Using Ontologies to Model Attacks in an Internet based Mobile Ad-hoc Network (iMANET)

Samrudhi Sharma
Dept. of Computer Engineering,
Dwarkadas J. Sanghvi College
of Engineering, Vile Parle,
Mumbai 400056, India

Manali Trivedi
Dept. of Computer Engineering,
Dwarkadas J. Sanghvi College
of Engineering, Vile Parle,
Mumbai 400056, India

Lakshmi Kurup
Assistant Professor, Dept. of
Computer Engineering,
Dwarkadas J. Sanghvi College
of Engineering, Vile Parle,
Mumbai 400056, India

ABSTRACT
In this paper the usage of Semantic Web techniques to secure Internet based Mobile Ad-hoc Networks (iMANETs) has been proposed. Ontologies will be used instead of Taxonomies to depict network security issues. These ontologies can be placed in the knowledge base of an Intrusion Detection System (IDS). Using inference over the semantic relations will help Intrusion Detection Systems recognize and add future attacks to its existing knowledge base.

Keywords
Intrusion Detection, Semantic Web, Ontology, Ad-Hoc Networks, Security, Attacks, Web Ontology Language, Protégé, OWL.

1. INTRODUCTION
Mobile Ad-hoc Networks are flexible networks consisting of mobile nodes connected by wireless links. These networks were originally used in military projects such as Defense Advanced Research Projects Agency (DARPA) projects. MANETs form a challenging yet interesting topic for research due to their flexibility and lack of rigid top-down administration.

Nodes in such networks are free to move independently forming new links and breaking existing links. These networks may be self-contained or have some nodes connected to the larger Internet. Networks in which at least one of the nodes is connected to the Internet are called as Internet Mobile Ad-hoc Networks (iMANETs). Although such networks are incredibly useful they face a number of problems such as processing power constraints, signal protection, reliability, limited range constraints, etc. Moreover, these networks must be secured against standard attacks on ad-hoc routing protocols as well as the attacks on the Internet connection.

Intrusion Detection Systems (IDS) are used to monitor network traffic and send alerts to system administrators if any malicious activity is detected. An Intrusion Detection System (IDS) consists of an audit data processor (sensor), a central knowledge base, decision engine, alarm generation and responses [1]. The sensor detects intrusions and contains decision making mechanisms regarding intrusions [2].The central knowledge base of an IDS is used to characterize and classify an attack or intrusion. In this paper optimizing the knowledge base of an Intrusion Detection System (IDS) by replacing taxonomies by ontologies to characterize attacks is the main focus.

Ontologies are better than taxonomies as they can be used to infer new relations and are not restricted to a particular domain. Also, ontologies include machine understandable definitions of concepts and hence allow systems to analyze the information better. Ontologies enable knowledge sharing and reuse between the knowledge database and the IDS sensors. We take advantage of the benefits of using ontologies by classifying the iMANET system according to attacks, payload, attack targets, broadcast approaches, vulnerabilities and attackers. This classification will be generated by using an ontology representation language OWL (Web Ontology Language). Protégé software will be used for implementation.

The goal of this paper is to use an ontology to define a conceptual model for the knowledge base in an Intrusion detection system. This conceptual model can be used to infer future relationships and allow intrusion detection systems to prevent future attacks in Internet Mobile Ad-hoc Networks.

The paper is structured as follows. Section 2 describes existing research that has been carried out in ontology based Intrusion Detection Systems. The vulnerabilities of iMANET system are discussed in section 3. In section 4 we describe the various attacks in Internet Mobile Ad-hoc Networks. Broadcasting approaches in iMANET are discussed in section 5. Ontologies and knowledge bases are discussed in section 6. In section 7 OWL language used to represent the proposed ontology is described. In section 8 we describe and represent the proposed ontology. The conclusions and future research will be discussed in section 9. References of this paper are stated in section 10.

