DYNAMIC NEURAL NETWORKS IN THE DETECTION OF DISTRIBUTED ATTACKS IN MOBILE AD-HOC NETWORKS

James Cannady

Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, FL, USA
cannady@nova.edu

ABSTRACT

This paper describes the latest results of a research program that is designed to enhance the security of wireless mobile ad hoc networks (MANET) by developing a distributed intrusion detection capability. The current approach uses learning vector quantization neural networks that have the ability to identify patterns of network attacks in a distributed manner. This capability enables this approach to demonstrate a distributed analysis functionality that 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.

KEYWORDS

Mobile ad-hoc networks, intrusion detection, neural networks

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 an ongoing research program that is focusing on the development of an effective intrusion detection capability for MANETs. 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 reply upon static wireless access points or dedicated servers. Instead, individual components rely upon the establishment of 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. At present, the ability to accurately detect and respond to these attacks relies upon computationally expensive cryptography [1], or centralized intrusion

detection controllers [2]. There are three inherent complexities in MANETs that make intrusion detection an especially complicated process and make it difficult to transfer existing wired intrusion detection approaches to the MANET environment:

1. 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 of controller for other components in the MANET. As a result there is similarly no possibility for a centralized detection monitor that can coordinate the inputs from host-based intrusion detections on each node. Current network-based intrusion detection systems require the placement of controlling systems on dedicated servers in strategic locations [2]. While this reduces the vulnerability inherent in the use of a single centralized controller the limited number of detection hubs are still vulnerable to loss. As a result, a distributed reasoning capability is required to support the identification of attacks in MANETs.

2. Limited Bandwidth Availability – There is typically far less network bandwidth available in MANETs than can be provided in traditional wired networks and wireless local area networks. As a result, the information passed between the distributed nodes must be prioritized for transmission. Since the primary function of any MANET is some task other than intrusion detection (e.g., distributing the results of low-power sensors, etc.), the priority assigned to detection-related messages will necessarily be low. Because of the limited available bandwidth MANETs are also ill suited to the use of mobile software agents. In this approach individual agents are dispatched throughout the network to collect and disseminate detection-relevant data and alerts. Unfortunately, the security of these mobile agents is extremely difficult to achieve without significant degradation of the limited bandwidth available in MANETs.

3. Dynamic Connectivity - As a peer-to-peer network that consists of a large 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. Nodes may pass beyond the proximity of any other node and be dropped off the network. They may later "appear" at a different point in the network at a later time as a result of their renewed proximity to other MANET components. This is a further complication for any centralized detection approach.

4. Use of end-to-end cryptography – Some networks and application utilize end-to-end cryptography to protect transmitted data. However, this causes the payload information in the packets to be unavailable for traditional network intrusion detection approaches.

1.1 Mobile Intrusion Detection Requirements

To overcome the inherent challenges posed by the detection of attacks in MANETs, an effective approach must possess several characteristics ([2]):

- **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.
- **Enable layered defense**. Multiple overlapping views of network activity reduce the potential for the compromise of the network through the penetration of a single node.
- **Provide adaptive defense**. This characteristic includes both the ability to provide intrusion detection capabilities in the event of failure, and the ability to identify new forms of attack against the network. The former requires considerations for system survivability and the latter is based on dynamic algorithms.

1.2 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.

In [2] a comprehensive architecture was 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.

Zhang, et al ([3]) 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.

Vigna, et al, ([4]), developed AODVSTAT, an intrusion detection tool for mobile environments that was based on earlier research in State Transition Analysis. A group of nodes on the MANET contained the AODVSTAT sensors. The sensors were designed to gather information about suspicious events in their neighborhood and share the attack information based on activity within the MANET.

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 approach used in this research attempts to overcome these inherent limitations by leveraging the power of neural networks. Neural networks have been previously applied to intrusion detection [5][6][7]. In this approach the Learning Vector Quantization (LVQ) algorithm is utilized to identify instances of MANET attacks in a distributed manner. The LVQ is a combination of a self-organizing map (SOM) for classification and a competitive multilayer neural network which uses the output of the SOM as input for pattern recognition (Figure 1).

