

Research Proposal

Title: Configuration and Visualization of a Wireless Network Monitoring Environment

Author: Thio Meng Aun, Mark

Supervisor: Dr Chris McDonald

Background

Many individuals and organizations depend on 802.11 wireless LANs to provide connectivity for time-sensitive applications like voice and video. With this reliance comes an increased need to monitor the traffic at the Media Access Control layer (MAC) to detect a growing set of simple but effective Denial of Service (DoS) attacks [1] that might compromise the throughput and disrupt the connectivity of the network.

A network monitoring tool like Dartmouth College's "MAP" (Measure, Analyze, Protect) system provides the capability to capture wireless traffic over a broad area, detect and merge duplicate frames captured by wireless access points with overlapping coverage areas, and detect 802.11 MAC-layer attacks in real-time [2]. Figure 1 in the appendix gives an overview of the architecture of the MAP system and a description is given below.

Software on a number of wireless access points termed Air Monitors (AMs), is used to capture frames from the network using a variety of sampling strategies. Some sampling strategies aim to capture a maximum number of frames with minimum redundancy from the overlapping AMs on the same channel [3]. Captured frames are sent to a centralized software component named the *merger*. The merger uses the received frames from all the AMs to form a unified stream on a coherent timeline. This stream is received by subscribing analysis software components which determine if there are any suspected MAC-Layer attacks taking place within the network. If so it would send this information (eg: MAC address of suspected attacker) to another software component named the *controller* and also to the software components in the protection engine layer. The controller acts on this information by instructing the AMs to focus more on the suspected target by using refocusing [4]. Components in the protection engine could react to this information by sending an alert to the network administrator or even changing of firewall rules to block the offending culprit. How the protection engine behaves is entirely up to how it is configured.

The MAP system offers a number of advantages over other monitoring systems including its provision of a flexible sampling strategy, having the ability to refocus on “interesting” areas of data collection and also the merging of duplicate frames that have been captured [2].

Limitations

Although the MAP system is useful and has its advantages, parts of its design and implementation could be improved or extended.

Currently, in order to set up an experiment for the MAP system, a tool called the *mapmaker* is required. This tool does not scale well as it requires many SSH connections to be maintained for the AMs in the environment. Also if the configuration is changed, all AMs may need to be restarted. The *mapmaker* also requires a configuration file. Users wishing to load another configuration require knowledge of the syntax of the *mapmaker*.

Another limitation is that only one experiment may be set up using a single MAP system at any time. Starting multiple instances of configurations created by *mapmaker* could cause unintended behaviour by the AMs and thus restricting their ability to effectively capture network traffic.

The current MAP system is also unable to provide any form of real time visualization of the data collected and analyzed.

The software running on the AMs also has certain limitations. It is unable to run multiple filtering predicates, this functionality would be useful in multiple environments.

The software component called the controller periodically polls every AM to determine their status. A better approach is to have a *watchdog* process that runs on the AMs themselves. This watchdog process could load other processes and one of these processes might just be to periodically alert the controller of its status.

Project Aim

The project’s aim is therefore to devise and develop a number of components that will enable configuration of the MAP system that addresses the limitations described above.

Part of this is a GUI component that will provide a current visual representation of the status of the wireless network being monitored. It would also display the current configuration of the experiment and also to present data that has been collected and analyzed in a meaningful manner. This will enable the user to visualize what is happening in the wireless environment in order to help determine the cause, effect and estimated area where the problem is present.

The GUI should also be able to allow configuration requests to be created and this would shield the user from the unnecessary complexity of learning the mapmaker syntax and also prevent errors that could be introduced by an incorrect configuration file.

Method

The project will consist of the following tasks

1. Background Research
 - a. Research into the inner workings of the MAP system. This is essential as thorough knowledge of how to communicate with the components of the system is required.
 - b. Learn how to perform remote configurations of AMs.
2. Developing the application
 - a. Develop a GUI which is used to present the configuration of the experiment and also to display relevant information in a meaningful manner.
 - b. Develop a tool that uses the input from the GUI and does the necessary configuration to the MAP system.
3. Setting up & testing
 - a. Set up a local instance of the existing MAP system in CSSE.
 - b. Implement the developed application and test if it works as intended.

Software and Hardware Requirements

Linksys WRT54GL wireless access points/ routers with OpenWrt Linux installed.

The lab computers in CSSE 2.07 will be sufficient to run the other software components.