2. RELATED WORK
While some papers have proposed using ontologies in Intrusion Detection systems, almost none of them have focused on applying the concept to Internet Mobile Ad-hoc Networks (iMANET).

Raskin [3] introduced and suggested using ontologies in information security. They reasoned that ontologies can organize terminology and nomenclature efficiently. They advocated using knowledge of the information security community to classify attacks.

Pinkston [4] and Undercoffer [5] suggested using ontologies instead of taxonomies to classify attacks. They defined a target centric model to model attacks in DAML (DARPA Agent Markup Language). In the model the class ‘intrusion’ consisted of the components: means of attack, system component most often targeted, consequence of attack, and location of attack.

Similarly, Salahi [6] proposed using ontologies to model network attacks. CAPEC, CWE, CVE datasets were used to evaluate their ontology based system. Their proposed method showed significant improvements over traditional relational models and reduced false alarms.

Hseih [7] used ontologies in a patrol detection system. Their proposed system has lower energy consumption than traditional Intrusion Detection Systems (IDS) and requires less memory. Relationships are created between sensor nodes which have pre-loaded knowledge. This knowledge is used to detect future anomalies.

3. IMANET VULNERABILITIES

3.1 Dynamic Topologies

The vulnerabilities of Internet based Mobile Ad-hoc Networks are the same as Mobile Ad-hoc Networks. In iMANETs, nodes can join and leave the network independently. This dynamic nature leads to frequent path breaks.

3.2 Wireless Link Characteristics

These links suffer from problems like fading, path loss, blockage, etc.

3.3 Lack of Centralized Management

There is no centralized node to monitor traffic and record information about nodes.

3.4 Limited Range of Wireless Transmission

Due to its dynamic nature bandwidth usage in an Internet based Mobile Ad-hoc network must be done judiciously.

3.5 Packet Loss

The loss of packets is high in iMANET due to issues like hidden terminal problem, collisions, interference, etc. [8]

3.6 Frequent Network Partitions

The network may be partitioned into sections due to the movement of nodes. This can affect intermediate nodes adversely as they might receive less power supply.

3.7 Cooperativeness

All routing protocols assume that nodes provide secure communication. However, some nodes may become malicious nodes which disrupt the network operation by changing routing information. [9]

3.8 Enemy within the Network

Due to its dynamic nature and lack of centralized management it is very difficult to detect a malicious node within an iMANET network.

3.9 Limited Power Supply Constraint

There may not be enough power supply for all nodes and some nodes may try to behave selfishly.

4. ATTACKS IN IMANET

The attacks on an Internet based Mobile Ad-hoc Network can be classified on the basis of data or packet alteration in a network into active and passive attacks. In a passive attack the attacker pries into the data exchanged in the network without explicitly changing it. As the operation of a network is not altered this attack is difficult to detect. Passive attacks are used to gather information about a network and may lead to an active attack. In an active attack the attacker attempts to alter the data being exchanged in the network. An attacker can modify, drop, and insert new packets into the network. The attacks can also be classified according to the location of the attacker nodes. External attacks occur when attacker nodes do not belong to the domain of the network. Internal attacks are carried out by internal nodes that have become malicious.

Humans, system or other issues can be grouped under the attackers the network. Humans could be seasoned hackers, a hostile user or a clueless user. The attack may be intentional or accidental. Discovering and recording the techniques used by attackers is essential for securing the network against similar attacks in the future.

4.1 Passive Attacks

4.1.1 Snooping or Eavesdropping

In these attacks the attacker attempts to obtain confidential information that is not meant for it. This information could be public key, private key, or location of the nodes.

4.1.2 Traffic Analysis

The attacker monitors the Internet Mobile Ad-hoc network to gain information about the communication between nodes. It tries to find out which nodes communicate more frequently.

4.1.3 Traffic Monitoring

This attack is used to identify the communication parties and functionality which could provide information to launch further attacks.

4.2 Active Attacks

4.2.1 Dropping Attacks

Malicious nodes can drop all packets that are not meant for them. If such a node is located at a critical point all communication may be hampered.

