Journal of Theoretical and Applied Information Technology
31st July 2013. Vol. 53 No.3
© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN ONTOLOGY-BASED INTRUSION DETECTION FOR VEHICULAR AD HOC NETWORKS

[1] M.ERRITALI, [2]B. EL OUAHIDI, [3]B.HSSINA, [4]B. BOUIKHALENE, [5]A. MERBOUHA

[1, 2] Laboratory of computer science research
Department of Computer Science
Mohamed V Agdal University, Faculty of Sciences Rabat, Morocco
[3, 4, 5] Sultan Moulay Slimane University, Faculty of sciences and technology Beni Mellal, Morocco
E-mail:[1]mederritali@yahoo.fr , [2] ouahidi@fsr.ac.ma , [3] hssina.badr@hotmail.fr , [4]bbouikhalene@yahoo.fr , [5] merbouhak@yahoo.fr

ABSTRACT

A vehicular ad hoc network (vanet) is an independent system of vehicles connected by wireless connection to form a network. This type of network is used to reduce the number of accidents via the exchange of alert messages between the neighborhood vehicles. These alert messages constitute an ideal target for attacks that aim to prevent them to reach their destinations, and thereby endangering human lives.
In vanet ,intrusion detection has become an indispensable defense line in face of vulnerabilities such as high mobility, shared wireless medium and the absence of centralized security services offered by dedicated equipment , where authentication and access control mechanisms routinely prove inadequate in preventing new and increasingly numerous and disastrous attacks .However, when we think to deploy an ids the major problem rest the characterization of an intrusion. The use of a semantic resource such as ontology could be an effective way to enrich data about intrusions to respond more specifically to complex questions about the definition, nature, characteristic of the intrusion.
In this paper, an ontology for vanets Security has been modeled and specified using Web Ontology Language (OWL). The aim is to provide a complete classification which takes into account the impact of attacks and intrusions on the offered service, in terms of functionality implemented in routing protocols and other applications.

Keywords: *Ontology, Intrusion detection, OWL, Vanets, security.*

1. INTRODUCTION

A Vehicular ad hoc network called VANETs [1, 2] is a mobile network allowing to vehicles to communicate with each other in a peer-to-peer manner without any access points. In VANET, no fixed infrastructure, like base station or, mobile switching center is required. Instead, every vehicle within the perimeter of radio link acts as an intermediate router and participates in setting up the network topology in a self organized way. This type of network is used to reduce the number of accidents via the exchange of alert messages between the neighborhood vehicles. These alert messages constitute an ideal target for attacks that aim to prevent them to reach their destinations, and thereby endangering human lives. The characteristics of these networks such as: shared wireless medium, the highly dynamic network topology absence of conventional security infrastructures pose a number of nontrivial challenges to security design. Vulnerabilities of vehicular ad-hoc networks are not limited unfortunately in the physically insecure environment but also in routing and auto-configuration mechanisms used.
These mechanisms are based on trust between the participating nodes. If a node has a malicious behavior, all services offered by the cooperative network will be paralyzed (routing table poisoning, congestion, packet alteration ...).
Several solutions to these problems are proposed, such as symmetric cryptography, authentication and secure routing protocols, the problem with these solutions is that they are mostly specialized for a specific attack. In addition, they do not offer the possibility to detect new attacks, nor even to defend the network against internal compromise nodes.
In (VANET), intrusion detection has become an indispensable defense line in face of vulnerabilities such as high mobility, shared wireless medium and the absence of centralized security services offered by dedicated equipment , where authentication and access control mechanisms routinely prove inadequate in preventing new and increasingly numerous and disastrous attacks .

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

An intrusion detection system (IDS) is a mechanism to identify abnormal or suspicious activities through examinations of various parameters such as network traffic, CPU utilization, I/O utilization, user location, and various log file [3].

In literature proposed IDS use two approach [4,5]: the behavioral approach and the scenario approach. The first is based on the observation of user behavior and the detection of deviant behavior with respect to a normal activity. This change in behavior may indicate an intrusion attempt, either due to impersonating of the user, either by running unauthorized commands. The second approach consist to identify each attack by a own signature, then search in network traffic traces of these signatures. We note that scenario approach requires knowing the signature of an attack so it can detect it. The behavioral approach can detect unknown attacks, but the definition of normal behavior of user remains the main challenge.

In order to realize an intrusion detection system in VANETs, the main problem that we encounter is characterization of an intrusion, the use of a semantic resource could be an effective way to enrich data about intrusions to respond more specifically to complex questions about the definition, nature, characteristic of the intrusion.

For this it is possible to design a multi-agent architecture based on a knowledge base represented as an ontology. The ontology can be used to define a high-level conceptual modeling of this knowledge. The use of such architecture reveals itself conducive to the development of intrusion detection systems for vehicular networks.

