus,
80 Karaoli and Dimitriou Str. Piraeus 18534, Greece
{mitrokat, rosa, cdoulig}@unipi.gr

Abstract – *The evolution of wireless network technologies and the recent advances in mobile computing hardware have made possible the introduction of various applications in mobile ad hoc networks. Not only is the infrastructure of these networks inherently vulnerable but they have increased requirements regarding their security as well. As intrusion prevention mechanisms, such as encryption and authentication, are not sufficient regarding security, we need a second line of defense, Intrusion Detection. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, we briefly describe intrusion detection systems and then we suggest a distributed schema applicable to mobile ad hoc networks. This anomaly detection mechanism is based on a neural network and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance of the proposed architecture is evaluated under different traffic conditions and mobility patterns.*

Keywords – *Emergent Self Organizing maps, Denial of Service, Intrusion Detection, Wireless Ad Hoc Networks, Neural Networks*

I. INTRODUCTION

Mobile ad hoc networks have received great attention in recent years, mainly due to the evolution of wireless networking and mobile computing hardware that made possible the introduction of various applications. Mobile nodes communicate using wireless interfaces without a fixed network infrastructure. In these environments each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbors in order to forward their messages to the appropriate destination. Applications of mobile ad hoc networks have increased requirements in order to ensure high quality of service for the provided services. Security in such infrastructure-less networks has been proven to be a challenging task.

Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks where an aggressor in order to launch an attack has to gain access to a wired infrastructure, firewalls and gateways, in ad hoc networks there is no clear line of defense. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination.

The insecure open medium combined with poor physical protection presents another disadvantage. Each node is able to roam independently running the risk to be easily compromised by a malicious attacker. Furthermore, when more sophisticated attacks take place nodes can be easily exploited. In addition, wireless ad hoc networks lack a centralized monitoring and management point. Indeed, most of the network algorithms rely on the cooperative participation of all nodes, which is usually exploited by malicious attackers in order to launch attacks and degrade the performance of the network.

In order to achieve network security apart from prevention techniques ([1], [2]) the use of reactive mechanisms, as a second wall of defense, is a necessity. A network is as secure as its weakest link so we need to deploy a defense-in depth. Intrusion detection plays a substantial role in order to maintain a highly survivable network. Intrusion detection presents the significant advantage to prevent or decrease the loss of an attack in an early stage. For example, in the early stage of a Denial of Service (DoS) we can mitigate and reduce the impact of the attack and respond accordingly. Intrusion detection techniques can be divided in misuse detection and anomaly detection.

Misuse detection uses a priori knowledge on intrusions and tries to detect attacks based on specific patterns or signatures of known attacks. Although misuse detection systems are very accurate in revealing known attacks, their basic disadvantage is that attacking mechanisms are under a continuous evolution, which leads to the need for an up-to-date knowledge base. Anomaly detection has the advantage of being able to discover unknown attacks while it adopts the approach of knowing what is normal. As a result it attempts to track deviations from the normal behavior that are considered to be anomalies or possible

intrusions. There is only a small body of research in the area of mobile ad hoc networks as to which "known" attacks or attack signatures can be used in misuse detection. That is why anomaly detection is more suitable in order to perform intrusion sensing in mobile ad hoc networks.

The majority of the proposed intrusion detection techniques are deployed in the network layer. In this paper, we focus on intrusion detection techniques in ad hoc networks applied on the MAC layer that present the advantage of revealing the origin of the attack. In particular, we describe a network-based intrusion detection method in order to detect selective packet dropping attacks in wireless networks using a set of features from the MAC layer. The proposed detection approach is based on a class of neural networks known as emergent Self-Organizing Maps (eSOMs). Combining machine learning and information visualization techniques we are able to have a clearer view of how secure our network is against attacks. Anomaly detection techniques in wireless ad hoc networks include mechanisms to gather "normal" and abnormal" audit data and clarify behaviors as normal and abnormal.

Following this introduction, the paper is organized as follows. Section 2 presents related work of intrusion detection approaches that have been proposed for mobile ad hoc networks. Section 3 discusses the proposed intrusion detection approach and the classification algorithm used. In section 4 the performance evaluation of the approach is presented, including the simulated attack, the statistical features used and finally the results of the proposed approach. Section 5 concludes the paper and discusses some future work.