4.2.2 Modification Attacks

These attacks modify packets and disrupt communication between network nodes.

4.2.3 Fabrication Attacks

In this attack the attacker sends fake messages to the neighboring nodes. It can also send a fake route reply message in response to a legitimate route request message.

4.2.4 Timing Attacks

The attacker fools neighboring nodes by advertising closeness to them.

4.3 OSI Protocol Stack based Active Attacks

4.3.1 Application Layer Attacks

The application layer contains the user data and software. The protocols supported here are HTTP, SMTP, TELNET, and FTP. The attacks at this layer are Malicious Code, and Repudiation. Malicious Codes consist of viruses, worms, spywares, and Trojan horses. Repudiation attacks make data appear to be invalid. These attacks are easy to accomplish as outbound data is not checked for validity.

4.3.2 Transport Layer Attacks

There are two attacks at this layer: Session Hijacking, and SYN Flooding attack. In Session Hijacking an attacker tries to exploit an unprotected session after initial setup. The attacker first obtains the sender node's IP address and then launches Denial of Service (DoS) attacks against the receiver. Hijacking a connectionless transport protocol such as User Datagram Protocol (UDP) is easier than connection oriented protocols. In SYN Flooding the attacker opens as many TCP

sessions as possible. Ping of Death and Buffer Overflow attack are subcategories of these attacks. During the ping of death attack a number of Internet Control Message Protocols (ICMP) are sent. Buffer Overflow attack attempts to put more data into the buffer than it can handle.

4.3.3 Network Layer Attacks

This layer has the most number of attacks. They are further classified as:

4.3.3.1 Blackhole Attack

A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. [10]

4.3.3.2 Tunneling Attack

Tunneling attack is also called wormhole attack. In a tunneling attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers. [11]

4.3.3.3 Sinkhole Attack

A malicious node tries to attract all data to itself from surrounding nodes. It can hence receive all the network traffic and can modify all the secure data.

4.3.3.4 Link Withholding Attack

In this attack the malicious node does not share information about the links it is aware of in the network. Thus, in case of changes in the network some of the nodes may not find out about new links.

4.3.3.5 Link Spoofing Attack

In these attacks the malicious node broadcasts incorrect route information to disrupt routing information.

4.3.3.6 Replay Attack

An attacker that performs a replay attack retransmits the valid data repeatedly into the network. This attack can adversely affect new or weak routes. [12]

4.3.3.7 Sybil Attack

In this attack the attacker creates a new identity or steals an identity of a legitimate node. Thus it may become difficult to identify a misbehaving node. This attack can prevent fair resource allocation among the nodes in the network.

4.3.3.8 Byzantine Attack

In this attack a malicious node or set of nodes work together to attack the system. Routing loops are created and packets may be dropped or forwarded through non-optimal paths.

4.3.3.9 Resource Consumption Attack

This attack is also called Sleep Deprivation attack. An attacker attempts to consume more power by requesting new routes frequently or forwarding unnecessary packets into the routes.

4.3.4 Data Link Layer Attacks

These attacks are subdivided into Selfish Misbehavior, and Malicious Behavior. In a Selfish Misbehavior attack the attacker node may refuse to take part in forwarding packets in order to conserve power or bandwidth. The node may also deliberately drop packets to conserve resources. Such nodes behave maliciously by disrupting the normal operations of a network. The malicious node operations can be categorized into the following types: Denial of Service (DoS), attacks on network integrity, misdirecting traffic, attacking neighbor sensing protocols.

4.3.5 Physical Layer Attacks

Jamming and Active Interference are examples of physical layer attacks. In a Jamming attack a malicious node determines the frequency of communication. It then transmits signals as well as security threats. In Active Interference a communication channel is blocked or communication is distorted. Old packets may be reintroduced to create confusion.

