DOI: https://doi.org/10.61841/ghfn8p51 **Publication URL: http://nnpub.org/index.php/MS/article/view/556**

SECURE AND EFFICIENT GRAPH DERIVATION REPRESENTATION APPROACH FOR MEASURING AND DISTRIBUTING CLUSTER BASED ONTOLOGY

R. *Suganya*[1]*, *Ms. A. Divya*[2]
*[1,2]*Ifet College Of Engineering, Villupuram*

Corresponding Author: -

Abstract: -

Secure data transmission for cluster-based measuring and comparing ontologies, where the clusters are formed dynamically and occasionally. We intend two sheltered and resourceful records Transmission (SET) protocols for CWSNs, is SET-IBS and SET-IBOOS, through by means of the IdentityBased digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme in that order.

During SET-IBS, protection relies on the rigidity of the DiffieHellman problem in the pairing domain. SET-IBOOS further reduces the computaional overhead for present a graph derivation representation-based approach (GDR) for stable semantic quantity, which captures structural semantics of ontologies, which is while its serving relies on the hardness of the discrete logarithm problem. The calculations and simlations are provided to illustrate the efficiency of the new protocols. The domino effect illustrates to, the future protocols have better performance than the existing secure protocols for measuring and comparing ontologies, in terms of security overhead and energy consumption.

Index terms: *Ontology, Ontology reuse, Ontology measure, SET-IBS, SET-IBOOS, Graph*

I.

1.INTRODUCTION

Ontologies have been widely applied in many fields such as knowledge management [1]–[3], Semantic Web [4], information integration [5]–[7], and semantic exploration [8]–[10], etc. A recognized improvement of ontologies is that they supply a acquaintance-allocation infrastructure that chains the depiction and allotment of realm awareness by formalizing significance of pleased and in sequence. As the dimension and the quantity of ontologies prolong to enlarge [11], the salvage and the constant capacity of ontologies proffer numerous imperative reimbursement. First, the attempt of constructing innovative ontologies can be drastically abridged by reusing obtainable ontologies as an alternative of preliminary from graze [12]–[14]. An additional benefit of ontology reuse is its latent to extensively ease the records interoperability in assorted information systems by sharing a common ontology[15]–[20].Ontology mapping is a relatively mature area of research used for aligning two or more ontologies (information sources) for the purpose of sharing information and overcoming heterogeneity issues [1,2,4–8]. The terms mapping and matching are often used interchangeably. However, matching is considered to be a prerequisite of mapping
[1]. determining semantic relatedness between two entities. On the other hand, mapping is the process of finding the data transformation based on the semantic relatedness for a given instance of a source entity that will produce an instance of a target entity [8,9].

1.1. Idea

Ontology can be defined as the Explicit Specification of conceptualization. In other words, we can define Ontology as an abstract view of set of concepts and their relationships. It gives the semantic structure of any concept related to the specific domain. In todays internet world, information retrieval is one of ontology the important things. For appropriate information retrieval, knowledge representation and knowledge management must be done accurately. For this purpose can be used eficiently. Ontologies are domain specific and give the complete idea about the particular domain correctly.In the concept of information retrieval, user should get accurate domain-specific information relevant to the query given. Hence to represent the domain, ontologies are used. It is the graphical view of domain. It gives the design of concepts which are semantically related to each other.

1.2. Motivation

Construction of ontology plays an important role in retrieval process. But ontology construction is very tedious and cumbersome job. To construct an ontology various algorithm can be used, e.g. Graph Derivation Based Approach. To avoid the problem of ontology construction the concept of Ontology Reuse is evolved. This means that the existing ontology of relevant concept can be taken into consideration. Also according to the users need some modifications can be done in generating new ontology which makes the retrieval process faster. the On-toKnowledge project to build an ontology-based tool suite that efficiently processses the many assorted, scattered and semistructured credentials normally found in intranets.

