Distributed Self-organized Collaboration of Autonomous IDS Sensors

Karel Bartos, Martin Rehak

Distributed Self-organized Collaboration of Autonomous IDS Sensors

Karel Bartos, Martin Rehak

Faculty of Electrical Engineering
Czech Technical University in Prague
Prague, Czech Republic
{karel.bartos,martin.rehak}@agents.fel.cvut.cz

Abstract. We present distributed self-organized model for collaboration of multiple heterogeneous IDS sensors. The adaptation model is based on a game-theoretical approach that optimizes the behavior of each IDS node with respect to other nodes in highly dynamic environment. We performed initial experimental evaluation of the proposed collaboration model on two autonomous IDS detectors deployed on different parts of university network. We show that this Intrusion Detection Network significantly improves the detection effectiveness and brings advanced defensive mechanism against novel highly sophisticated threats.

1 Introduction

Protecting network security assets against modern, highly sophisticated network attacks represents complex challenge for researchers and security experts. Many successfully targeted attacks have shown large vulnerabilities and unpreparedness of corporate network security mechanisms to face novel and more advanced network threats. One of widely used mechanisms for network protection is Intrusion Detection System, which helps to secure network infrastructures by using static signature matching or dynamic anomaly detection methods. Signature-based IDS systems evaluate each network connection according to predefined signatures regardless of context, showing promising results on well-known attacks. However, these systems cannot detect novel intrusions or zero-day attacks. On the other side, anomaly-based IDS systems are designed to detect wide range of network anomalies including yet undiscovered attacks, but at the expense of higher false alarm rates. Thus each IDS system perceives information differently depending on its functionality or deployment. Considering the benefits and limitations of these systems, the key to detect nowadays advanced threats and collaborative attacks lies in distributed collaborative mechanism consisting of multiple heterogeneous IDS systems deployed in various parts of the network.

The proposed research work is specifically aimed at the investigation of global distributed collaboration of individual autonomous detectors and the relationship between system response characteristics (e.g. detection sensitivity), stability of these characteristics, and their predictability by the opponent. The collaboration mechanism is controlled by game-theoretical model, where multiple IDS sensors seek to optimize global collective objective though local decision making.

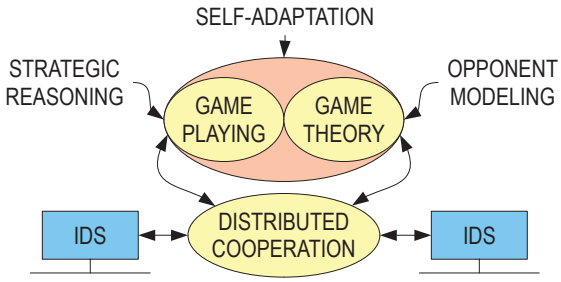

Fig. 1. Proposed game-theoretical model for distributed collaboration of IDS sensors.

2 Distributed Collaboration

In collaborative IDS system, each node shares information with other nodes according to predefined policies. Information sharing among heterogeneous systems can be utilized by fusion methods to reduce false alarm rates or find some relationships between reported alerts. Moreover, results from various parts of the network infrastructure may reveal more complex attack scenarios. However distributed information sharing can be also used for local/global optimization or reconfiguration, where each node adapts on the network environment with respect to other nodes in the system.

Distributed collaboration has been studied by research community from two perspectives. Majority of research focuses on multi-sensor alert correlation and data fusion techniques, where the goal is to fuse alerts from heterogeneous sensors to provide more reliable output of the system, e.g. by reducing false alerts [2]. However, another possible approach is to employ alert correlation into a feedback mechanism that influences behavior of all nodes and the whole collaborative system reacts as intelligent and robust Intrusion Detection Network.

In our work, we assume that the monitored network is covered by multiple heterogeneous IDS systems (nodes). We introduce game-theoretical framework (see Fig. 1) for distributed co-adaptation that requires the following assumptions:

- **Local self-monitoring** - all IDS nodes should be able of local reconfiguration to adapt on current state of the network according to the game model.
- **Interoperability** - outputs of all nodes should be in standardized format (e.g. IDMEF - Intrusion Detection Message Exchange Format), allowing their interaction even if their detection mechanisms are different.
- **Communication** - in our model, each node communicates with the rest of the nodes in a fully distributed manner. We justify the choice of distributed topology for its scalability and security properties - it does not introduce single point of failure. Moreover, possible communication overhead can be reduced by grouping alerts from a single node into one message.
- **Security** - for security reasons, nodes do not provide information about their internal state. Furthermore, secure communication channel should be provided to reduce the possibility of attacker's manipulation with the system.