5. BROADCASTING APPROACHES IN IMANET

The broadcasting approaches in iMANET can be classified as [13]:

5.1 Unicasting

A message is sent from a source to a single destination. If messages have to be sent to multiple devices then multiple unicast messages will be sent along with the receiver device information.

5.2 Multicasting

A message is sent from a source to a number of destinations. The Internet Group Management Protocol (IGMP) is used by this approach to identify group members. Nodes can belong to multiple multicast groups.

5.3 Broadcasting

A source node floods all the remaining nodes in a specified network. The message will be sent to all the devices which have a special broadcast address.

5.4 Geocasting

In this approach a message is sent from a source to all nodes inside a geographical region.

6. ONTOLOGIES AND KNOWLEDGE BASES

In Greek the word ontology means ' a description of what exists'. Despite its numerous definitions, in this paper an ontology denotes a formal organization of entities and their relationships. In the context of computing applications ontologies are schemas for metadata. Terms and relationships in an ontology can be defined, organized, and processed. This semantic portrayal allows a clear and concise description of a domain of knowledge. A knowledge base is an ontology with a set of the instances of the different kinds of entities it specifies. Thus an ontology will denote the general conceptual structure necessary to describe the domain, while the knowledge base will contain individual instances that are described by the ontology.

Using ontologies instead of controlled vocabulary has its advantages. First, is the ability of ontologies to combine information from different categories. For example we can correlate which network vulnerability was exploited to cause which attack. Thus, having information about how terms relate to one another is needed instead a controlled vocabulary of terms.

Other advantages of ontologies are: no unique name assumption, open world assumption, and efficient inference by ontology axioms. No unique name assumption means that entities may have more than one name. In addition, missing

information is treated as unknown and not false. These advantages of ontologies make them a powerful choice when not enough information is available, or the schema is large and complex. In the case of Internet based Mobile Ad-Hoc networks both these conditions are true, and thus a domain centric ontology is a good option.

7. WEB ONTOLOGY LANGUAGE (OWL)

The Web Ontology Language (OWL) is a family of language proposed by the World Wide Web Consortium (W3C) which enables us to not only explicitly define and express information, but also process its content. The basic design of OWL is based on DAML+OIL. It is a semantic markup language which has three species: OWL Lite, OWL DL, and OWL Full. The expressiveness of each of these species increases in order. OWL can define plenty of concepts which include partitions, and class documentation. Attributes can be defined by specifying their domain in order to distinguish between class and its instances. Attribute properties, taxonomies, and axioms are also constructed by OWL.

OWL Lite uses only the basic classifications and simple constraints like 0 and 1. OWL Lite is the least expressive but most of the elements of OWL DL are constructed using complex combinations of OWL Lite constructs. OWL DL will is said to be "computationally complete" and gives a guarantee that a conclusion is computable. In OWL DL, the DL stands for Description Logics, which is a very advanced formal knowledge representation language. OWL Full is the most expressive out of all three and includes features of OWL Lite, and OWL DL. Although since expressiveness increases with OWL Full, reasoning support is less predictable. [14]

A class in OWL can be defined using the owl:class tag. In order to specify a subclass which has inherited its parent class, we use the tag rdfs:subClassOf. As for defining attributes, it can be done in two ways, first using owl:DatatypeProperty for literal values and owl:ObjectProperty for references to class instances. Another unusual aspect of OWL is that a property cannot directly belong to a particular class and it has to be associated to a class by specifying its domain using the rdfs:domain tag. [15, 16]

8. PROPOSED ONTOLOGY

The taxonomy proposed by Hansman et al. [17] is used for as a starting point to build the proposed attacks ontology. Their proposed taxonomy consists of four dimensions: attack vector, attack target, vulnerabilities, and payloads. In our proposed ontology we add two additional dimensions broadcasting approach, and attacker information. By using these two dimensions further information about a malicious node and its preferred method of sending out malicious packets can be incorporated. OWL is used to describe the ontology. Protégé software will be used to model the ontology. [18] Using OWL is preferable as it is more machine readable than Resource Description Framework Schema (RDFS). [19]

The proposed ontology consists of six main classes: Attackers, Payload, AttackTargets, Attacks, Vulnerabilities, and BroadcastApproaches. Each of these classes is subdivided into subclasses as given in their descriptions above. Thing is a super class in the given ontology, and the entire model hierarchy can be traversed to get more detailed information the classes.

