DETECTION OF DISTRIBUTED ATTACKS IN MOBILE AD-HOC NETWORKS USING SELF-ORGANIZING TEMPORAL NEURAL NETWORKS

James Cannady
Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, FL, U.S.A.

Keywords: MANET, Intrusion detection, Self-organizing map, Learning vector quantization.

Abstract: Mobile ad hoc networks continue to be a difficult environment for effective intrusion detection. In an effort to achieve reliable distributed attack detection in a resource-efficient manner a self-organizing neural network-based intrusion detection system was developed. The approach, Distributed Self-organizing Intrusion Response (DISIR), enables real-time detection in a decentralized manner that demonstrates a distributed analysis functionality which facilitates the detection of complex attacks against MANETs. The results of the evaluation of the approach and a discussion of additional areas of research is presented.

1 INTRODUCTION

Because of the increasing dependence which companies and government agencies have on their computer networks the importance of protecting these systems from attack is critical. A single intrusion of a computer network can result in the loss, unauthorized utilization, or modification of large amounts of data and cause users to question the reliability of all of the information on the network. There are numerous methods of responding to a network intrusion, but they all require the accurate and timely identification of the attack. The individual creativity of attackers, the wide range of computer hardware and operating systems, and the ever-changing nature of the overall threat to targeted systems have contributed to the difficulty in effectively identifying intrusions. Intrusion detection has been an active area of research for the last twenty years. However, advances in information technology, especially in the use of wireless systems, and the increasing variety of vulnerable software applications have made the accurate and timely detection of network-based attacks a critical, but elusive goal.

This paper describes a research effort that focused on the development of an effective intrusion detection capability for Mobile Ad Hoc Networks (MANET). MANETs are peer-to-peer wireless networks that rely upon the presence of other network nodes in a limited geographical proximity to communicate in an ad hoc manner. Unlike other wireless network architectures a MANET does not rely upon static wireless access points or dedicated servers. Instead, individual components establish dynamic connections with other MANET nodes based on proximity at each point in time. The inherent flexibility of MANETs has led to their application in a wide range of applications, including military and emergency response situations. The potential for use as part of a critical information infrastructure, and the distributed nature of the connections, has increasingly made MANETs the target of focused complex distributed attacks.

1.1 Complexity of MANET Intrusion Detection

While the process of effective intrusion detection continues to be difficult, as noted in Sterne (2005), there are several inherent characteristics of MANETs that further complicate the accurate detection of attacks:

- Lack of a Centralized Control – Since the nodes in a MANET are distributed independent entities reliant on localized connectivity there is no single node that is designed to act as a hub or controller for other components in the MANET.

Cannady J. (2010).
DETECTION OF DISTRIBUTED ATTACKS IN MOBILE AD-HOC NETWORKS USING SELF-ORGANIZING TEMPORAL NEURAL NETWORKS.
In *Proceedings of the 2nd International Conference on Agents and Artificial Intelligence - Artificial Intelligence*, pages 229-234
DOI: 10.5220/0002712802290234

- Limited Resources – There is typically far less network bandwidth available in MANETs than can be provided in traditional wired networks and wireless local area networks.
- Dynamic Connectivity - As a peer-to-peer network that consists of a variable number of nodes that may be highly mobile an effective intrusion detection approach cannot rely on the presence of any particular node at any particular point in time.

1.2 Mobile Intrusion Detection Requirements

To overcome the inherent challenges posed by the detection of attacks in MANETs, an effective approach must possess several characteristics (Sterne):

- **Enable the detection of a wide variety of potential attacks**. Particular attention should be provided for distributed attacks that are conducted across the network.
- **Minimize consumption of network resources**. Limitations in network bandwidth and processing power of individual nodes must be conserved for the primary function of the MANET. Security functions, including intrusion detection, must operate within the limited resources that remain after the primary functions of the network have been satisfied.
- **Provide autonomous detection**. The approach must not rely upon any external analysis engine or controller. The variability in the connectivity of individual nodes would eliminate reliable data exchange with any external monitor or centralized controllers/monitors.
- **Utilize data from a variety of sources**. Some types of attacks, particularly distributed attacks, may only be detected through the use of data from multiple sensors. As a result, the approach should have the ability to leverage data from throughout the MANET.

