International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Review on: Ontology Based Approach to Detect DDos Attacks in Ad Hoc Networks

Bikramjit Singh[1], Er.Maninder Sharma[2]
[1]Computer Science & Engineering,
Doaba Group of College, PTU, Punjab, India
[2]Electronics & Communication Engineering,
Doaba Group of College, PTU, Punjab, India
[1]bikram4127@gmail.com, [2]maninderecediet@gmail.com

Abstract: *Adhoc network have a features of their less infrastructure network consisting of mobile terminal with the capability to communicate with each other nodes. Due to less infrastructure any mobile terminal can attach and leave the network. Mobile nodes can attach each other nodes through automatically configuration. So this feature make mobile Ad hoc network powerful and flexible when mobile nodes of Ad hoc network try to transfer the data. Then various security flaws and attacks have created to interrupt the services of Ad hoc Network. which makes the Ad hoc network vulnerable. DDoS attacks are more powerful attack in Ad hoc network as compare to other attacks. In this work we purposed a effective approach to detect and identify the DDoS attacks class, consequences and perquisites. We use Ontology based approach to developed the ontology of DDoS attacks .We detect the security flaws, weakness ,vulnerability and other various attacks of DDoS attacks in Ad Hoc. By using the Ontology based approach the first goal of this work is to developed the DDoS attacks Ontology and their consequences ,perquisites, impacts and attacks in logical way . Then we utilized Jena Framework to detected and read the DDoS attacks classes from DDoS RDF and knowledge base and then we can extract the logical and reasonable results from DDoS attacks knowledge base .In this work we used DDoS attacks domain purposed Ontology is generated the well known Taxonomy CAPEC,CVE CWE .ISS-X-Force and OSVDB data sets. This purposed work is used to read the DDoS attacks but also detect and defined the DDoS attack Classes in Ad hoc.*
.

Keywords: *Adhoc, DDos, Protégé, Ontology.*

I. INTRODUCTION

One of the most bright and discussed technology in the last decagon is the wireless technology which allows users to utilize devices that enable the access to information at any time any place. These desires make wireless networks the greatest solution for interconnecting devices and people. Wireless networks are comprised of devices that communicate through media such as radio signals and infra-red, and they are commonly classified into two categories: Infrastructure-based and ad hoc wireless networks.

Infrastructure-based wireless network consists of base stations restricted in convenient places, which provide wireless connectivity to devices surrounded by their coverage area. An example of this category is Wireless Local Area Networks (WLANs) [1]. A WLAN is a bendable data communication system structured as an extension to a wired LAN within a building or campus. WLAN technology is currently experiencing tremendous growth in popularity, presenting secure, flawless mobile access into commercial environments, homes and residential areas, and public spaces. WLAN technology is not new; however, with the increasing awareness of the require for security, the advanced assumption rate of mobile user devices such as PDAs, cellular phones and WLAN-enabled laptops, and the availability of new interactive applications, WLANs are becoming a common option.

On the other hand, Ad hoc wireless networks do not have a pre-reputable infrastructure. Moreover nodes connect to each other through automatic configuration when they are in transmission range and willing to dispatch data for former nodes. In this tatic, an ad hoc wireless network is formed which is both flexible and powerful.

Any node in this type of network can participate and leave at any point of time. Therefore these networks are more vulnerable to the different type of attacks out them are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks which occur due to their availability for anyone. The reasons behind these types of attacks are that there is no idea when any particular node attached and leaves the network. The previous work done is upon the study about the impact of the denial of services on ad hoc networks and measured their performance based on various parameters. But it has not been considered that the attacker can dominate the performance of this network [2].

In this research work Ontology based approach have been used to construct by using Protégé tool in order to identify these types of attacks. This approach helps to build the framework for the DoS and DDoS attacks [9] that define how to detect and remove these attacks by using the various parameters. Once the Ontology is asserted into the knowledge source and all of the imitative rules ensuing from the chains of implication are generated, the knowledge base is ready to receive the instances of the Ontology. Instances are asserted and de-asserted into and from the knowledge base as temporal events dictate. To query the knowledge base for the existence of an attack or intrusion, the query could be so granular that it requests an attack of a specific type [8]. These parameters will be stored into the knowledge based expert system and using this knowledge base we will identify the DDOS attack which can be known and unknown.

II. LITERATURE REVIEW

Amina Souag et al. [14] proposed a security ontology, but a gap still exists between the two fields of security requirement engineering and ontologies. This paper is a survey about the analysis and a typology of existing security ontologies and their use for requirements definition.

A.Lavanya1and K.Saravanan [21] discussed about the Distributed Denial of Service (DDoS) attack which has become a major problem to networks. Network resources such as network bandwidth, web servers, and network switches are mostly the victims of DDoS attacks. In this paper the different types of DDoS attacks are summarized and the detection mechanisms are described. Also highlights some of the DDoS incidents occurred in the year 2010-2011.

Lamsfuset al. (2004) describes a domain ontology developed to represent the associated knowledge and enable the description, exchange and sharing of multimedia added-value content for the creation of artistic expressions. It seeks to extend domain specific aspects of CIDOC-CRM. CIDOC-CRM is a formal ontology intended to facilitate the integration, mediation and interchange of heterogeneous cultural heritage information; its scope is the curated knowledge of museums [28]

Hyvonen et al (2004, 2006) present one of the more comprehensive attempts to apply ontology based semantic web approach for the integration of Museum information. It enabled the integration the databases of three different museums with different relational database schemas, database systems and collection management systems. The end user is provided with a semantic search engine with two major services: (1) a semantic view-based search engine based on underlying concepts and ontologies instead of simple keywords. (2) a semantic recommendation system through which explicit and implicit semantic associations can be found and used for browsing the collections.

