An Ontological View of Trusted OLSR Protocol of Ad hoc Network

Amandeep Verma
Punjabi University Regional Centre for IT & Management, Mohali, India

Manpreet Singh Gujral
University College of Engineering, Punjabi University, Patiala, India

ABSTRACT
Ad hoc network infrastructure is dynamically changing, and the links are wireless with less capacity and more prone to errors. Adding trust to the existing security infrastructures would enhance the security of these environments. Describing components and their sub-components using ontologies, creates a methodology and mechanism in order to efficiently design. With a viewpoint to add trust as a component in traditional OLSR routing protocol to enhance the security of ad hoc network and to present the modified structure in an efficient way, ontological engineering approach was used. This paper presents the ontological view of trusted OLSR protocol where knowledge and information are structured on classes and concepts.

Keywords
Ad hoc Networks, OLSR, Ontology, Trust

1. INTRODUCTION

The network infrastructure is dynamically changing, and the links are wireless with less capacity and more prone to errors. Adding trust to the existing security infrastructures would enhance the security of these environments.

Today, ontologies are finding their way into a wide variety of applications. Ontology defines a common vocabulary for researchers who need to share information in a domain. It includes machine-interpretable definitions of basic concepts in the domain and relations among them. Developing ontology is akin to defining a set of data and their structure for other programs to use. Each ontology O contains a set of concepts (classes) C and a set of properties P. The OWL, which is recommended by W3C3, is used to describe the trust ontology. Protégé [8] is a free, open source ontology editor and knowledge-base framework; developed by the Stanford Medical Informatics group (SMI) at Stanford University.

This paper presents the ontological view of trusted OLSR routing protocol for ad hoc network. The OLSR protocol uses trust component in decision making about routing. The paper is intended for the researchers having interest in the usage of trust for security purposes for ad hoc networks. The paper is organized as follows. The section II presents the review of literature. The section III gives the ontological representation of the protocol under study. The section IV concludes the paper.

2. REVIEW OF LITERATURE

An exhaustive review of the effect and worthiness of trust in ad hoc networks was presented in the study [6]. There are number of routing protocols for ad hoc network, the OLSR protocol was selected on the basis of the results of the study [7].

The usages of ontologies in ad hoc networks were quoted by following studies. The modeling of the necessary application knowledge [1] in using contexts for addressing and routing in mobile ad hoc networks is done as ontologies in OWL. An ontology based dynamic updates in sparse mobile ad hoc networks [5] for rescue scenarios was presented. The construction of security ontology was proposed [3] according to the features of WSN to represents the formal semantics for intrusion detection. Ontology of MANET attributes [2] including device security and performance characteristics can be leveraged to efficiently and effectively make dynamic configuration decisions for managing a MANET was shown.

The ontology generates a level of abstraction that largely characterizes a model and the dependencies of activities [4] and consequently being valuable for system to interact and helpful in the development process.

3. THE ONTOLOGY

A. The Concepts

The main class hierarchy, consisting six concepts involved in the trust oriented OLSR ontology and the brief description about each class is given in Table 1. Thing is abstract super-class for all classes.

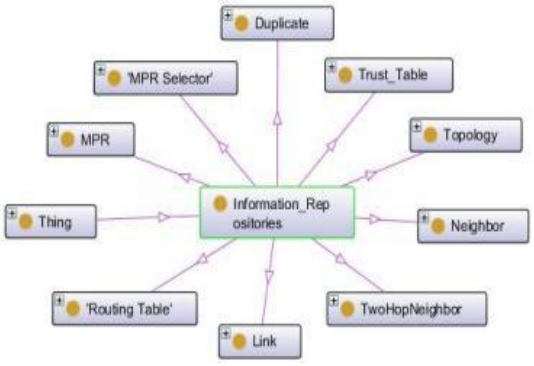

Figure 1: Concepts in Information Repositories

TABLE 1
MAIN CONCEPTS OF OLSR ONTOLOGY

Concepts	Description
Node	This is the basic representation of a machine i.e. represented by identity
Object	This is the basic entity in the ad hoc network
Attributes	It is about the various attributes of the objects
Information Repositories	This is to represent the information repositories of the object used by it for the operation of the ad hoc network
Packet	The description of the Packet in such type of network.
Operations	The operations performed while in operation