Following code should be used to make classes and subclasses using OWL. The file should be saved with an .owl extension. Figure 1 illustrates the code snippet that was used to make the classes and subclasses of the proposed ontology.

```
<rdf:RDF

    <!-- OWL namespace-->
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:owl="http://www.w3.org/2002/07/owl#"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#">

   <!-- OWL Class Definition Example-->
   <owl:Class rdf:about="#Vulnerabilities"/>
   <owl:Class rdf:about="#BroadcastApproaches"/>
   <owl:Class rdf:about="#Attacks"/>
   <owl:Class rdf:about="#AttackTargets"/>
   <owl:Class rdf:about="#Payload"/>
   <owl:Class rdf:about="#Attackers"/>

    <!-- OWL Subclass Definition Example-->
   <owl:Class rdf:about="#PassiveAttacks">
   <rdfs:subClassOf rdf:resource="#Attacks"/>
   </owl:Class>

</rdf:RDF>
```

Figure 1: Code snippet to make the Classes and Subclasses using OWL

Figure 2 illustrates the first level of the proposed ontology. The six main classes of ontology are Vulnerabilities, BroadcastApproaches, Attacks, AttackTargets, Payload, and Attackers. In Figure 3, we have further expanded the Attacks class from level one. The layer attacks under active attacks are further expanded in Figure 4. While expanding the Attack class four unique levels are obtained. The levels may increase in the future and can be easily incorporated in the knowledge base. The conceptual model of the proposed ontology is depicted in Figure 5. All the classes and subclasses have not been expanded in order to make the image less congested. This figure depicts how detailed the ontology of this system can be. Conventional databases are not powerful enough to store such detailed information along with the relations between them. Another advantage of this conceptual model is the use of simple linguistic variables which give adequate details for novice users.

9. CONCLUSION AND FUTURE WORK

In this paper an ontology for an Internet based Mobile Ad-hoc Network (iMANET) has been proposed and created. Web Ontology Language (OWL) has been used to describe the schema. Protégé software has been used to model the schema. By creating an ontology the use of semantic web techniques to give rich descriptions of schema has been depicted. This concept can be extended to other machine interpretable formats with Web Markup Languages, or Web Ontology Languages such as XML, DAML, and OIL after appropriate refinement. A further extension is also possible in emerging fields of wireless technology like Bluetooth, and Wireless Sensor Networks (WSN). Moreover, new classes such as Time, Motive, and System Component can be added to the ontology. The class Time can record the timestamp of an attack. Whereas the System Component class can store can store the components of the system which were attacked by the attacker. The Motive class can be subdivided according to various motives of an attacker. Some attackers are driven by

curiosity, fame, or maliciousness. Adding such class can enable the administrator to understand attackers and their nature better. We are continuing our research and plan on integrating this ontology with the SPARQL-DL query engine [20] and the OWL API. [21] Testing the proposed ontology against attacks such as the Mitnick Attack is the next step in our research. [22]

