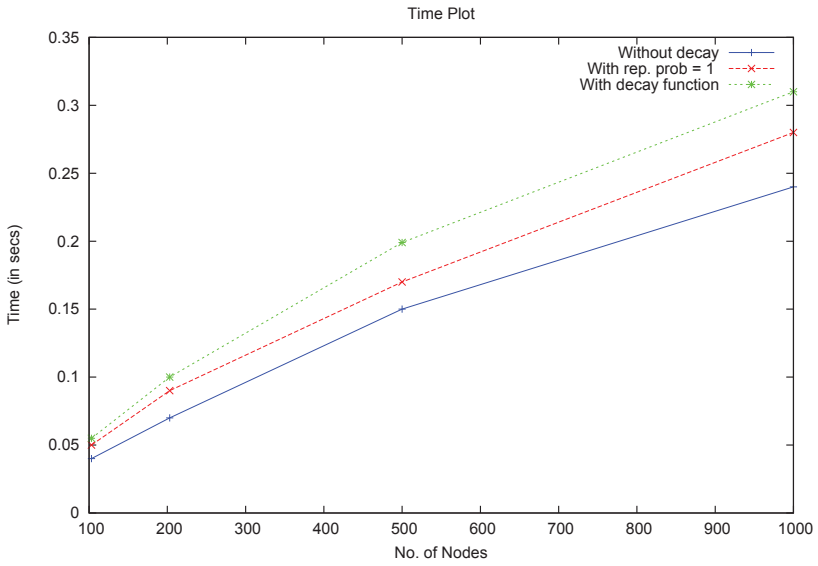

Figure 3.3: Variation of metric computation time (in sec) with size of attack graphs. Memoryless, partial memory and full memory of attacker for repeated vulnerabilities are considered. Time is reported in seconds.

Workstation (8 GB memory). It can be seen that the the growth of computational time is sub-exponential. The computation time is highest for the case of partial memory attacker scenario.

3.5 Conclusion

Security analysis is a challenging problem due to inherent complexities of attack modalities, scale and computational cost. We present a structured framework for probabilistic security metric computation using an multiplicative idempotency operation that can handle repeated vulnerabilities in an attack path. Proof of correctness and complexity analysis of security metric computation are provided. The metric is then extended to model the scenario where attackers have (i) full memory of previous exploits, (ii) partial memory of repeated vulnerabilities as characterized by a decay function, and (iii) no memory of past exploits. The metrics are then used for computing vulnerabilities of large attack graphs having cycles and repeated vulnerabilities. Scalability of the propose method with increasing network size is studied.