The various subclasses under Information_Repositories are shown in the Figure 1. These are the classes used to keep the information required by the node for their operation in the network. Some of these repositories are used for routing, route selection and others used to avoid duplicate receipt of packets and some of them to disseminate the topology information to the other nodes in the network.

The Attributes class with components representing attributes of the node is depicted in Figure 2. The attributes power, type, trust and willingness are there. The Neighbor in the Figure 3 is used to store the information about the direct neighbors of node. The neighbors address, trust in that neighbor and the willingness of the neighbor to participate are the components of this class.

The Twohop Neighbors with the address of two hop neighbour, the trust on that neighbor, The address of the neighbour via this is twohop , and the time till this twohop is valid are the main components of this class shown in Figure 4. The MPR is Multi Point Relay used by the neighbor for routing purposes with its address and the trust on it is shown in Figure 5. A node has number of MPRs and a MPR selected for forwarding as per the route table entry for the desired destination.

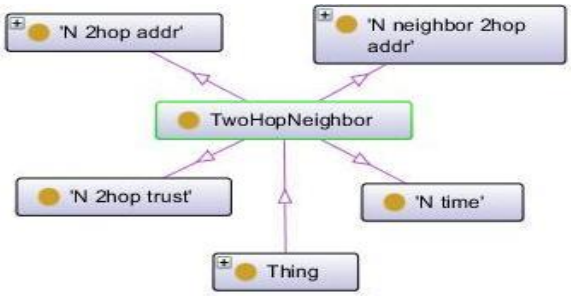

Figure 2: Concepts in Attributes

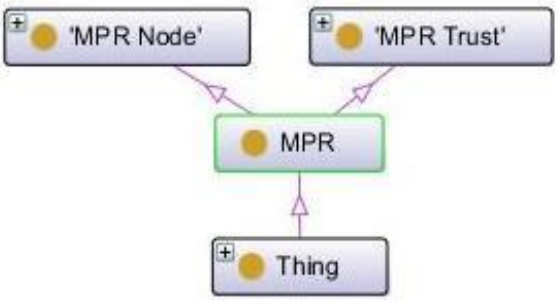

Figure 3: Structure of Neighbor

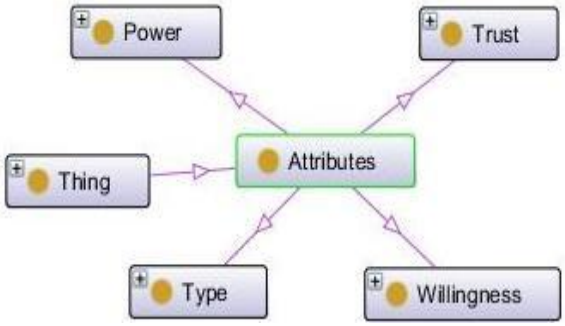

Figure 4: Structure of TwohopNeighbor

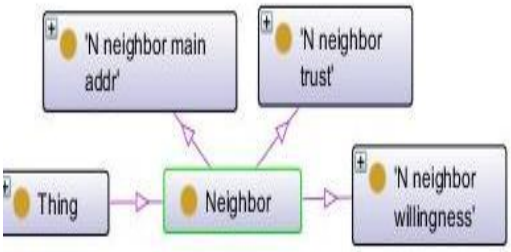

Figure 5 Composition of MPR

The MPR Selector is the nodes address with its validity selects the holding node as its MPR presented in Figure 6. The MS main addr gives the address of the node that selects this object as one of its MPR. The Duplicate class is used to avoid the reprocessing of packets that are already processed is shown in Figure 7. The address of the sender node its sequence number and the retransmitted state are the components of this class. The retransmitted state is true or false depending on whether the packet is retransmitted or not.