II. RELATED WORK

Intrusion detection techniques deployed for wired networks cannot be easily applied in wireless ad hoc networks due to the differences between these two types of networks. Compared to wired networks where traffic monitoring is performed in gateways, routers and switches, wireless ad hoc network lack traffic management points. As a result, intrusion detection in wireless networks should be based on local audit data. Moreover, because of the resource constraints that wireless networks present, one should focus on security mechanisms keeping in mind their resource consumption characteristics. This means that it is better to use a periodic intrusion detection system (IDS) than an 'always-on' prevention mechanism.

The resource constraints that ad hoc networks face include limited battery, bandwidth and frequent miscommunication. These constraints complicate the discrimination between a new qualified operation after a disconnection and an intrusion. Another serious constraint that wireless ad hoc networks present is the difficulty of classification between normal and anomaly behavior. For example a node that sends out false routing information is not necessarily compromised but may have been out of sync, due to mobility.

Zhang and Lee [3] propose the first (high-level) distributed and cooperative anomaly based IDS, which provides an efficient guide for the design of IDS in wireless ad hoc networks. They discussed an intrusion detection approach is anomaly detection in routing updates, on the MAC layer and in the application layer.

Huang and Lee [4] extended their previous work by proposing a cluster based IDS, in order to combat the resource constraints that mobile ad hoc networks face. They used a set of statistical features that can be derived from routing tables and apply the classification decision tree induction algorithm C 4.5 in order to detect normal vs abnormal behavior. The proposed system is able to identify the source of the attack, if the identified attack occurs within one hop.

Deng et al. [5] proposed a hierarchically distributed and a completely distributed intrusion detection approach. The detection approach used in both architectures is based on the Support Vector Machines (SVM) classification algorithm. They use a set of parameters derived from the network layer. They suggest that a hierarchically distributed approach may be a more promising solution versus a completely distributed intrusion detection approach.

Kachirski and Guha [6] proposed a cluster-based Intrusion detection system using mobile agent technologies. The proposed system uses mobile agents each performing a particular role. The results of each node are aggregated in cluster points in order to limit the packet monitoring task in a few nodes and minimize the IDS-related processing time by each node.

Liu et al. [7] proposed a completely distributed anomaly detection approach on the MAC layer. The proposed approach selects features from the MAC layer to profile normal behavior of mobile nodes and then apply cross-feature analysis [8] on feature vectors constructed from the training data.

Tseng et al. [9] propose a specification based intrusion detection approach in order to detect attacks in the AODV routing protocol. The correct AODV routing behavior is specified using finite state machines and the actual behavior of AODV flows is compared with these specifications. The disadvantage of specification based techniques is the need of balancing the tradeoff between complexity and accuracy.

Anjum et al. [10] propose a signature based intrusion detection approach for wireless ad hoc networks based on the assumption that attack signatures are completely known in an ad hoc network. Moreover, this approach investigates the ability of various routing protocols to facilitate the intrusion detection procedure. The authors conclude that

the choice of the routing protocol depends on the type of detection we want to perform. The latter one may be a main factor that one should consider in the case of misuse detection.

In this paper, we propose a completely distributed intrusion detection approach that is better suited for the vulnerable characteristics of wireless ad hoc networks. The intrusion detection approach is performed using neural networks. Neural networks have the great advantage of tolerance towards imprecise data. We exploit this important feature of neural networks and introduce an intrusion detection approach based on Emergent Self-Organizing Maps.

III. PROPOSED INTRUSION DETECTION MODEL

A. Intrusion Detection Architecture

Malicious nodes in a wireless mobile ad hoc network may target to exploit features of the physical, network or MAC layers. The majority of the security mechanisms in such networks have been focused in the network layer. Little research has been done on the MAC layer security. The role of MAC layer in wireless ad hoc networks is substantial as it is responsible for maintaining the communication between nodes and the scheduling of the access in a shared radio channel.

MAC layer is directly affected by almost every anomaly, since it is placed in the first layers of the protocol stack. Indeed, the data delivery ratio or throughput may be affected by malicious behavior or misuse of the shared medium (e.g., selfishness) due to increased routing load. The control overhead for each delivered data packet may also increase. Thus, intrusion detection mechanisms that are based on features selected in the MAC layer are faster regarding detection delays and response time. Furthermore, these features make the discrimination between normal and abnormal behavior easier.