1.3 Prior Research

With the increasing application of MANETs in a variety of applications the need for effective intrusion detection is in these network is growing. Numerous research efforts have been conducted to address the requirements for effective MANET intrusion detection. However, there are a limited number of seminal research efforts that have formed the basis for most of the current research in the field.

Zhang, et al (Zhang, 2004) developed a model in which each node is responsible for independently conducting localized intrusion detection and with sharing data with neighboring nodes to provide collaborative detective on a broader level. The intrusion detection agents on the nodes communicate via a secure communication channel with cooperative detection engines. The resulting multi-layered integrated intrusion detection system demonstrated a scalable approach that provided both local and global detection.

Sterne, et al, (Sterne, 2005), proposed a comprehensive architecture designed to address the unique requirements of a MANET-based detection approach. In their proposed model detection occurs through the use of a hierarchy in the MANET formed by nodes that serve as clusterheads. These nodes coordinate the identification of potential attacks between nodes at lower levels in the hierarchy. The paper describes how the approach could be used to detect specific forms of MANET attacks.

A significant weakness among most current approaches is the reliance on dedicated messages that are disseminated throughout the network on a continuous basis. While the data communicated between the nodes provides valuable information for intrusion detection, it also utilizes the limited bandwidth available in a MANET. Further, the reliance on dedicated detection nodes results in a potential vulnerability to the entire process if those nodes are dropped from the network topology.

2 APPROACH

The Distributed Self-organizing Intrusion Response (DISIR) system attempts to overcome these inherent limitations by leveraging the power and flexibility of a modified Learning Vector Quantization (LVQ) neural network. LVQ neural networks combine self-organizing maps (SOM) with a supervised competitive layer that provides pattern recognition capabilities.

2.1 Neural Processing

The LVQ is a combination of a SOM for classification and a competitive multilayer neural network that uses the output of a SOM as input for to the competitive layer pattern recognition. The LVQ architecture (Figure 1) contains one hidden

layer with Kohonen neurons, adjustable weights between input and hidden layer and a winner takes it all mechanism. This layer is a traditional SOM neural network. The output from the SOM is then provided to the linear layer, which is the supervised learning layer of the architecture. LVQ algorithms have been employed in the past for applications ranging from speech recognition (Mäntysalo, 1992), to radar image classification (Chang, 1994). They are frequently used in supervised learning applications that require efficient processing. (Linde, 1980).

2.2 Modified LVQ Algorithm

While the use of a standard LVQ was shown to be capable of detecting man-in-the-middle attacks in (Cannady, 2009) that approach was unable to identify more complex attacks that evolve over time. A single snapshot of activity does not contain the data necessary to evaluate trends and cumulative effects that would provide evidence of more complex attacks. To address this deficiency a method was required that captured the dynamic nature of network traffic over time. A temporal approach would enable the system to identify patterns that only emerge over time. The temporal method chosen for inclusion in DISIR was the recursive SOM. (Voegtlin, 2002)

The original SOM mandates that each unit *i* of the map compare its weight vector M_i to the input vector X(t) at time *t*. However, in the recursive SOM each unit *i* has associated with it two weight vectors w^x_i and w^y_i. In the recursive SOM, the best matching unit c is the node with the highest activity. The learning rules used for the unit weights are described as follows:

$$w^x_i(t+1) = w^x_i(t) + \gamma\, H_{ic}\, [x(t) - w^x_i(t)]$$

$$w^y_i(t+1) = w^y_i(t) + \delta\, H_{ic}\, [y(t-1) - w^y_i(t)]$$

where γ and δ are the learning rates, and H_{ic} is a Gaussian neighborhood function of the distance between each node *i* and the winner node c. The recursive SOM algorithm is essentially the original SOM applied to both weight vectors. However, the inclusion of the additional weight vector allows the algorithm to consider past activity when evaluating current data.