In order to keep the topology information at any stage the Topology concept holds the required attributes or components is shown in Figure 8. The T_last_addr is the address that is to be reached to reach at T_dest_addr. The Link Class to store the information about the links with the trust value on that link is shown in Figure 9

The Trust Table is additional component in the present study which is not in traditional OLSR have the information about the trust of the source node on the other nodes is shown in Figure 10. The Routing Table class having the information used for routing of the network with the address of the destination, its distance in terms of hop from the source node and the address of the next node to which packet is to routed is shown in Figure 11.

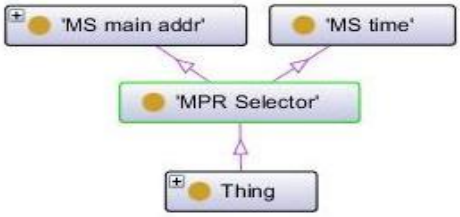

Figure 6: Composition of MPR Selector

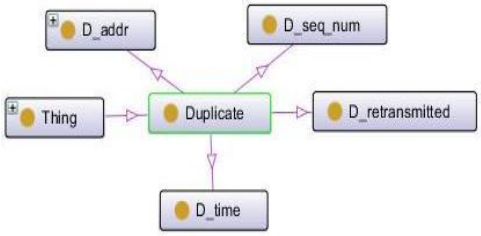

Figure 7: The Duplicate Class

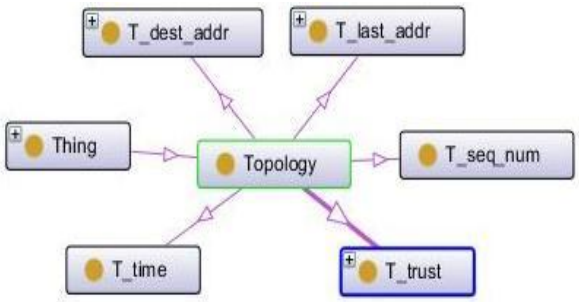

Figure 8: Topology Class and its components

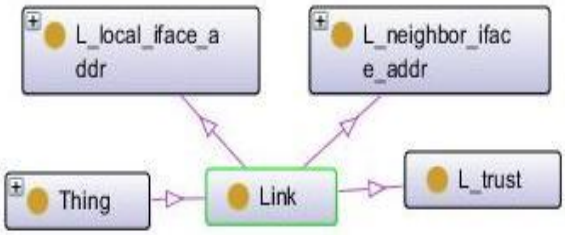

Figure 9: The Link Class

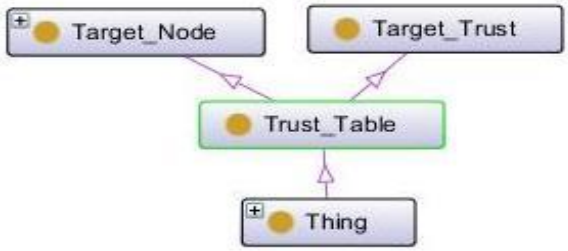

Figure 10: Trust Table Class

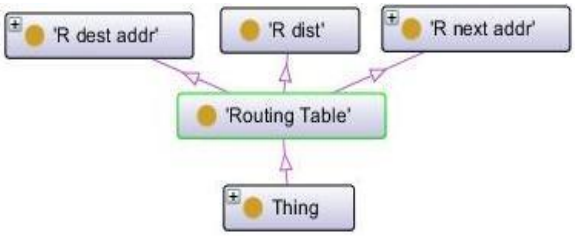

Figure 11: The Routing Table Ontology

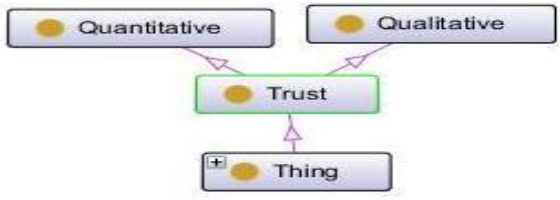

