

# An Anomaly-based Intrusion Detection Architecture to Secure Wireless Networks

Shu Yun Lim<sup>1</sup>, Andy Jones<sup>2,3</sup>

<sup>1</sup> British Telecommunications plc., Malaysian Research Centre, Malaysia.

<sup>2</sup> British Telecommunications plc., Information and Network Security Research Centre, Ipswich, United Kingdom.

<sup>3</sup> Edith Cowan University, Perth, Australia.  
{shuyun.lim, andrew.28.jones}@bt.com

**Abstract.** Ensuring that the appropriate level of security is available in wireless networks is absolutely essential. To aid in the defense and detection of potential threats, WLANs should employ security solutions that include an anomaly-based intrusion detection system (ADS) that identify wireless network intrusions by gathering and analyzing the data that is available on the system. This paper is to propose an hierarchical, extensible and flexible detection architecture to thwart such threats. By splitting anomaly detection into several stages it is possible to minimize the resources used as the common functionality of a system is less affected by a hierarchical system than by a system that keeps the whole of the detection functionality in one stage. This architecture can also be extended to include new anomaly detection mechanisms into the basic stage of the detection system. It can be deployed in a range of different networks and scenarios as a result of its flexibility.

**Keywords:** anomaly detection, wireless network.

## 1 Introduction

The use of wireless networking is becoming ubiquitous throughout the world. The real threat to security starts with the IT implementers who may not accurately assess the risks involved in the deployment of wireless technologies. Wireless signals often go beyond four walls of their organization or facility and, as a result, the organisation may be exposed to malicious systems that carry out activities such as sniffing, session hijacking and denial of service attacks in the vicinity of a particular access point. Damage can include the leakage of sensitive information, message contamination and node impersonation. Such networks need measures in place to autonomously detect adverse events and apply suitable countermeasures.

The problem of detecting anomalies, intrusions, and other forms of computer abuses can be viewed as finding unusual deviations in the characteristic properties in the monitored network. This assumption is based on the fact that intruders' activities must be different from the normal users' activities. However, in most situations, it is very difficult to detect or identify such differences before any damage occurs during break-ins. The conventional intrusion detection approaches need clearly pre-labeled

datasets for training, which requires a significant amount of human experts' participation. Data labeling is not only time consuming but is also error prone. An alternative approach of network behavior analysis is more robust and scalable. At the core of network behavior analysis are anomaly-based algorithms used to identify emerging threats. By applying anomaly algorithms best suited to the attacks they are designed to detect, they can proactively identify zero-day worms, malware, acceptable-use policy violations and insider misuse. It requires less configuration and ongoing maintenance than many other security methods.

However, existing anomaly detection systems use network processors to perform deep packet inspections of all observed packets in a backbone network. A lot of anomaly-based approaches cannot be applied in high speed network due to their high resource consumption or are only capable of performing a very coarse-grained detection without further refinement. This paper is to propose an hierarchical, extensible and flexible detection architecture to thwart security threats to wireless networks. By splitting anomaly detection into several stages it is possible to minimize the use of precious resources. The common functionality of a machine is less affected by the type of hierarchical system that is proposed than by a system that keeps the whole of the detection functionality in one stage. The proposed architecture can also be extended to include new anomaly detection mechanisms into the basic stage of the detection system. It can be deployed in a range of different networks and scenarios due to its flexibility.

## 2 Related Works

The aim of this paper is to propose an efficient wireless ADS in an infrastructure-based wireless network and to use anomaly detection techniques to detect different types of attacks within the wireless network. To do this we investigate the recent evolution in intrusion detection.

Zhang and Lee [1] first presented a distributed intrusion detection and response architecture for wireless ad hoc networks, which provides an excellent guide for the later works. M Thottan et. al. [2] proposed a proactive network anomaly detection model. They defined a set of proactively detectable anomalies in terms of management information base variables and the time series data obtained from these variables when they are analyzed by a signal processor. This work is shown to be amenable to distributed implementation and is a promising approach to self-managed networks.

Hongmei Deng et. al. [5] proposed an agent-based cooperative anomaly detection scheme for wireless ad hoc networks. The approach addresses the underlying distributed and cooperative nature of wireless ad hoc networks and adds one more dimension of cooperation to the intrusion detection process. That is, the anomaly detection is performed in a cooperative way involving the participation of multiple mobile nodes. The scheme detects various types of attacks based on the model learned only from normal network behaviors. Without the requirements of pre-labeled attack data, the approach eliminates the time-consuming labeling process and the impacts of an imbalanced dataset.

E. Y Chen [3] proposed the deployment of shields which scan for several different anomalies but which have to do deep packet inspection that can cause a delay in the

forwarding of packets. In addition, a command module can for further anomalies in aggregated traffic behind the shields, in order to try to learn the signatures of normal traffic in order to detect Distributed Denial of Service (DDoS) attacks. This procedure is likely to use significant resources, primarily memory and processor time.