In this paper, we propose an intrusion detection approach for the packet dropping attack based on features selected from the MAC layer. Moreover, we propose a response technique to detect the malicious node. The architecture of the suggested IDS could be either distributed and cooperative or distributed and hierarchical. The distributed and hierarchical IDS, are based on dividing the mobile ad hoc network in clusters. Although cluster-based IDSs have the advantage of lower detection workload, the procedure of creating clusters and electing cluster heads may cause a great overhead. Moreover, the existence of cluster heads and the obvious possibility of their exploitation by malicious attackers lead to the weakness of fictitious security. Furthermore the distributed hierarchical IDSs are more efficient for ad hoc networks with low mobility. Thus, the cooperative and dynamic nature of mobile ad hoc networks implies that the intrusion detection system should be distributed and cooperative. The lack of central monitoring nodes and the lack of trust between peer nodes of a wireless ad hoc network render a central intrusion detection system impractical. Each node of the wireless ad hoc network should perform its local intrusion detection using local audit data. When the confirmation of other nodes to detect an attack is necessary, the local intrusion detector should cooperate. Furthermore, this cooperation between local intrusion detectors should be held through secure channels.

The proposed intrusion detection system is composed of multiple local IDSs agents. Each IDS agent (Fig. 1) is responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the mobile wireless ad hoc network. Each local IDS agent is composed of the following components:

Data Collector: is responsible for selecting local audit data and activity logs

Detection Engine: is responsible for detecting local anomalies using local audit data. The local anomaly detection is performed using the eSOM classification algorithm.

The procedure that is followed in the local detection engine is the one described below:

- Select labeled audit data and perform the appropriate transformations.
- Compute the classifier using training data and the eSOM algorithm.
- Apply the classifier to test local audit data in order to classify it as Normal or Abnormal.

Response Engine: If an intrusion is detected by the Detection Engine then the Response Engine is activated. The Response Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion. Special attention should be paid on the function of the Response Engine in order to avoid possible flooding caused by the notification messages of intrusion. Thus, the broadcasted notification of intrusion is restricted to a few hops away from the node where the anomaly has been detected since the neighboring nodes run the greatest risk of possible intrusion.

When the Response Engine is activated, the node fires a fake RTS (Ready to Send) message destined to the suspicious node. If the suspicious node replies to that packet then the node is classified as malicious. Otherwise, the node fires an AODV_ERROR message as the suspicious node is indicated as moved. After the discovery of the adversary the local IDS agent fires an ALERT message notifying its one hop neighbors. Alternatively, the local IDS agent could send ALERT messages to all potentially traffic generators that exist in its routing table,

thus achieving a global response to all nodes that are directly influenced by the malicious node.

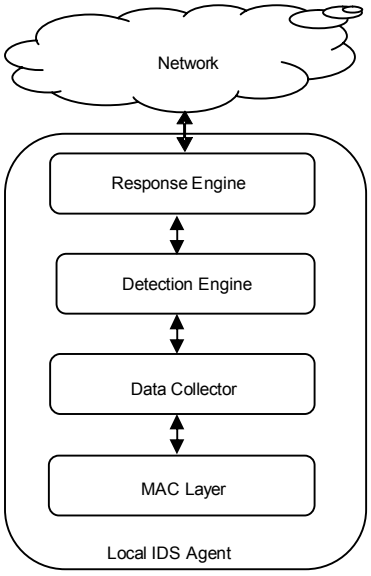

Fig 1. Intrusion Detection Architecture

B. *Emergent Self Organizing Maps*

Kohonen's Self-Organizing maps (KSOMs) [11] have their base in biology. They belong in the category of unsupervised or competitive learning networks and produce a topological map, which illustrates the input data according to their similarity. The Self Organizing Map is trained using only the characteristics of the trained data. KSOMs are competitive, because there is only one winning neuron in the output layer. That is why the Self Organizing Map is also referred as a winner-take-all unsupervised learning neural network. The trained KSOMs create clusters of data, where similar vectors of features are located in a specific region in the output space. This is very useful for discovering clusters and relationships in data. The generated mapping is topology preserving.