Figure 12: The Trust Class

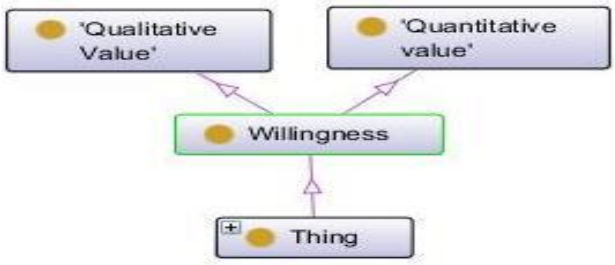

Figure 13: The Willingness Class

The trust class with the choices of having either Qualitative or Quantitative value is shown in Figure 12. The same choices are also available for the willingness class shown in Figure 13.

In adhoc network all nodes are represented by an instance of the Object class as per OLSR protocol, is shown in Figure 14. Battery is used to show the status of Battery at a given instant. The Type is used to identify the type of node for current operation. The possible values of it are – Source, destination or Intermediate.

The possible operations while a node is in an operating environment are shown in Figure 15. The trust component is introduced in most of the operations for processing. In addition to the traditional operation, the trust message gets introduced to request and reply of the trust about a node.

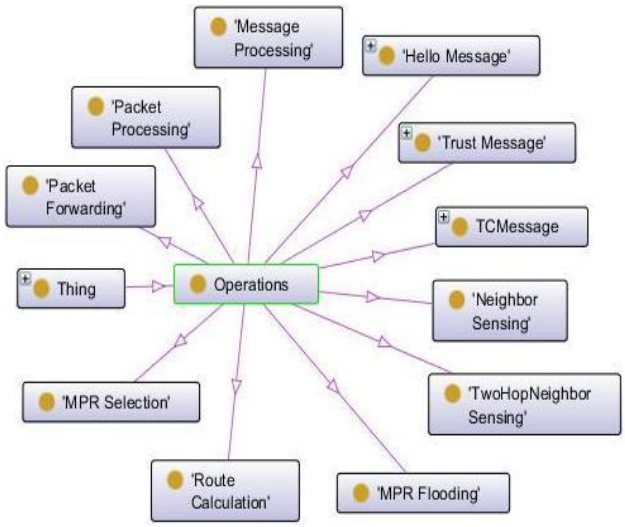

Figure 14: The Object Class

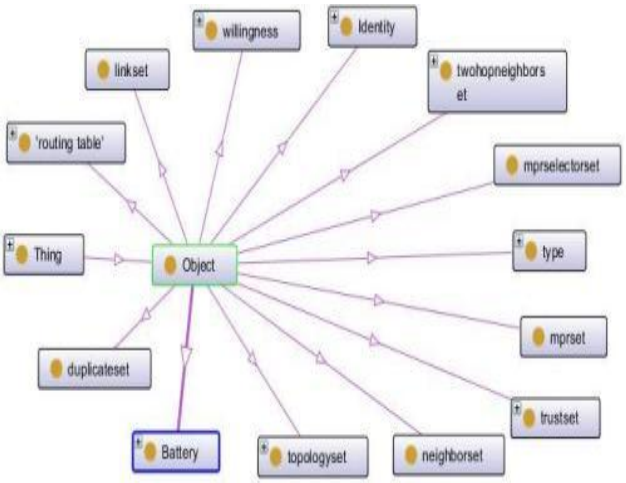

Figure 15: The Operations class Hierarchy

The classes described have restriction on their objects. Most of the object values are restricted by universal quantification as the objects of these classes have well defined possible types for their values.