D. Sterne et. al. [4] gave an architecture which is organised as a dynamic hierarchy. Detection data is acquired at the leaves and is incrementally aggregated, reduced and analysis as it flows upward toward the root. Our proposed approach also uses the distributed hierarchical architecture, however, it carries out the detection process stage by stage. This is necessary in order to use the resources efficiently.

### **3 Anomalies in Wireless Networks**

#### **3.1 Worm Propagations**

Worm propagation attacks exploit security weaknesses in operating systems or applications to penetrate a system and to propagate themselves to as many other systems as possible. Today's countermeasures to worms are signature-based detection systems scanning for identified worms. These systems are typically located at the victim's edge of the internet, preventing the worm propagation to a specific network. The ability to detect and suppress the worm at a very early stage in its propagation is essential and we need to monitor and react to worm traffic within the shortest possible interval of time. A signature-based detection system cannot respond to these attacks at the required speed due to time-consuming worm packet content analysis. An anomaly based detection system can improve detection speeds by monitoring traffic changes, for example by matching destination port numbers between incoming and outgoing connections, analysing the ratio of error messages due to closed ports generated by the scanned systems to the total number of connection requests [6].

#### **3.2 Wormhole Attacks**

The wireless environment facilitates mobility and cannot guarantee any knowledge about a participating node and as a result it is much easier to threaten the routing protocols or certain connections than in wired networks. By establishing a wormhole [8], an attacker aims at attracting as much traffic as possible to a node controlled by himself. This can be done by influencing the routing metrics in such a way that the other nodes assume the attacker, who has established a tunnel, is in their neighborhood. In fact the attacker may be located a significant distance away. A wormhole attack causes an anomalous increase in the volume of traffic near the tunnel endpoints as well as an increasing drop rate for packets which are routed through the tunnel.

### **3.3 Distributed Denial of Service (DDoS) Attacks**

The DDoS attack is a major threat. The attacker does not exploit a weakness of the victim's OS or application but aims to overload resources such as the link capacity or system memory by flooding the system with more traffic than it can process. The objective of any denial of service attack is to prevent users from accessing network resources. The usual methods of triggering DDoS attacks are to flood a network with degenerate or faulty packets, crowding out legitimate traffic and causing systems not to respond. This anomaly would result in heavy traffic volumes.

### **3.4 Botnet**

A collection of compromised hosts, called zombies or bots, when controlled by a single command and control infrastructure, form what is called a botnet. Botnets often involve thousands of hosts that can be collectively commanded to launch highly effective coordinated cyber-attacks. A botnet detector can look at exploit patterns, code downloading, bot coordination communications and outbound attack launches. By comparing these known botnet traffic patterns to the traffic flows within the trusted network, it can alert users when it detects flows that are likely to comprise botnet traffic.

## **4 Attack Detection Approach**

In the event of wireless attacks, a malicious compromised node attracts other nodes to send their traffic to it; causes traffic collisions that can disrupt networks; and exhausts a node's resources by sending a large number of packets to the target. It can clearly be seen that these types of attacks will make the network traffic deviated from that in normal condition in different ways. If a wormhole is set up by an attacker, traffic to some nodes (compromised nodes) will be observed to suddenly increase. A DDoS attack will raise the number of packet collisions while botnet and malware propagation will demonstrate an increasing amount of traffic related to one node. Therefore, we can detect attacks in wireless networks by monitoring for these anomalies.

Anomaly detection systems can be extremely effective and can run without modifications on a range of different networks. Nevertheless, it is necessary to adjust some thresholds whenever the application is moved as every network or host has its own peculiarities and without threshold tuning the network administrator is often alerted by events that are normal on some hosts.

## **5 Proposed Architecture**

WLANs typically encompass a relatively large physical area. In this situation, many wireless APs can be deployed in order to provide an adequate signal strength over a

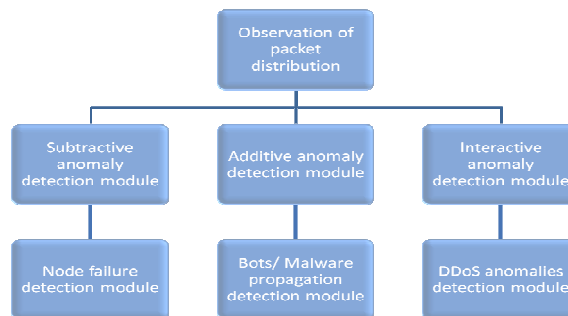
given area. An essential aspect of implementing a wireless ADS solution is to deploy sensors wherever a wireless AP is located. By providing comprehensive coverage of the physical infrastructure with sensors at all wireless AP locations, the majority of attacks can be detected.