In DISIR the recursive SOM has replaced the traditional SOM portion of the overall LVQ algorithm. As shown in Figure 1, each recursive SOM provides feedback, in the form of an additional weight vector, to the subsequent map. This additional weight vector represents the last SOM (time *t*). By continually updating each new SOM with the data in the previous SOM the maps develop a cumulative view of activity being processed by the SOMs over time. This cumulative view further allows the enables to the LVQ to identify changes in activity over time in the form of dynamic patterns.

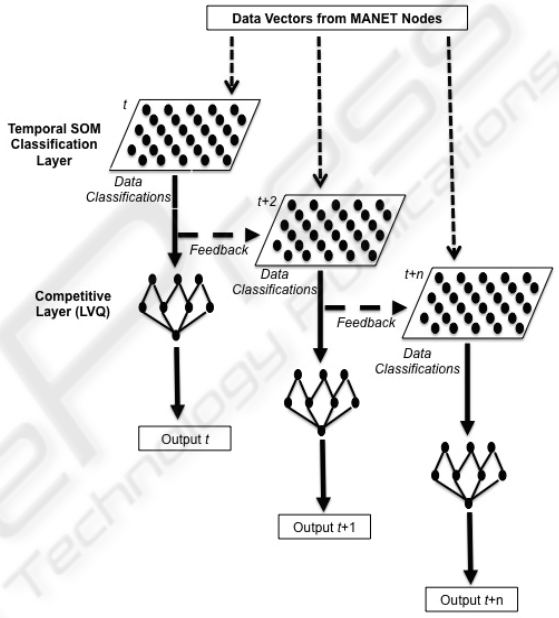

Figure 1: Recursive SOM-based LVQ Approach.

To manage the sum of vectors that would eventually occur as data is accumulated at each new time period, the modified LVQ architecture also includes the use of leaky weight integrators. Leaky integrators function by gradually degrading connection weights over time. If no new data is provided to increase the sum of a particular weight value the weight will eventually decrease to zero. Leaky integrators were originally included in a modified SOM algorithm in (Choe, 1997) and the approach is commonly used in other neural network algorithms that attempt to emulate the neural structure of biological systems. The inclusion of leaky integrators in this application enables the approach to more accurately track patterns of activity that are distributed over time.

2.3 Distributed Architecture

In DISIR the LVQ is used to classify network activity using a first-stage recursive SOM and then identify patterns of activity representing attacks in the MANET using the LVQs competitive layer. While the LVQ, like many other host-based intrusion detection approaches, can effectively identify attacks targeting an individual MANET node, the purpose of this research was to develop an intrusion detection approach capable of detecting distributed attacks that require data from multiple nodes for accurate analysis.

To effectively identify activity in multiple locations within the MANET each node is placed in promiscuous node. This allows a node to monitor activity on all other nodes within range. Each node maintains a SOM that processes the activity of the nodes contained within a spatial area of the node as defined by the range of the node in promiscuous mode. Each of these "area maps" allows each node to monitor local activity within its range and classify the activity vector into a class representing network events on the two-dimensional SOM map. The output from the area map held by each node is then fed to the competitive layer of the LVQ which is also on each node (Figure 2). If a pattern matching a known attack is identified by the competitive layer the node disseminates an alert throughout the MANET. If a node identifies activity which is suspicious, but short of the threshold necessary to initiate an alert, it can disseminate the suspicious results to other nodes in the network by utilizing modified HELLO messages that are regularly broadcast by nodes in the MANET. HELLO messages are used in the AODV protocol to enable nodes to monitor the presence and proximity of nodes in their neighborhood. By extending the HELLO message format to accept an additional 512 bytes (essentially doubling the size of the HELLO message) the characteristics of a 64x64 SOM grid could be disseminated through the MANET. This extension could be modified based on processing requirements and network bandwidth limitations.