It is possible to represent semantically the intrusion attempts and due to special abilities of agents, prevent and abort these attempts. This paper proposes a model of ontology for Vanets Security and its specified using OWL.

The rest of this paper will be structured as follows. Section 2 describes Ontology-based intrusion detection techniques. In section 3 we describes the OWL language used to specify ontology. In section 4 we present our ontology. Finally, the conclusions and future research are shown in section 5.

2. ONTOLOGY-BASED INTRUSION DETECTION TECHNIQUES

The term ontology is used in the field of semantic web and refers to a structured set of concepts in a particular field of knowledge. There are generally two global entities in ontology. The first aims terminology, that defines the nature of the elements making up the field of ontology in question, as the definition of a class in oriented object programming in definition of the nature of the objects that we will manipulate later . The second part of ontology explicit relationships between multiple instances of the classes defined in the terminology. Thus, within an ontology, concepts are defined in relation to each other (a graph model of the organization of knowledge), which enables reasoning and manipulation of knowledge.

In the last years, several papers have been proposed about Ontology-based intrusion detection techniques as the proposed by Filman and Linden [¬6].In this paper the authors propose an ontology OntoSec “ontology for security.” for representing security requirements of a software architecture based on agents called SafeBots.

Denker et al. [7] propose a security ontology for DAML+ OIL [8] in order to secure web services and data integrity of Web resources. For this, well known security methods and techniques are used such as password-based login or X509 certificates for authentication.

In [9] Simmonds et al. are proposed an ontology for wired network security attack with the focus on threat profiles and vulnerability profiles.

J. Undercoffer et al. [10] are presented a target-Centric Ontology for Intrusion detection, the ontology defines properties and attributes that are observable and measurable by the target of an attack.

In applying ontologies to the problem of intrusion detection, the power and utility of the ontology is realized by the fact that we can express the relationships between collected data and use those relationships to deduce that the particular data represents an attack of a particular type. Moreover, specifying an ontological representation decouples the data model defining an intrusion from the logic of the intrusion detection system. The decoupling of the data model from the IDS logic enables non-homogeneous IDS to share data without a prior agreement as to the semantics of the data. To affect this sharing, an instance of the ontology is shared between IDS in the form of a set of XML, RDF or OWL statements. If the recipient does not understand some aspect of the data, it obtains the ontology in order to interpret and use the data as intended by its originator.

3. OWL OVERVIEW

OWL is a new language in the domain of the web semantic used to represent ontologies

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

,developed by the World Wide Web Consortium (W3C) Web Ontology Working Group (Webont).
The first Working Draft "OWL Web Ontology Language 1.0 Abstract Syntax " is published in July 2002 and, ultimately, OWL became a W3C Recommendation in 10 February 2004.
As OWL is an effort in W3C's Semantic Web activity, it had to fit into the Semantic Web vision of a stack of languages including XML and RDF/RDFS[11,12],and had to maintain as much compatibility as possible with existing ontology languages, including SHOE [13], OIL [14] and DAML + OIL [8].
OWL has three sublanguages with increasing capabilities of expression and, of course, for different communities of users:
• OWL Lite is the primitive language of OWL. It is intended for users who need a hierarchy of concepts simple. OWL Lite is suitable, for example, for fast migrations from old thesaurus.
• OWL DL is more complex than OWL Lite, allowing a much greater expressiveness. OWL DL is based on logic description (hence its name, OWL Description Logics), despite its relative complexity facing OWL Lite, OWL-DL guarantees the completeness of reasoning (all inferences are computable) and their decidability (their calculation is done in a finite time).
• OWL Full is the most complex version of OWL, but also the one that provides the highest level of expressiveness. OWL Full is meant for situations where it is more important to have a high level of ability to describe, even if it can not guarantee the completeness and decidability of calculations related to the ontology. OWL Full provides however interesting mechanisms, such as the ability to extend the default OWL vocabulary.

4. CREATION OF ONTOLOGY

Within an ontology, concepts are defined in relation to each other using a graph model to organize knowledge, which enables reasoning and manipulation of knowledge.