Our security architecture relies on the combined functionality of two agents: *Nodal* and *Root Agents*. The nodal agent is used to monitor local security. It functions with no abstraction and is specifically designated to an individual network node. All nodes on the network have a corresponding nodal agent. A nodal agent sits in the network to observe packet distribution which is the first stage of the detection mechanism. In the event of a security breach or an attack, it will alert the root agent. Using a centralised approach, the root agent is deployed in the AP itself. It serves as the central management system to process all the data gathering and processing. Its primary goal is to monitor the state of its corresponding network infrastructure and nodal agents.

The proposal is a hierarchical, extensible and flexible system. In 2008, D. Brauckhoff et. al. [9] introduced FLAME, a flow level anomaly modeling engine that can be used to do meaningful evaluations of anomaly detection mechanisms. The authors also presented three categories of anomalies in a given flow trace i.e. *additive anomaly*, *subtractive anomaly* and *interactive anomaly*. After detecting an indication of an attack, by an exceeding of the threshold, another stage of the detection module will be loaded. These are the *subtractive anomaly detection module*, *additive anomaly detection module* and *interactive anomaly detection module*.

The first stage of the hierarchical detection system dedicates only a low level of analysis effort. It only observes packet distribution. Further stages are then loaded whenever an adverse event is assumed in first stage. These further stages detect only anomalies based on the information about the adverse event assumed in the first stage. Splitting anomaly detection into several stages can help to save resources. The common functionality of a machine is less affected by a hierarchical system than by a system that keeps whole detection functionality in one stage.

Lastly, the proposed system can be extended to include new anomaly detection mechanisms into the basic stage of the detection system. It can be deployed in a range of different networks and scenarios due to its flexibility. This architecture allows for broad security throughout a ubiquitous networking scheme.



**Fig. 1.** Architecture of the detection system.

### **5.1 Subtractive Anomaly**

By creating a baseline for the local network data and then observing any significant anomalies in the traffic from that baseline, it is possible to detect that network attacks are occurring. Careful distinctions can be made between normal amounts of control packets, and anomalous amounts of control packets. In the case of subtractive anomaly, outages or failures can cause a removal of specific network traffic from the baseline traffic.

### **5.2 Additive Anomaly**

Network scans and botnet activities can add network packets to the baseline but do not interact with the existing traffic.

### **5.3 Interactive Anomaly**

An example of interactive anomaly is the denial-of-service (DoS) attacks that add traffic and have an impact on the baseline traffic. Most of the existing DoS attacks lead to an imbalance in the symmetry between incoming and outgoing sub-aggregates which belong together by protocol definition. For instance, a TCP SYN flooding attack tries to exhaust a victim's open connection storage space by flooding the victim with TCP packets with SYN flag set. Due to the mass of connection request the victim can only respond to a proportion of all of the requests by sending TCP packets with SYN and ACK flag set. All remaining requests are dropped and the victim sends no response at all if storage space is already exhausted. This leads to an asymmetry between incoming TCP packets with SYN flag set and outgoing TCP packets with SYN and ACK flag set which can be used to detect this kind of DoS attack.

## **6 Conclusions**

A wireless anomaly detection system is an important addition to the security arsenal of wireless local area networks. While there are drawbacks to implementing a wireless ADS, the benefits should prove to outweigh the shortcomings. With the capability to detect DDoSs, zero day worm outbreaks and a variety of 802.11n attacks, the benefits of a wireless ADS can be substantial. In view of the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.

## References

1. Y. Zhang, W. Lee, Intrusion Detection in Wireless Ad-Hoc Networks, Proceedings of the 6th International Conference on Mobile Computing and Networking, MobiCom 2000, pp.275-283, MA, USA (2000)
2. M. Thottan and C. Ji, Proactive anomaly detection using distributed intelligent agents, IEEE Network, vol. 12, pp. 21–27 (1998)
3. Eric Y. Chen, AEGIS: An Active-Network-Powered Defense Mechanism against DDoS Attacks, Proceedings of the IFIP-TC6 Third International Working Conference on Active Networks, p.1-15, (2001 )
4. 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, Proceeding of the Third IEEE International Workshop on Information Assurance (IWIA'05), USA (2005)
5. Hongmei Deng, Roger Xu, Jason Li, Frank Zhang, Renato Levy, Wenke Lee, Agent-Based Cooperative Anomaly Detection for Wireless Ad Hoc Networks, 12th International Conference on Parallel and Distributed Systems (2006)
6. Xuan Chen, John Heidemann, Detecting Early Worm Propagation through Packet Matching, ISI-TR-2004-585 (2004)
7. Mell, Mark McLarnon, “Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems” International Workshop on Recent Advances in Intrusion Detection, Purdue University, September 7-9, (1999)
8. Yi Hu, A Perrig, DB Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Vol. 3 (2003), pp. 1976-1986 vol.3. INFOCOM (2003)
9. Daniela Brauckhoff, Arno Wagner, Martin May, Flame: A Flow-level Anomaly Modeling Engine Usenix Security, CSET Workshop, San Jose, CA, USA, July (2008)