The learning procedure is composed of the following steps:

a. Initialize the random weights w_{ij} (also known as codebook vectors of the neurons) with small random values.
b. Use an input pattern x
c. Calculate the Euclidean distance (eq. 1 [11]) between input data sample x, and each neuron weight w_{ij}. The winner (Best Matching Unit) is chosen as o(x):

$$o(x) = \arg\min_j \left\| x - w_{ij} \right\|, \text{ j=1,2,...} l \quad (1)$$

d. Adjust all the weights in the neighborhood, in order to achieve the topological mapping, depending on their distance from the winning neuron according to the following equation [11]:

$$\forall j : w_{ij}(t) = w_{ij}(t-1) + a(t)\eta(t') \cdot \left(x_i(t) - w_{ij}(t-1)\right) \quad (2)$$

where α is the learning rate, η the neighborhood function and t' the time that was spent in the current context. The neighborhood function η decreases as t' increases.

e. Repeat steps b, c, d until convergence.

Something that is often neglected in KSOM is that self organization allows the emergence of structure in the data. According to [12] "Emergence is the ability of a system to produce a phenomenon on a new, higher level". In order to achieve emergence the existence and cooperation of a great number of elementary processes is necessary. Emergence may be presented not only in natural but also in technical systems. One of the basic disadvantages of SOM maps is that their abilities are limited to a few neurons.

On the other hand, Emergent Self-Organizing Maps (eSOMs) may expand to some thousands neurons. More specifically, the number of neurons in some cases may be greater than the number of input data. As a result only a small number of input data may correspond to each neuron. A large number of neurons in eSOM is necessary in order to achieve emergence. The cooperation of such a big number of neurons leads to structures of a higher level. The clustering procedure in emergent SOMs is performed by observing the whole Emergent Self-Organizing Map and not by focusing on its neurons.

We have used the distance based (U-Matrix) method in order to visualize the structures generated by eSOMs. According to this method [12] the sum (height) of distances between the neuron-weights and its neighbours is normalized by the largest height. The result of the sum of distances is represented as the elevation of each neuron. Thus the input data set is displayed and depicted at a 3D landscape. The height will have a large value in areas of the map where few datapoints belong and small in areas that represent clusters. Thus, hills and valleys will be created correspondingly. The height ($uh(n_i)$) of each neuron (n_i) is given by the following equation (eq.3) [13]:

$$uh(n_i) = \sum_{n_j \in U_i} d(n_i, n_j) \quad (3),$$

where U_i represent the neighbor neurons of n_i.

We trained Emergent SOMs with logs of network traffic and used eSOM U-matrices [13] in order to perform intrusion detection. In our case, each log of network traffic is represented by a vector with some fixed attributes. Each vector has a unique spatial position in the U-Matrix and the distance between two points is the dissimilarity of two network traffic logs. The U-Matrix of the trained dataset is divided into valleys that represent clusters of normal or

attack data and hills that represent borders between clusters. Depending on the position of the best match of an input data point that characterizes a connection this point may belong to a valley (cluster (normal or attack behaviour)) or this data point may not be classified if its best match belongs to a hill (boundary). The map that will be created after the training of the Emergent SOM, will represent the network traffic. Thus an input data point may be classified depending on the position of its best match.

IV. PERFORMANCE EVALUATION

A. Simulation Environment

To evaluate the feasibility of our approach we have conducted a series of experiments. For our experiments we have made some assumptions. First of all, we assume that the mobile network employs 802.11 in the MAC layer, with a 4-way RTS/CTS/DATA/ACK handshake exchange. No other secure fairness access mechanism is used. The network has no preexisting infrastructure and the ad hoc routing protocol that was employed is AODV.

We implemented the simulator within the ns-2 library. Our simulation modeled a network of 50 hosts placed randomly within a $1800 \times 1000m^2$ area. Each node has a radio propagation range of 250 meters and the channel capacity is 2 Mb/s. The nodes in the simulation move according to the 'random way point' model. At the start of the simulation, each node waits for a pause time, then randomly selects and moves towards a destination with a speed uniformly lying between zero and the maximum speed. On reaching this destination it pauses again and repeats the above procedure till the end of the simulation. The minimum and maximum speed is set to 0 and 10 m/s, respectively, and pause times at 0, 20, 50, 70 and 200 sec. A pause time of 0 sec corresponds to the continuous motion of the node and a pause time of 200 sec corresponds to the time that the node is stationary.