F. Abodoli et al. [15] introduced the ontology for attacks using the tool PROTÉGÉ. In this paper they have discussed about utilizing methods and techniques of semantic web in the Intrusion Detection Systems. To extract semantic relations between computer attacks and intrusions in a Distributed Intrusion Detection System, they used ontology. Protégé software is the selected software for building ontology. In addition, they utilized Jena framework and SPARQL query language to identify and detect the attacks [6].

III.OBJECTIVES

The objectives of the thesis are summarized as follows:

- Study of ad hoc network, its characteristics, usage, security goals, challenges and security flaws in these types of networks.
- To understand the reliability and security issues related to ad hoc network along with their impact on the network.
- Study of Denial of Service and Distributed Denial of Service attacks.
- Identifying the method to be used for the detection of Distributed Denial of Service attacks.
- To design Ontology based approach for the detection of Distributed Denial of Service attack by using PROTÉGÉ software.
- Finally to design an interface to access the proposed Ontology through Jena framework.

.

IV. CONCLUSION

An ad hoc network is the multi-hop model with no pre-established infrastructure in which nodes are self configuring and self managed which can set up momentary network on demand in a dynamic network topology. An ad hoc network is an infrastructure less network consisting of mobile terminals with the capability to communicate with each other. As ad hoc networks do not have a pre-conventional infrastructure. Moreover nodes unite to each other through automatic configuration when they are in transmission range and willing to forward data for other nodes. In this way, an ad hoc wireless network is formed which is both flexible and powerful. Any node in this type of network can participate and leave at any point of time. There are different security flaws and attacks on ad hoc networks. Therefore these networks are more vulnerable to the different type of attacks out of them are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks which occur due to their availability for anyone. This study is an attempt to review the ad hoc networks, and hence understood its research challenges and goals. This thesis also presents an in-depth literature review of the existing vulnerabilities and attacks like DoS and DDoS and also includes the methodology to be used for the detection of these attacks. For this Ontology based approach has been used and for accomplishing this task PROTÉGÉ software is used. For this research work PROTÉGÉ 2000 version 4.2 and OWL Plug-in are used.

In this paper, an Ontology based approach for DDoS Attack on Ad hoc Network has been designed. In this research work we used some new Data sets and Ontology. And an interface is used to access the proposed Ontology through JENA framework. Because of generalized and conceptualization feature of ontology we can present an ontology for DDoS attacks which illustrate the relationship between many classes, subclasses and instances used in the DDoS Attacks. The Results includes various DDoS attack related classes from the DDoS knowledge base. The Knowledge Base is created by some Dataset's heterogeneous relationship with other weaknesses, vulnerabilities and some other attacks classes of the DDoS Attack in ad hoc network. In our purposed work DDoS attack based ontology stores N-triples i.e. Subject, Predicate and Object in DDoS knowledge Base. We detected the particular attack relationship with other attacks weakness and vulnerability by using the SPARQL Query and JENA framework. Some issues have been found when doing work on ontology based approach:-

- First issue is how to create and define the DDoS Class. In this work DDoSS classes are created by their types. But these can also be created in some other way.

- Reasoner is used in this work which classifies all the classes. If Reasoner is not used then how inconsistency (if any) available can be resolved. Can we develop the DDoS attack base ontology without hierarchical structure? if this can be done then how we extract the results from the given knowledge base.

REFERENCES

[1]. K.higgins, R.Egan, S.Hurley, M. Lemur, "Ad Hoc Networks", *Technological Survey,* 2005.

[2]. Gray Breed, "Wireless Ad Hoc networks: Basic Concepts," *High Frequency Electronics,* Summit Technical Media, LLC, vol 12, no 4, pp 30-36, 2007.

[3]. Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F. Hassan, Magdy S. El-Soudani, "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a Proposed Decentralized Scheme," *Proc. of Third International Conference on Availability, Reliability and Security,* vol 13, issue 2, pp 50-55, 2006.

[4]. A.Lavanya, K.Saravanan, "A Review of DDoS Attacks In Mobile Ad-hoc Networks," *Proc. of International Journal of Societal Applications of Computer Science,* vol 1, Issue 1, pp 22-28, November 2012.

[5]. Daljeet Kaur, Monika Sachdeva, Krishan, "Study of DDoS attacks using DETER Testbed," *Proc. of International Journal of Computing and Business Research (IJCBR) ISSN (Onlinev)* vol 3, Issue no. 2, May 2012.

[6]. Jelena Mirkovic and Peter Reiher "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *Proc. of ACM SIGCOMM Computer Communication Review,* vol 34, no 2, pp 39-53, 2004.

[7]. Ahmad Salahi , Morteza Ansarinia, " Predicting Network Attacks Using Ontology-Driven Inference," *Elesver Computer Networks,* vol 47, no 4, pp 445-487, 2005.

[8]. Amina Souag, Camille Salinesi, Isabelle Wattiau, "Ontologies for Security Requirements: A Literature Survey and Classification," *Proc. of Journal on Advanced Information Systems,* vol 112, pp 61-69, 2012.

[9]. Ju An Wang and Minzhe Guo, "OVM: An Ontology for Vulnerability Management," *Proc. of 5th Annual Workshop on Cyber Security and Information Intelligence Research,* pp 1-4, 2009.

[10]. John Pinkston, Jeffrey Undercoffer, Anupam Joshi and Timothy Finin, "A Target-Centric Ontology for Intrusion*,"* *Proc. of 18th International Joint Conference on Artificial Intelligence,* pp 9-15, 2004.

[11]. Andrew Simmonds, Peter Sandilands, Louis van Ekert, "An Ontology for Network Security Attacks," *Proc. of Applied Computing, Springer Berlin Heidelberg,* vol 3285, pp 317-323, 2004.