Sample Reviewed Paper

- Here insert Title of the Paper example:

A Data Mining Analysis of RTID Alarms

- Reviewer: Type your Name & ID No.
- Type a shorter summary about the paper. For example

Short Summary of the Paper

The paper mainly presents two key contributions:

1. The idea of using volumes of alerts generated by a misuse detection system to achieve anomaly detection by characterizing "normal" alarm patterns.
2. The notion of using alarm contexts and histories to achieve better anomaly detection.

The authors also present some experimental results on real sensor data to show that the methodology is effective and can be improved. The paper, however, seems to be unclear along several lines making the technical and presentation aspects appear weak. With suggested improvements along these lines, the paper can make a good case for the integration of both misuse and anomaly detection systems for network intrusion detection. This integrated approach, I think, has good practical implications, particularly since misuse detection system sensors can generate very high volumes of alarms, analysis of which becomes a daunting task. Segmentation of customers based on the sensors they use, for assisting service strategies is a nice idea. Comments and suggestion are listed in the next section.

Comments on the Paper

(Here you can enter your comments in detail for the author(s). you can give comments in any parts of the paper by considering the main contributions; positive aspects; and negative aspects of the paper)

Example:

The paper addresses the issue of effectively utilizing alarm sets generated by a misuse detection system for detecting alarm anomalies. The novel contribution is the idea of using contexts and histories of alarms in detecting anomalies. The use of “alarm burst” seems to be a novel idea and will properly fit the need of a real-time system, which the authors intend to pursue. An alarm burst has been said to correspond to a transaction, but since we are dealing with alarm data generated by the RTID sensors, this correspondence appears a little fuzzy and I think it requires some more clarification. For example, how do we view a stream of alarms, which may be independent, as a coherent group as suggested by the notion of a transaction? The importance of the clear notion of an “alarm burst” is even more heightened by the fact that the basic notion of the “normal” alarm stream is related to frequent item sets within an alarm burst. …

General Suggestions on the Paper

(Here you can give general suggestions on the paper)

Example:

The paper makes a good effort in trying to use data mining techniques over a huge volume of data produced by a set of misuse detection systems. The critical components involved in this technique are:

•Characterizing properly the alarm bursts from the incoming streams of alarms from the RTID sensors.

Capturing and using context and history information to better detect the anomalous behaviors of alarm streams.

The paper clearly indicates that it is reporting preliminary results towards building anomaly detection system over the misuse detection systems. Efforts to develop empirically justified way of characterizing "alarm burst" cannot be seen in the paper. Information gathering, in section 3, is also somewhat ad hoc and seems to have many attributes related to each alarm. Although they may capture a lot of information, dimensionality may be a problem, because the RTID sensors generate huge volumes of alarms. The paper, however, presents a practically viable technique, which I think can be very useful, provided authors can establish empirically sound sets of "alarm burst" characteristics that can be used in different kinds of networks. I think, at its present form, with improvements suggested in the previous section, the paper makes an acceptable case for publication. I think this will generate research interests in improving the two components mentioned above

- Finally, write the full citations of the paper.

Example:

Pwerd A, Hearxu, T. K., & Mealex, S. Z. (2020). A Data Mining Analysis of RTID Alarms. *Int. J. Adv. Comput. Sci. Appl.*, *10*(3), 555-561.