We evaluated the performance of the suggested intrusion detection scheme for 5, 10, 15 and 20 malicious nodes. In each case the number of all nodes in the network is set to 50. The malicious behavior is carried between 50 and 200 sec. The nodes perform normally between 0 and 50 sec. These parameters result in a network with rather high mobility and high traffic activity.

Twenty, on average, traffic generators are developed to simulate TCP data rate to ten destination nodes. This traffic pattern results in twenty connections among source and destination nodes. The sending packets have random sizes and exponential interarrival times. The sources and the destinations are randomly selected with uniform probabilities. The mean size of the data payload was 512 bytes. Each run is executed for 200 sec of simulation time with a feature sampling interval of one sec. We used the IEEE 802.11 Distributed Coordination Function (DCF) as the medium access control protocol. The mobility of the nodes is random determined by scenario files that are generated by the scene generator of ns-2. A free space propagation model with a threshold cutoff was used in our experiments. In the radio model, we assumed the ability of a radio to lock onto a sufficiently strong signal in the presence of interfering signals, i.e., radio capture.

B. Simulated Attacks

Attacks in mobile ad hoc networks follow the same discrimination, as in WLAN and wired networks, namely passive attacks and active attacks. Passive attacks are based on eavesdropping of the network traffic and attempt to gain and/or utilize information without modifying it or altering the system resources. This type of attacks is very difficult to detect by nature. On the other hand, active attacks attempt to modify information and/or system resources and manipulate their functionality.

One example of active attacks is the *packet dropping attack*. In a packet dropping attack a misbehaving node simply destroys or discards data or routing packets without taking responsibility. The packet dropping attack is also known as an *ignorance attack* and has the following variations regarding frequency and selectiveness. *Random or constant dropping* concerns the period of time that the malicious node drops the packets. In *selective dropping,* packets are dropped according to some specific criteria. Selective dropping is also known as a *gray hole attack*.

In our experiments we have simulated a constant selective dropping attack where the attacker simply discards all data packets while it functions legitimately concerning routing and MAC layer packets. This type of attack is extremely difficult to detect if we consider that packet dropping is due to a malicious behavior or mobility. To add to the problem the malicious node may exhibit malicious behavior when it is most advantageous to him and not from the beginning of the traffic

C. Features

The feature vectors that would be used in the eSOM classification is a critical step in building the proposed intrusion detection approach. The features of network traffic should be in a form suitable for easy processing by eSOM and representative of network activity in order to increase the contrast between normal and abnormal activity and have a high information gain so that we may be able state if an event is normal or abnormal without ambiguity.

The statistical features we have used have been introduced by Liu et al. [7] in their proposed approach for

performing intrusion detection in the MAC layer. These features are as follows:

Network allocation vector (NAV): it is a node specific characteristic which depicts the time that the node will occupy the medium for sending its messages.

Transmission traffic rate: indicates the rate of the transmitted packets.

Reception traffic rate: indicates the rate of the received packets.

Retransmission rates of RTS packets: indicates the rate of the ReadyToSend packets that are retransmitted by the monitoring node. A high value of this feature suggests a possible packet dropping attack.

Retransmission rates of DATA packets: indicates the rate of the data packets that are retransmitted by the monitoring node. A high value of this feature suggests a possible packet dropping attack.

Active neighbor node count: represents the number of neighbor nodes that have data transmission activities.

Forwarding node count: represents the number of neighbor nodes that communicate directly with the monitoring node.

In order to avoid having a great influence of the attributes of some input vectors it is necessary to normalize the input data. Many methods are used for the data normalization. We have normalized the data with mean zero and variance one, a technique that produces very good results in most cases as reported in the literature. For the evaluation we have used the Databionics ESOM tool ([14], [15]). We have to note here for the three features – protocol type, service type and status flag- whose values are alphanumeric in order to perform our experiments we map each instance of an alphanumeric value to sequential integer values.