When the LVQ indicates that an attack is probable but the threshold of a "confirmed" attack has not been achieved, the frequency of the dissemination of HELLO messages is increased. This facilitates the exchange of additional information when the probability of an attack is high. The HELLO_INTERVAL parameter of the AODV protocol is directly associated with the attack probability so that the time period between messages between nodes was reduced to facilitate additional data exchange between the nodes. The frequency change is local, not global, and disseminates the reduced HELLO_INTERVAL through the network as the HELLO messages are passed between nodes. As other nodes eventually also increase their recognition of intrusive activity they would similarly reduce the period between HELLO messages that they initiate. As the threat level, based on the current attack probability decreases, the frequency of HELLO messages similarly decreases. As a result, the overhead imposed by the additional HELLO messages throughout the MANET is limited to periods of heightened network threats.

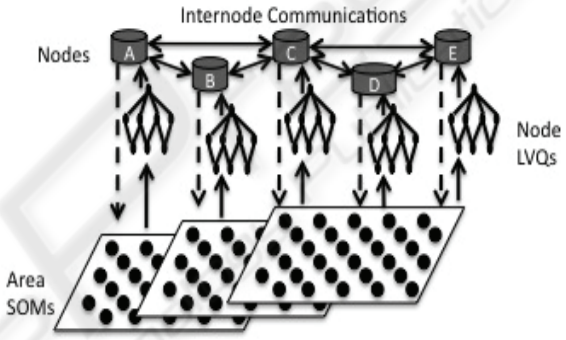

Figure 2: DISIR Structure.

By distributing the analysis of network activity and the detection of network attacks among all the nodes in the MANET the need for a centralized processing node, or a limited number of processing nodes in a hierarchy, is eliminated. The detection process is evenly spread throughout the entre MANET. This avoids the potential loss of a critical detection component as a result of a physical loss of the node or dynamic connectivity unrelated to a network attack. Further, the lack of a centralized detection manager greatly reduces the amount of intrusion detection-related data that must be disseminated throughout the MANET to support a centralized analytical engine.

3 RESULTS

To evaluate the effectiveness of the approach a DISIR simulation using Matlab/Simulink™ and ns-2 was developed. A MANET consisting of 36 nodes was created with each node operating in promiscuous mode.

The DISIR prototype was evaluated against three scenarios that are realistic representatives of distributed attacks that occur in MANETs representative of the most common forms of threats in the network.

3.1 Packet Dropping

Packet dropping is the process of discarding packets that are being transmitted across the network. A malicious node may specifically select the packets that are dropped or the node may discard all packets that are received. The attack not only results in the loss of data destined for an intended recipient but the practice also has negative impacts on the entire network. Network delays can occur as applications wait for data that is never received, and the retransmission of packets can further consume limited network bandwidth.

The detection of packet dropping in DISIR involved the identification of patterns of lost packets in the network. As data was identified as missing by individual nodes the constituents in the current route were noted. As additional instances of packet loss were recorded the consistent presence of a particular node in the route would increase the probability that the node was in fact discarding the missing packets. The more packets that were discarded the higher the probability that the responsible node could be identified.

As shown in Figure 3 the probability that DISIR was able to identify a packet dropping attack increased quickly as the number of missing packets increased. The detection probability leveled off at approximately 65 packets in the evaluation. This indicated that DISIR could correctly identify packet dropping reliably with a few as 65 packets lost and any additional lost packets contributed little to the analysis.

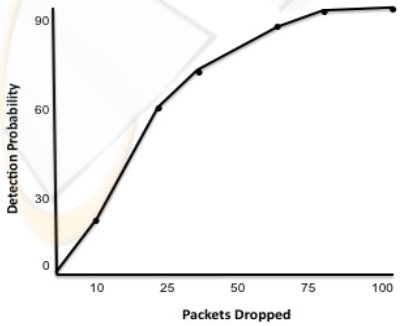

Figure 3: Results of packet dropping detection evaluation.

3.2 Port Scans

A port scan attack is primarily a reconnaissance techniques designed to allow attackers to discover host and network services that are vulnerable. A port scan typically involves interrogating ports sequentially by sending a message to each port and determining its status. Because of the nature of the port scan it was selected for the evaluation to validate the ability of DISIR to identify a more distributed attack.