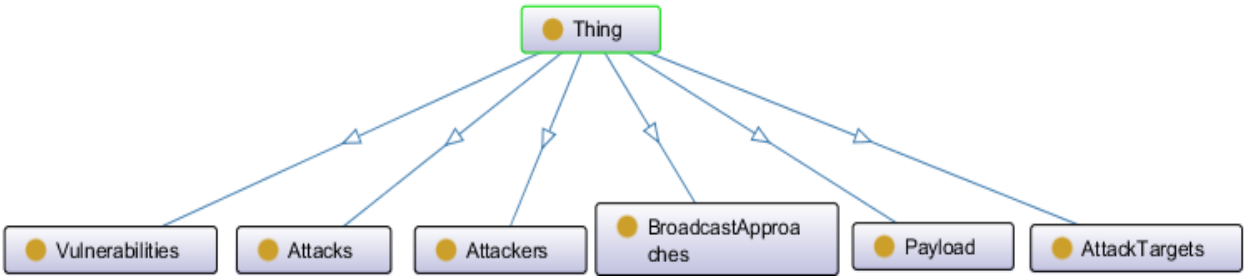

Figure 2: First level of the proposed ontology hierarchy

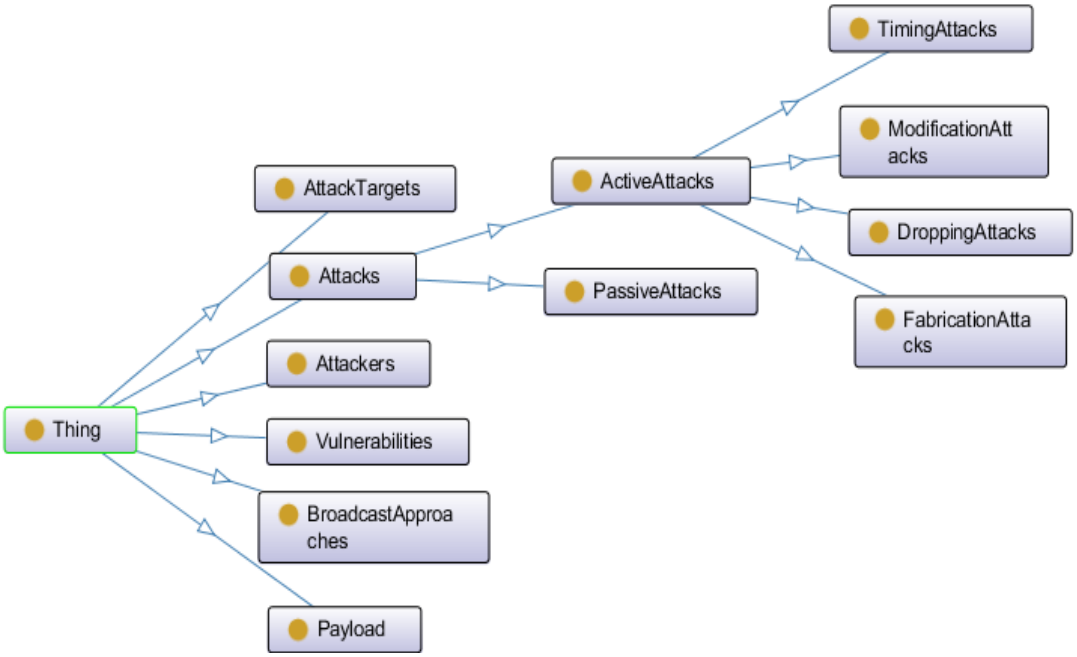

Figure 3: First, second, and third levels of the proposed ontology

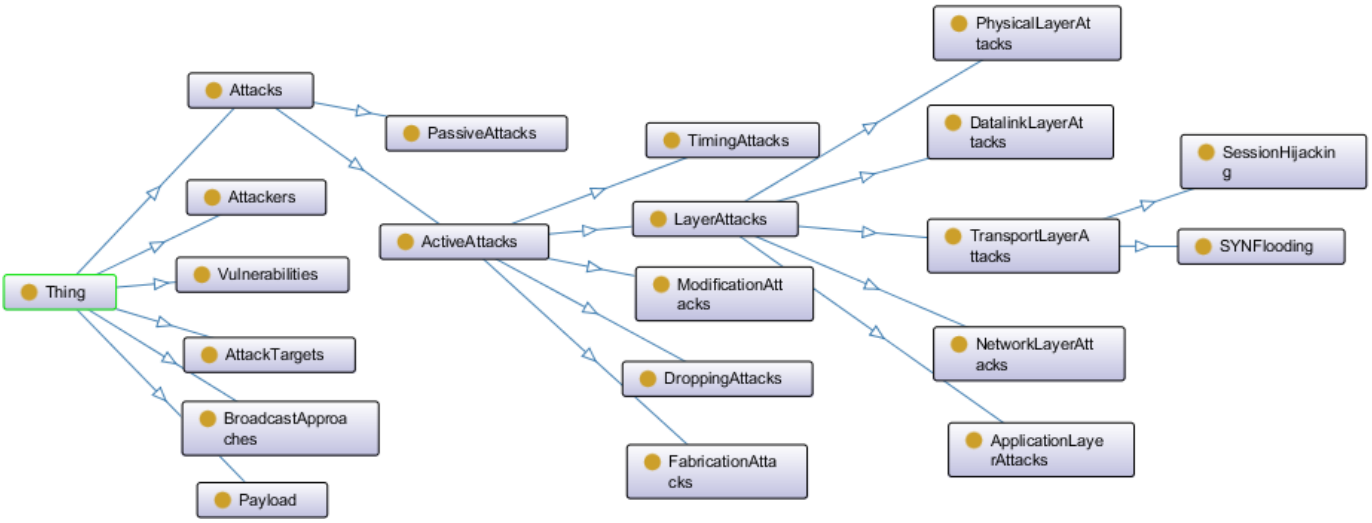

Figure 4: Subclasses of the Attacks class

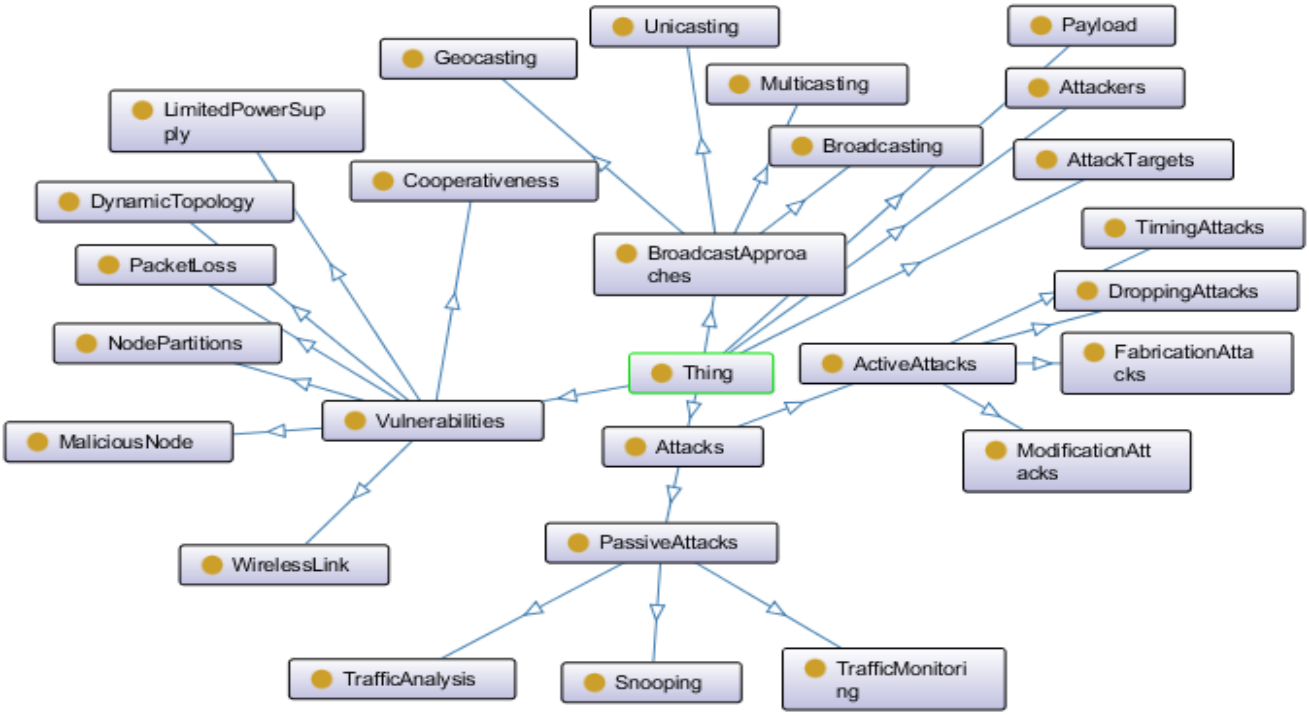

Figure 5: Conceptual model of the proposed ontology for an Internet based Mobile Ad-Hoc network (iMANET)

10. REFERENCES

[1] S. Stolfo, 'Intrusion Detection Systems', 2006.

[2] P. Kazienko, 'Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture)', WindowSecurity, 2003.

[3] V. Raskin, C. Hempelmann, K. Triezenberg and S. Nirenburg, 'Ontology in information security: a useful theoretical foundation and methodological tool', pp. 53--59, 2001.

[4] J. Pinkston, J. Undercoffer, A. Joshi and T. Finin, 'A target-centric ontology for intrusion detection', University of Maryland, Baltimore County Department of Computer Science and Electrical Engineering, 2003.

[5] J. Undercoffer, A. Joshi, J. Pinkston, "Modeling Computer Attacks: An Ontology for Intrusion Detection" August 2003