– **Traffic assumptions** - strategic deployment of IDS nodes in the network is important to provide relevant information to the game model.

The above-mentioned assumptions define initial conditions of distributed co-adaptation controlled by game-theoretical model explained in Section 3.

3 Game-theoretical Model

We formalize distributed co-adaptation as a game between an attacker and a set of defenders represented by individual IDS nodes. Each player performs certain actions to achieve its predefined goal. An example of attacker's goal is to exploit secret data from private network. On the other hand, defenders' goal may be to prevent any attacker to achieve its goal.

In static environments, this game is well studied and converges to Nash equilibrium by using large variety of algorithms. However, in highly dynamic environments (like computer networks), behavior of the optimal algorithm is subject of recent research and has many unknown properties that are not yet well described. Pareto-optimal algorithms converge to more equilibria that may change in time as the game conditions evolve, so the system should be flexible and scalable for changing policies and goals. That means the optimal algorithm should select among more equilibria rather than converge to a single one.

In our model, we will modify regret minimization [1], which is well studied in static environments, and combine it with approaches from reinforcement learning to adapt regret minimization for dynamism of the network environment. More specifically, the combination of regret minimization and ε-greedy technique [4] may result in changing of equilibria according to the current network state.

4 Experimental Evaluation

In our experimental evaluation, we have deployed two IDS systems [3] in two different parts of the network infrastructure and have performed measurements on how distributed adaptation technique can improve detection performance of each IDS system. The first IDS was placed topologically in front of the second IDS and both nodes share their outputs (events).

In this scenario, we have inserted real malware behavior into 500 minutes of academic network traffic and have analyzed how well is the malware traffic separated from the background traffic in each 5-minute time window, by using sigma distance from threshold dividing legitimate and malicious zones [3]. Better separation from the threshold leads to more reliable detection. Analysis from the second IDS is depicted in Fig. 2, where we can clearly see the benefits of distributed adaptation, when both systems interact and reconfigure (we used ε-greedy mechanism - see Section 3). The number of successfully detected malware traffic was doubled when compared to the case when both systems only combine and fuse their results (no-feedback), which is still much better than stand-alone

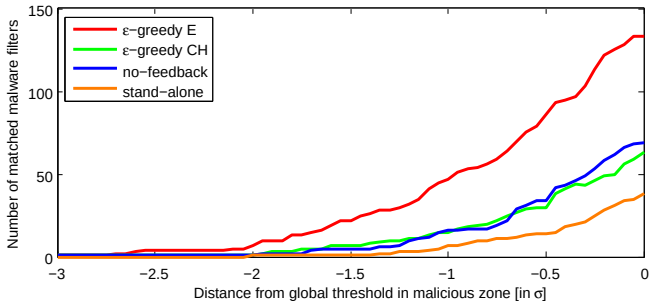

Fig. 2. Number of successfully detected malware traffic depending on their position in network distribution for various types of collaboration mechanisms - second IDS. Higher values are better.

configuration, when both systems ran separately. The first IDS shows very similar results. Note that in all cases, the number of false positives was similar as well.

This brief evaluation shows possible strength of distributed collaboration and their usefulness in current IDS systems to increase the overall detection potential, where alert fusion techniques may not be sufficient.

5 Conclusion

The proposed work aims to shift from individual, local intrusion detectors to the robust global security mechanism covering whole network infrastructure. The proposed distributed architecture will benefit from collective information sharing, where all individual detectors contribute to global modeling of the underlying network state, while strategically selecting the optimal amount of information to share. Moreover, each detector shall be able to adaptively modify its own local model on the basis of globally coordinated game playing strategy against corresponding opponent's sophisticated scenario. The concept of opponent aware, self-coordinating and strategically reasoning Network Intrusion Detection Networks allows effective collaboration of individual system defenders that may match a market-based collaboration structures of the attackers.

References

1. A. Blum and Y. Mansour. Learning, regret minimization and equilibria. In *Algorithmic Game Theory*, chapter 4, pages 79–101. Cambridge University Press, 2007.
2. H. T. Elshoush and I. M. Osman. Alert correlation in collaborative intelligent intrusion detection systems–a survey. *Applied Soft Computing*, 2011.
3. M. Rehak, M. Pechoucek, M. Grill, J. Stiborek, K. Bartos, and P. Celeda. Adaptive multiagent system for network traffic monitoring. *Intelligent Systems, IEEE*, 24(3):16 –25, 2009.
4. R. S. Sutton and A. G. Barto. *Reinforcement Learning: An Introduction*. The MIT Press, Mar. 1998.