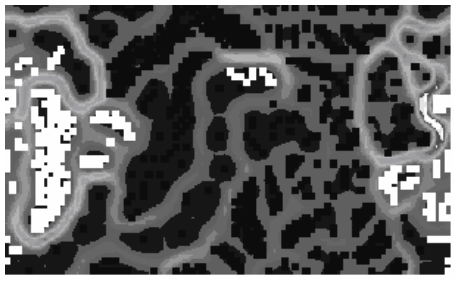

Fig 2. Emergent SOM U-Matrix of Trained Dataset

D. Simulation Results

The presented evaluation proves that we can achieve a differentiation between normal and abnormal behaviors concerning packet dropping attacks. In order to perform clustering with eSOM U-Matrices we followed the proceeding procedure. The best matches of the trained dataset and thus the corresponding dataset were manually grouped into clusters representing normal and attack behavior. Thus, we identify the regions of the map that represent a cluster that can be used for the classification on new datasets. The eSOM of a trained dataset is depicted in figure 2. As it can be clearly seen the training data set has been divided in two classes that are very well distinguished, normal data class (dark color) and packet dropping data class (light color). In order to make sure that our approach will always provide efficient and accurate results we should update our trained eSOM U-matrix according to the new conditions concerning mobility.

In order to evaluate the efficiency of the proposed approach we use two measures: the Detection rate and the False alarm rate:

Detection rate $= \frac{TP}{TP + FN}$, False alarm rate$= \frac{FP}{TN + FP}$,

where TP is the number of true positives (attack logs classified as attacks), TN the number of true negatives (normal logs classified as normal), FP the number of false positives (normal logs classified as attacks) and FN the number of false negatives (attack logs classified as normal). The most effective approach should reduce as much as possible the *False alarm rate* and at the same time increase the *Detection rate.*

Figure 3 presents the average Detection rate of the all source nodes that present traffic activity and are recognized as normal or attack by eSOM regarding the used pause times. The detection rate seems not to be influenced by the mobility and in all cases to be over 80%. For long pause times the rate slightly lessens which is due to the TCP traffic and the degradation of the mobility. Indeed, a TCP agent stops sending data packets when it doesn't receive acknowledgment. Even after AODV discovers a new path to that destination, the agent keeps sending data packets through the malicious node, as the latter respond normally to control packets. As the network exhibits a rather low mobility, traffic always is rejected by the malicious node

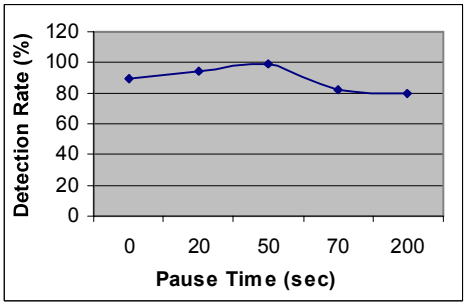

Fig 3. Detection Rate vs. Pause Time

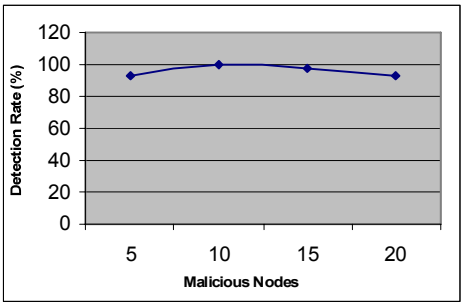

Fig 4. Detection Rate vs. Number of Malicious Nodes

and soon stopped by the TCP agent, which degrades the audit data fed to eSOM.

The detection rate as a function of the number of malicious nodes is presented in figure 4. The rate is rather high and, as in the previous figures, always over 80%. When few malicious nodes exist in the network the connections that are influenced by them are also a few, since source nodes move randomly in the network. This results in duplicated lines in the audit data set which is fed to eSOM, thus the decrease in the detection rate. When the number of malicious nodes is high compared to the number of source nodes, the TCP connections generated automatically by NS are a few, which leads to multiple duplicate lines in the audit data that is fed to eSOM, which explains the decrease in the detection rate. TCP traffic is used as a more realistic one. Another data traffic type (e.g CBR) is under future investigation.

Table 1 and Table 2 present the average false alarm rate as a function of the paused times used and the number of malicious nodes, respectively. When a source node generates traffic to different destinations and one of these connections is influenced by malicious nodes, then eSOM finds it difficult to distinguish among normal and abnormal traffic. If this is combined with multiple duplicate lines in the audit data due to mobility, the malicious node number produces rather high False alarm rates. The high values of false alarm rates are combated by the activation of the Response Engine which is able to indicate if the alarm has been triggered by a malicious node or because of mobility issues.