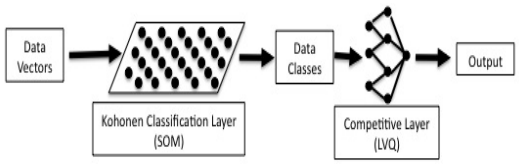

Figure 1: LVQ Architecture

A SOM is a vector quantization method that map patterns from an input space onto a lower dimensional space of the two-dimensional map. The process preserves the topological relationships between the inputs to find the best matching unit b in time step t in the following equation:

$$||x(t) - w_b(t)|| = \min_i \{||x(t) - w_i(t)||\}$$

where $I \in V_M$, $x(t)$ is a input vector, and $w_i(t)$ is a weight vector of the unit i in the map. Subsequently the weight vector of the best matching unit b is updated towards the given input vector $x(t)$ according to:

$$w_b(t+1) = w_b(t) + \gamma(t)h_b(t)(x(t) - w_b(t))$$

where $\gamma(t)$, $0<\gamma(t)\leq 1$, is a learning rate, and $h_b(t)$ is the neighborhood function. SOMs have been successfully employed in a variety of classification tasks, including anomaly detection in wired networks [5][6].

The second part of the LVQ algorithm uses the output of the SOM as input to the competitive layer. The LVQ competitive architecture (Figure 2) contains one hidden layer with Kohonen neurons, adjustable weights between input and hidden layer and a winner takes it all mechanism. LVQ algorithms have been employed in the past for applications ranging from speech recognition [8], to radar image classification [9]. They are frequently used in supervised learning applications that require efficient processing.

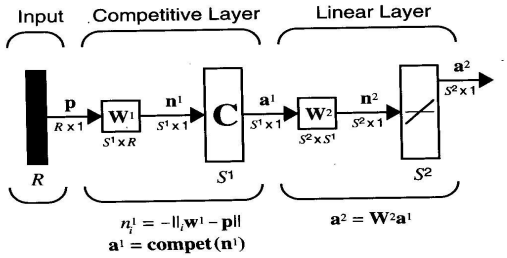

Figure 2: LVQ Competitive Layers

In this approach the LVQ is used to classify network activity using a first-stage SOM and then identify patterns of activity representing attacks in the MANET. 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 represented by a node 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 3). 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 unused space in the regular HELLO messages that are regularly broadcast by nodes in the MANET.

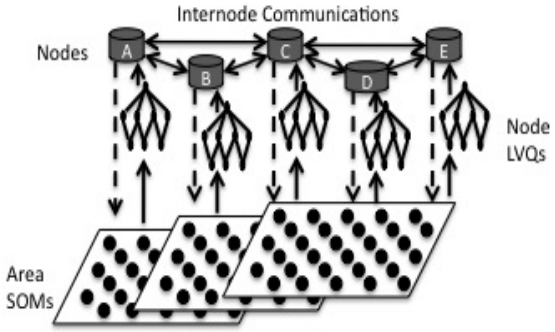

Figure 3: Distributed Detection Architecture

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 about 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 our initial approach a simulation using Matlab/Simulink™ and ns-2 was developed. A MANET of 18 nodes was created using ns-2 with each node in promiscuous mode (Table 1).