4.1 Namespaces

In order to use terms in an ontology, it is necessary to specify precisely from which vocabularies these terms comes. This is why, like any other XML document, an ontology begins with a namespace declaration contained in a rdf tag "rdf: RDF".
We want to write An ontology-based intrusion detection for vehicular ad hoc networks. Here is the namespace declaration of our ontology:

```
<rdf:RDF
xmlns=http://www.owl-ontologies.com/Ontology1364497614.owl#
xmlns:protege="http://protege.stanford.edu/plugins/owl/protege#"
xmlns:owl=http://www.w3.org/2002/07/owl#
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
```

The last four statements introduce the OWL vocabulary and objects defined in the namespace of RDF, RDF Schema and data types of XML Schema.
We can write, following the declaration of namespaces, a header describing the contents of the current ontology. This is the tag "owl: Ontology" is used to indicate this information:

```
<owl:Ontology rdf:about="">
  <rdfs:comment> ontology describing VANETs</rdfs:comment>
  <rdfs:label> ontology about VANETs</rdfs:label>
    ...
```

4.2 Declaration of class

The description of the classes is done directly by the naming of this class.

```
<owl:Class rdf:about="#Actor"/>
  <owl:Class rdf:about="#consequences"/>
  <owl:Class rdf:about="#Attaks"/>
  <owl:Class rdf:about="#vulnirabilites"/>
```

It exists in every OWL ontology a superclass named Thing, which all other classes are subclasses. This brings us directly to the concept of inheritance.
Each vehicular network intrusion can be described according to a specific schema. We may associate to this schema four distinct classes constituting the highest level of abstraction shown in Figure 1.

Journal of Theoretical and Applied Information Technology
31st July 2013. Vol. 53 No.3
© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

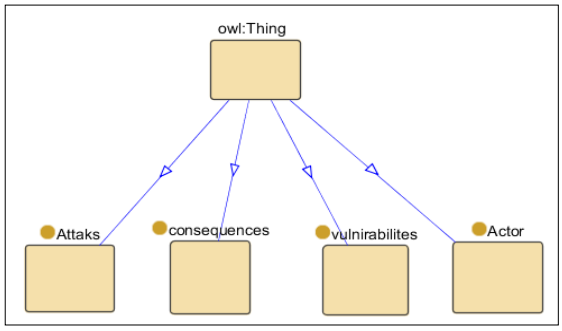

Figure 1: High Level Ontology (Generated by Protégé 3.4.8)

The first class, Attacks includes all concepts related to the intrusion. Several subclasses are described and show a clear separation between the types of attacks. The figure 2 illustrates the attacks ontology.

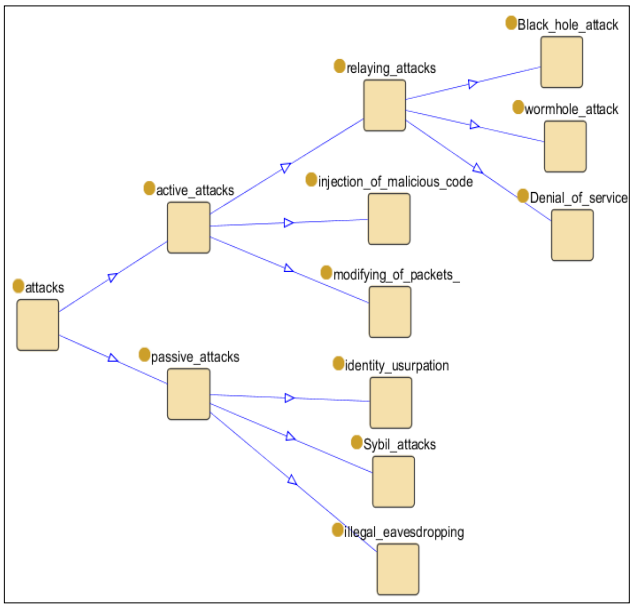

Figure 2: Ontology types of attacks

The class vulnerabilities of upper High Level Ontology describes VANETs vulnerabilities such as: shared wireless medium, the highly dynamic network topology, the absence of centralized security service and the cooperatives relationships. The figure 3 illustrates the vulnerabilities ontology.

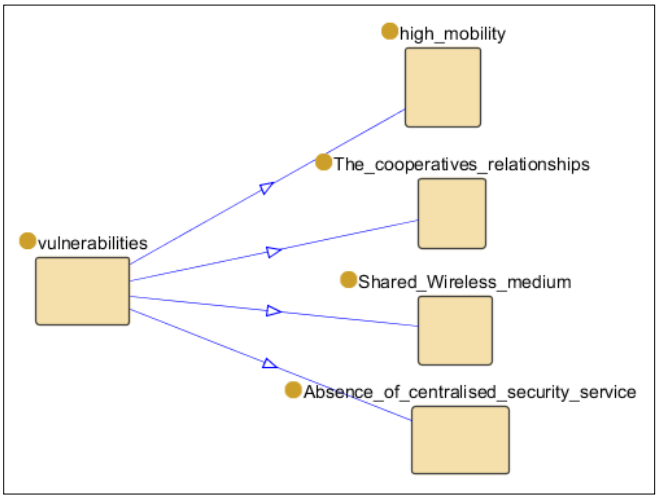

Figure 3: Ontology of possible vulnerabilities .