The Properties

The hasNeighbor object property has three sub properties shown in Table 2. The properties are for the subclasses of the Neighbor class – N_neighbor_main_addr, N_neighbor_trust and N_neighbor_willingness respectively.

The has2hopNeighbor object Property has three sub properties for the sub classes of TwohopNeighbor Class – N_2hop_addr, N_2hop_trust and N-neighbor_2hop_addr shown in Table 3.

TABLE 2
HASNEIGHBOR OBJECT PROPERTY OF OLSR ONTOLOGY

Sub Property	**Description**
hasNeighborAddress	This is the functional property that Neighbor's address to the identity of node
hasNeighborTrust	The property mapping neighbor trust to an instance of Trust
hasNeighborWillingness	This is the mapping from neighbors willingness to an instance of the class Willingness

TABLE 3
HAS2HOPNEIGHBOR OBJECT PROPERTY OF OLSR ONTOLOGY

Sub Property	Description
has2hopAddr	This maps the address of the 2 hop neighbor to its identity.
has2hopTrust	It is the mapping of the trust in 2 hop neighbor to an instance of the Trust class
hasNeighbor2hopAddr	This is to map the address of the direct neighbor through which designated 2 hop neighbor is connected to source, to its identity.

TABLE 4
SOME DATA PROPERTIES OF OLSR ONTOLOGY

Property	Description
Is retransmitted	This is a Boolean for D_retranmitted of Duplicate
hasNodeIdentity	It is to int form Node class
hasIdentityvalue	It is to an int value from Identity of Node
hasMaxvalue	It is to int value indicating Maximum permissible value of
hasMinValue	It is to int value indicating Minimum permissible value of
hasMaxWillingness	It is to int value indicating Maximum permissible value
hasMinWillingness	It is to int value indicating Minimum permissible value

The Table 4 gives the description of some of the data properties with the names of the Domain class and data type as range for these properties.

4. CONCLUSION

The idea of the ontology is to accomplish, to describe and to denote the comprehension of similar fields for providing a widespread understanding of the fields to present an apparent characterization of the terminology and the shared relations among the terminologies from the diverse perspectives. The suggested ontology is going to be used as a component, providing inherent features of ad hoc networks in building a trust oriented security framework for adhoc to capture the essence of ad hoc networks.

5. REFERENCES

[1] Eigner Robert and Mair Christoph, "Using Context Ontologies for Addressing and Routing in Mobile Ad Hoc Networks", Proceedings of Eighth International Conference on Networks, pp. 415-420, 2009

[2] Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine, "An Ontological Approach to Secure MANET Management", Proceedings of International Conference on Availability, Reliability and Security, pp. 787-794, 2008

[3] Mao Yuxin, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", Proceedings of 6th International Conference on Networked Computing, pp. 1-5, 2010

[4] Nair V and Dutta A, "Ontology based Session Management Protocol for Teleteaching Domain", Proceedings of the 2nd International Conference on Computer and Automation Engineering", Vol. 5, pp. 866-870, 2010

[5] Sanderson N, Goebel V and Munthe-Kaas E, "Ontology Based Dynamic Updates in Sparse Mobile Ad-hoc Networks for Rescue Scenarios", Proceedings of 7th International Conference on Mobile Data Management, pp. 70, 2006

[6] Verma Amandeep and Gujral M S, "Impact of Trust Usage in Routing, Authentication and Access Control of Adhoc Network", International Journal of Advance in Communication Engineering, Vol. 2, No. 2, pp. 1-7,Jan – June 2009

[7] Verma Amandeep and Gujral M S , "Performance Analysis of Routing Protocols for Ad hoc Networks", International Journal of Computer Science and Emerging Technologies, Vol. 2, No. 4, August 2011, pp. 484 – 487.

[8] http://protege.stanford.edu/download/download.html