References

- [1] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, August 2003.
- [2] Sheng, Chen, Tan, Deshpande, Vance, Yin, McDonald, Henderson, Kotz, Campbell, Wright, *MAP: A scalable monitoring system for dependable 802.11 wireless networks*. (to appear) in "IEEE Wireless Computing", October 2008
- [3] U. Deshpande, C. McDonald, and D. Kotz. *Coordinated sampling to improve the efficiency of wireless network monitoring*. In Proceedings of the Fifteenth IEEE International Conference on Networks (ICON), September 2007.
- [4] U. Deshpande, C. McDonald, and D. Kotz. *Refocusing in 802.11 wireless measurement*. In Proceedings of the Passive and Active Measurement Conference (PAM 2008), volume 4979 of Lecture Notes in Computer Science, pages 142–151. Springer-Verlag, April 2008.

Appendix

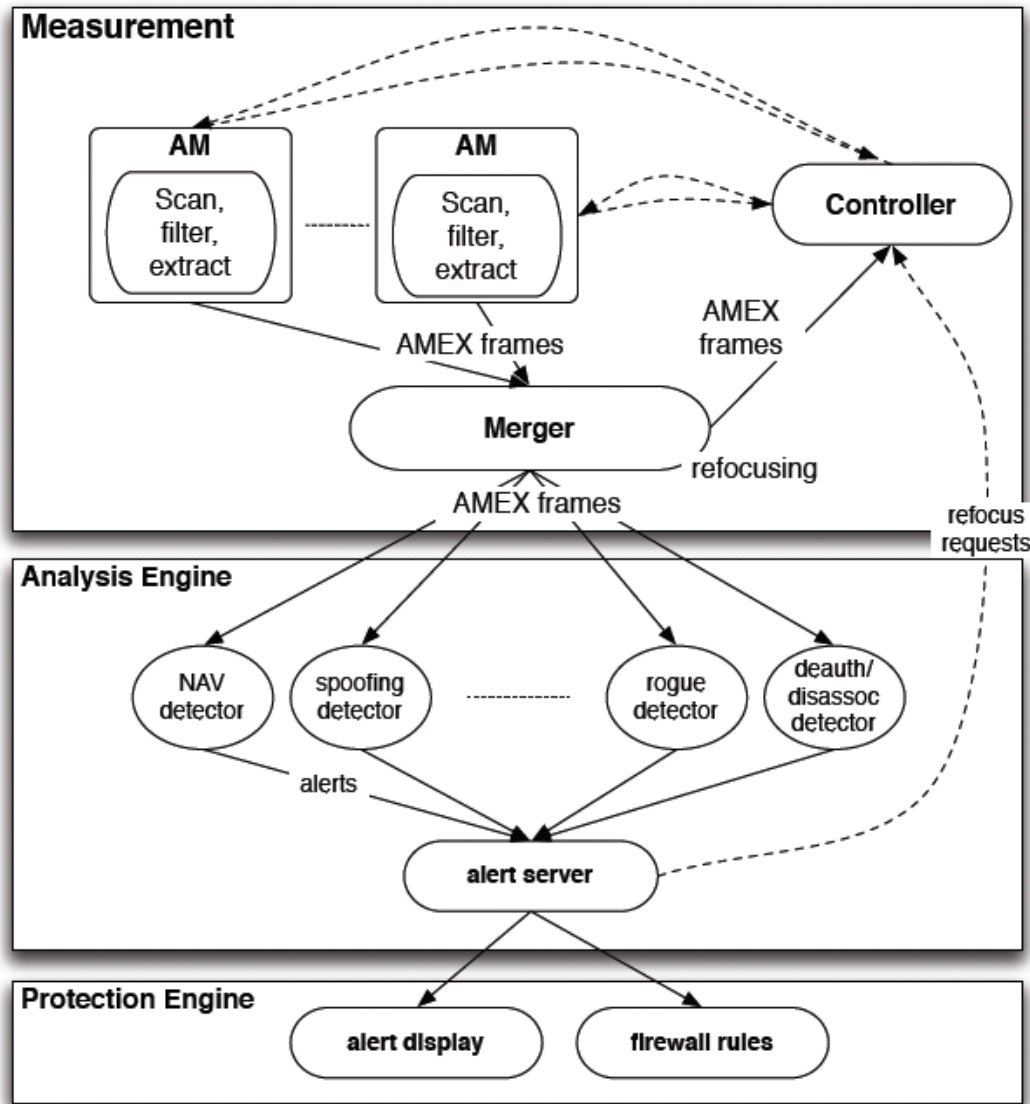


Figure 1. The MAP architecture; dashed lines are control streams and bold lines represent data streams.