Table 1. False Alarms vs. Pause Time

Pause time (sec)	False Alarm (%)
0	21
20	20
50	22
70	20

Table 2. False Alarms vs. Number of Mobile Nodes

Malicious nodes	False Alarm (%)
5	26
10	22
15	17
20	21

VI. CONCLUSIONS AND FUTURE WORK

The area of ad hoc networking has received increased attention among researchers in recent years, as the evolution of wireless networking and mobile computing hardware have made possible the service of various applications by this type of networks. Security in such environments is a critical issue. Intrusion detection can compliment intrusion prevention. In this paper, we have proposed a completely distributed IDS for mobile ad hoc networks using eSOM. By exploiting the visualization of network traffic our approach detects selective packet dropping attack by classifying malicious and normal behavior. The proposed approach uses the MAC layer feature set as audit data. This audit data are used as input a type of neural networks known as Emergent SOM in order to perform intrusion detection. We examined how eSOM performs in classifying normal and abnormal behavior in mobile ad hoc networks and we exploited the advantage of visualizing network traffic that is achieved through eSOM. The proposed intrusion detection approach is also able to identify the source of the packet dropping attack. We should note that during the classification procedure used in intrusion detection, the classes of the trained data have to be defined manually through the observation of the map something that may introduce a process error.

Special attention should be paid to the fact that the proposed intrusion detection system could be employed for various routing protocols. Regarding possible extension of this work, we plan to examine the performance of other types of neural networks and select features from other layers (e.g. network layer) in order to detect packet dropping and other type of attacks.

ACKNOWLEDGEMENT

Special thanks to the Databionic research team for the valuable advice and comments concerning the use of the Databionic ESOM tool.

This work has been partially supported by the Greek Research and Technology Secretariat under a PENED grant.

REFERENCES

[1] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks", in Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor networks, pp. 17-22, October 2004.

[2] M. G. Zapata, and N. Asokan, "Securing Ad-Hoc Routing Protocols,", in Proceedings of the 2002 ACM Workshop on Wireless Security, pp. 1-10, September 2002.

[3] Y. Zhang, W. Lee, Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks Vol. 9, pp 545-556, 2003.

[4] Y. Huang, and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks",in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 135-147, October 2003.

[5] H. Deng, Q. Zng, and D. P. Agrawal, "SVM-based Intrusion Detection System for Wireless Ad Hoc Networks", In Proceedings of the IEE Vehicular Technology Conference (VTC'03), Vol.3, pp 2147-2151, October 2003.

[6] O. Kachirski, and R. Guha, "Intrusion Detection Using Mobile agents in wireless Ad hoc Networks", in Proceedings of the IEEE workshop on Knowledge Media Networking, pp.153-158, July 2002.

[7] Y. Liu, Y. Li, H. Man, "MAC Layer Anomaly Detection in Ad Hoc Networks", In Proceedings of 6th IEEE Information Assurance Woskshop, June 17, 2005.

[8] Y. Huang, W. Fan, W. Lee, P.Yu, "Cross-Feature analysis for Detecting Ad-Hoc Routing Anomalies", In Proceedings of the 23rd International Conference on Distributed Computing Systems, pp.478, 2003.

[9] Tseng, P. Balasubramanyan, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based Intrusion Detection system for AODV", In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp.125-134, October 2003.

[10] Farooq Anjum, Dhanant Subhadrabandhu, Saswati Sarkar. "Signature-based Intrusion Detection for Wireless Ad-Hoce Networks." In Proceedings of Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, Oct. 2003.

[11] S. Haykin, "Neural Networks: A comprehensive Foundation", Prentice-Hall, New Jersey, USA, 2nd edition, 1999.

[12] A. Ultsch, "Data Mining and Knowledge Discovery with Emergent SOFMs for Multivariate Time Series", In Kohonen Maps, (1999), pp. 33-46.

[13] A. Ultsch, "Maps for visualization of high-dimensional Data Spaces", Proc. WSOM, Kyushu, Japan, (2003), pp. 225-230.

[14] A. Ultsch, F. Moerchen "ESOM-Maps: tools for clustering, visualization, and classification with Emergent SOM", Tech. Report Dept. of Mathematics and Computer Science, University of Marburg, Germany, (46), (2005).

[15] Databionic ESOM Tools, Available from <http://databionic-esom.sourceforge.net/devel.html>