Consequences of intrusion in a vehicular ad hoc network may be: Degradation of network performance, flight of personal information, insulation of nodes, lead to road accidents and road congestion. The figure 4 illustrates the consequences ontology.

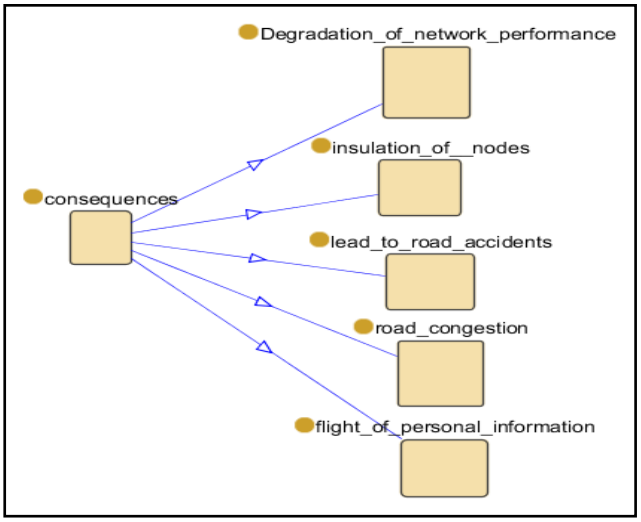

Figure 4: Ontology of consequences

5. CONCLUSION AND PERSPECTIVES

This paper proposes a formal description of various intrusions in vehicular ad hoc networks using an ontology. In this ontology we consider intrusion detection in terms of vulnerabilities as well as, point of view attacks and point of view consequences.

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The description of domain concepts and highlighting relationships between these concepts through ontology will allow the implementation of intrusion detection solutions more efficient and reliable.

Thereafter we propose to build a platform for validation of intrusion, the idea is to provide a method for identifying intrusion based on the semantics of intrusions that occurred before calling of different mechanisms of intrusion detections. This could provide a means of reducing the amount of false alerts generated by intrusion detection systems.

REFRENCES:

[1] S.Khalfallah, M. Jerbi, M. O. Cherif , M. Senouci , B.Ducourthial, Expérimentations des communications inter-véhicules, *Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)*, Les Arcs : France (2008).

[2] M. JERBI , Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections. *UNIVERSITE D'EVRY VAL D'ESSONNE, Thèse* , France (2008).

[3] O. Depren, M. Topallar, E. Anarim, M.K. Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Expert Systems with Applications 29 (2005) 713–722.

[4] F.Anjum,D. Subhadrabandhu , S. Sarkar, "Signature Intrusion Detectio for Wireless Ad Hoc Networks: A Comparative study of various routing protocols", in 2003.

[5] P. C. Kishore Raja, Dr.Suganthi.M, R.Sunder, "WIRELESS NODE BEHAVIOR BASED INTRUSION DETECTION USING GENETIC ALGORITHM", *Ubiquitous Computing and Communication Journal*, 2006.

[6] R. Filman, T. Linden, SafeBots: a paradigm for software security controls,*Proceedings of the 1996 Workshop on New Security Paradigms*, 1996,pp. 45–51.

[7] G. Denker, L. Kagal, T. Finin, M. Paolucci, K. Sycara, Security for DAML web services: annotation and matchmaking, *The Semantic Web-ISWC 2003, Lecture Notes in Computer Science, LNCS, vol. 2870, Springe*r,2003, pp. 335–350.

[8] DAML+OIL. http://www.daml.org/

[9] A. Simmonds, P. Sandilands and L.V. Ekert, "An Ontology for Network Security Attacks", *In Proceedings of Asian Applied Computing Conference(AACC 2004), LNCS 3285, Springer Verlag*, Oct. 2004, pp 317-323.

[10] J. Undercoffer, J. Pinkston, A. Joshi and T. Finin, "A Target-Centric Ontology for Intrusion Detection", *In IJCAI Workshop on Ontologies and Distributed Systems, IJCAI'03*, August, 2003, Acapulco MX.

[11] W3C: Resource Description Framework (RDF) model and syntax specification,*http://w3c.org/TR/2000/CR-rdf-syntax-19990222/*, 1999.

[12] W3C: Resource Description Framework Schema Specification (RDFS),*http://w3c.org/TR/2000/CR-rdf-schema-20000327/*, 2000.

[13] J. Heflin, J. Hendler, S. Luke, SHOE: A Knowledge Representation Language for Internet Applications, *Technical Report CS-TR-4078*, Department of Computer Science, University of Maryland, 1999.

[14] D. Fensel, F. van Harmelen, I. Horrocks, D.L. McGuinness, P.F. Patel-Schneider, OIL: an ontology infrastructure for the Semantic Web, *IEEE Intell. Syst. 16 (2) (2001)* 38–45.