[6] A. Salahi and M. Ansarinia, 'Predicting Network Attacks Using Ontology-Driven Inference', arXiv preprint arXiv:1304.0913, 2013.

[7] Hsieh, C., Chen, R. and Huang, Y. (2014). Applying an ontology to a patrol intrusion detection system for wireless sensor networks. International Journal of Distributed Sensor Networks, 2014.

[8] A. Jayasuriya, S. Perreau, A. Dadej and S. Gordon, 'Hidden vs exposed terminal problem in ad hoc networks', 2004.

[9] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[10] Jhaveri, R., Patel, A., Parmar, J. and Shah, B. (2010).MANET Routing Protocols and Wormhole Attack against AODV. International Journal of Computer Science and Network Security, [online] 10(4), pp.12-17.

[11] Hu, J. and Burmester, M. (2004). Network-layer Security of Mobile Adhoc Networks. Florida State University.

[12] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[13] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks".

[14] G. Antoniou and F. Van Harmelen, 'Web ontology language: Owl', Springer, pp. 67--92, 2004.

[15] W3.org, 'OWL Web Ontology Language Overview', 2014. [Online]. Available:http://www.w3.org/TR/2004/REC-owl-features-20040210/#s2.1.

[16] De Vergara, J., Villagra, V. and Berrocal, J. (2004). Applying the Web ontology language to management information definitions. IEEE Communications Magazine, 42(7), pp.68-74

[17] Simon H, Ray," A taxonomy of network and computer attacks, "Elsevier, Computers & Security (2005) 24, 31e43.

[18] Protege.stanford.edu, 'protégé', 2014. [Online]. Available: http://protege.stanford.edu/.

[19] W3.org, 'RDF Schema 1.1', 2014. [Online]. Available: http://www.w3.org/TR/2014/PER-rdf-schema-20140109/.

[20] Derivo.de, (2015). SPARQL-DL API – derive GmbH. [online] Available at: http://www.derivo.de/en/resources/sparql-dl-api.html [Accessed 29 Dec. 2014].

[21] Owlapi.sourceforge.net, (2015). OWL API. [online] Available at: http://owlapi.sourceforge.net/ [Accessed 29 Dec. 2014].

[22] Shahriari, H., Makarem, M., Sirjani, M.,Jalili, R. and Movaghar, A. (2010). Vulnerability analysis of networks to detect multiphase attacks using the actor based language Rebeca. Computers and Electrical Engineering, 36(5), pp. 874-885.