The detection of port scans was based on the identification of patterns of scanning across the network. While the process would be trivial if a global view of network activity was available, the distributed nature of DISIR requires an effective data sharing process to provide a broader view of the activity across the network. As a result, DISIR was designed to increase the frequency of the HELLO messages, which provided detection data, when a port scan was detected on the network. The increasing frequency of the HELLO messages allowed data from distant portions of the MANET to more quickly share relevant data.

As shown in Figure 4, the detection time varied directly based on distance (number of drops) and the frequency of the HELLO messages. However, even in the worst-case scenario of 35 hops travelled and 30 seconds between HELLO messages the MANET-wide port scan was detected in approximately 60 seconds.

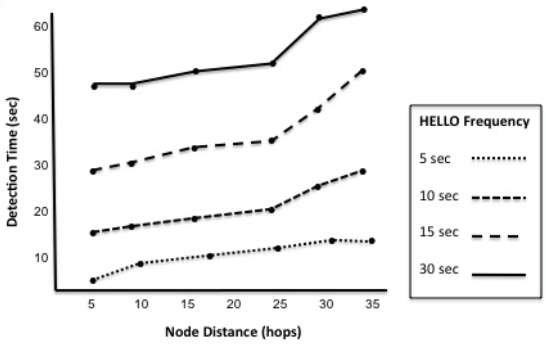

Figure 4: Results of port scan detection evaluation.

4 CONCLUSIONS

The scenarios used to evaluate the DISIR prototype have determined that the approach is extremely effective in meeting the stated requirements of a mobile intrusion detection system:

- DISIR facilitates the detection of a wide variety of potential attacks. While the evaluation scenarios were limited to common distributed attacks the results of the evaluation process indicates a significant potential for DISIR to accurately identify other forms of distributed attacks.
- Because of the overlapping nature of the "area SOMs" used in DISIR all of the network traffic on the MANET is capable of being monitored. Nearby nodes are observed through promiscuous monitoring and more distant nodes are included in area evaluations as their localized analysis results are disseminated throughout the MANET. The overlapping nature of the detection process also enables a layered defense structure.
- By utilizing a de-centralized approach that disseminates attack data only during periods of increased threat DISIR is able to efficiently detect attacks while minimizing resource consumption. The de-centralized approach also facilitates autonomous detection since there is no reliance on any external analysis engine or controller.
- Since the attack recognition capability of DISIR is distributed throughout all of the nodes on the MANET the approach is capable of providing continuous detection capabilities in the event of the loss of individual nodes. As a result, DISIR can maintain the same per capita level of intrusion recognition regardless of network scale.

REFERENCES

Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C.., Balupari, R., Tseng, C.-Y., Bowen, T. (2005). "A general cooperative intrusion detection architecture for MANETs" *Proceedings of the 3rD International Workshop on Information Assurance*.

Mäntysalo, J., Torkkola, K., and Kohonen, T. (1992). "LVQ-based speech recognition with high-dimensional context vectors". In *Proceedings of the International Conference on Spoken Language Processing*, Edmonton, Alberta, Canada.

Chang, K., and Lu, Y. (1994). "Feedback learning: a hybrid SOFM/LVQ approach for radar target classification". In *Proceedings of the International Symposium on Artificial Neural Networks*.

Linde, Y. (1980, January). "An Algorithm For Vector Quantier Design", *IEEE Transactions on Communications*, vol. 28, No. 1.

Cannady, J. (2009). "Distributed Detection of Attacks in Mobile Ad Hoc Networks Using Learning Vector Quantization". *Proceedings of the 1st International Workshop on Wireless and Mobile Networks Security*.

Voegtlin, T. (2002). "Recursive self-organizing maps". *Neural Networks*, 15(8-9).

Choe, Y. and Miikkulainen, R. (1997). "Self- organization and segmentation with laterally connected spiking neurons". In *Proceedings of the International Joint Conference on Artificial Intelligence* (IJCAI-97).

Zhang, Y., Lee, W., and Huang, Y. (2003). "Intrusion detection techniques for mobile networks". *Wireless Networks*, Volume 9, Issue 5.