Parameter	Value
Topology	1000m x 1000m
Simulation Time	360 seconds
Nodes	18
Malicious Nodes	1-6
Packet Size	512 bytes
Packet Generation Rate	6 packets/sec
Node Movement Model	Random waypoint
Node Movement Speed	10 m/sec
Pause Time	2 seconds
Feature Sampling Interval	3 seconds

Table 1: Simulated MANET Characteristics

The experiment evaluated the ability of the proposed approach to identify instances of Man-in-the-Middle (MIM) attacks in the Ad Hoc On Demand Distance Vector (AODV) routing protocol. AODV is a reactive distance vector protocol in which routes are established on demand. When a node seeks to establish a route to a new destination, it broadcasts a route request (RREQ) through the network. When the first copy of the RREQ reaches its destination, the destination node sends back a route reply packet traversing the path taken by the RREQ in reverse order. This establishes that particular route as the shortest path between the requester and destination. Subsequent RREQs that arrive via longer paths are ignored. Each RREQ contains a sequence number that is propagated from the requester to the destination. However, to distinguish "stale" copies of old RREQs from interfering with newer RREQs, the protocol specifies that RREQs with higher sequence numbers supersede those with older sequence numbers.

When a malicious node attempts to place itself into the route between two nodes it modifies the sequence number of the RREQ it receives to a higher number before forwarding it on to its neighbors. This modification makes it appear that the modified RREQ is the shortest route. This incorrect RREQ will override the legitimate RREQs from other nodes due to the higher sequence number. As a result, the malicious node will be able to insert itself into the route. If this incorrect route is accepted by the other nodes the malicious node will be in a position to monitor, delay, delete, or otherwise interfere with traffic traveling between the two targets of the MIM.

During the tests of the approach 80% of the simulated MIM attacks were detected (Figure 4). Those that fell below the detection threshold did so because the MIM activity being conducted by the malicious node lasted less than 30 seconds (the HELLO messages were set for broadcast every 30 seconds). A shorter period between HELLO messages would lower the detection threshold but also increase the amount of data being broadcast through the MANET. An example of this type of successful attack was the manipulation of a single RREQ for the purpose of intercepting one message. While this activity could be potentially significant,

depending on the content of the intercepted message, it is believed that future refinements will mitigate this residual vulnerability.

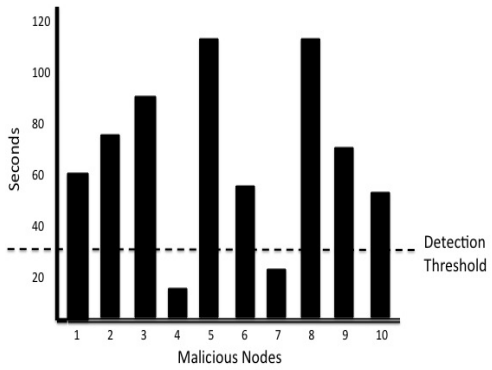

Figure 4: Simulation Results

4. CONCLUSION

A new approach to the detection of attacks in MANETs has been presented. While currently limited to relatively straightforward attacks, such as those against the routing protocols, the approach has demonstrated positive results within the confines of the decentralized, low bandwidth, nature of a MANET.

REFERENCES

[1] Razi, M., Quamar, J. "A hybrid cryptography model for managing security in dynamic topology of MANET" *International Symposium on Biometrics and Security Technologies*, 2008.

[2] Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C.., Balupari, R., Tseng, C.-Y., Bowen, T. , "A general cooperative intrusion detection architecture for MANETs" Proceedings of the 3rD International Workshop on Information Assurance. IEEE, Santa Clara, CA, 2005

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

[4] Vigna, G, Gwalani, S., Srinivasan, K., Belding-Royer, E., and Kemmerer, R. (2004). "An Intrusion Detection Tool for AODV-based Ad Hoc Wireless Networks". In Proceedings of the Annual Computer Security Applications Conference.

[5] Rhodes, B., Mahaffey, J., Cannady, J., "Multiple Self-Organizing Maps for Intrusion Systems" In Proceedings of the 23rd National Information Systems Security Conference. 2000.

[6] Fox, K. L., Henning, R. R., Reed, J. H., and Simonian, R. "A neural network approach towards intrusion detection". In Proceedings of the 13th National Computer Security Conference. 1990.

[7] Cannady, J. "Applying CMAC-based On-line Learning to Intrusion Detection". Proceedings of the 2000 IEEE/INNS Joint International Conference on Neural Networks. 2000.

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

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