1.3 Formal Definition

The following formal definition is adapted from Medche. An ontology configuration O is defined as

$$O = \{C, R, AO\},$$

Where:

1. C is a set whose elements are called concepts.
2. $R \subseteq C \times C$ is a set whose elements are called relations. For $r = (c\ c) \in R\ 1\ 2$, , one may write $1\ 2\ r(c) = c$.
3. AO is a set of axioms on O.

To cope with the lexical level, the notion of a lexicon is introduced. For an ontology structure $O = \{C, R, AO\}$ a lexicon L is defined as $L = \{LC, LR, F, G\}$,

Where:

1. LC is a set whose elements are called lexical entries for concepts.
2. LR is a set whose elements are called lexical entries for relations.
3. $F \subseteq LC \times C$ is a reference for concepts such that

F(l) {c C l c F} C C = ∈ : (,)∈ for all C
C l ∈ L ,F c {l L (l c) F} C,C −1 ( ) = ∈ : , ∈ for all c∈C . 4. G ⊆ LR × R ,s a reference for relations such that G(l) {r R l r G} R R = ∈ : (,)∈ for all R, R l ∈ L , G r {l L G} R,R, R −1( ) = ∈ : , ∈ for all.

It is noted that this definition allows for a lexical entry to refer to several concepts or relations (homonymy) and for one concept or relation to be referred to by several lexical entries (synonymy). Furthermore, Maedche (2003) includes a concept hierarchy H C ⊆ C ×C to express the inherent hierarchical structure of concepts. It is felt that this is disused, particularly in illumination of the current conversation, since a hierarchical structure can be explicitly defined in terms of R.

2.RELATED WORKS

2.1 Measuring and Distributing ontologies

The distributed ontologies are assumed to be OWL DL ontologies. Some terminologies are as follows: A name is a URI (literal is not discussed for cleanness). The glossary of an ontology is the locate of names that occur in the ontology as individuals, classes and properties, except for built-ins. We use Σ to denote a set of ontologies {Oi | i∈I}, here I be a set of indexes. V(Oi) denotes thevocabulary of Oi, while VI(Oi), VC(Oi) and VP(Oi) denote the individual,

class, and property vocabulary of Oi, respectively. The terminology of Σ, denote by V(Σ), is the amalgamation of the vocabulary of ontologies within Σ, more formally, V(Σ)={ν | ν∈V(Oi),Oi∈Σ}. And VI(Σ), VC(Σ) and VP(Σ) denote the individual, class, and property vocabulary of Σ, respectively. We assume that VI(Σ), VC(Σ) and VP(Σ) are pairwise disjointed..An ontology measure is an indicator that is used to reflect some quality properties of ontologies.

2.2 Graphical Ontology Representation

The Visual Notation for OWL Ontologies (VOWL) defines a visual language for the user-oriented representation of ontologies. It provide graphical depiction for rudiments of the Web Ontology Language (OWL) that are combined to a forcedirected graph layout visualizing the ontology.This requirement focus on the apparition of the ontology schema (i.e. the classes, properties and datatypes, occasionally called TBox), while it also include recommendation on how to portray folks and data values (the ABox).

3.DEFINITION AND NOTATION

3.1 Ontology Language

OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting in sequence to human. OWL facilitate superior appliance interpretability of Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a official semantics. OWL has three ever more-communicative sub language: OWL Lite, OWL DL, and OWL Full. This article is printed for readers who want a first impression of the capability of OWL. It provide an prologue to OWL by unofficially describing the features of each of the sub language of OWL. A few information of RDF Schema is functional for sympathetic this deed, but not essential.

Example 1. TBox={1.Researcher People, 2.Researcher ≡ ssor PhD, 3.Prof_with_PhD ≡ Professor ∗ PhD, 4.PhDStudent Student, 5.Student ≡ ∃ register.Dept ∗ ∃take.Course, 6.PhDStudent ∀advisedBy.Professor, 7.Researcher ScientificPersonnel, 8. Prof_with_PhD Researcher, 9. ScientificPersonnel Researcher}. ABox={10.register(John, CS), 11.take(John, Java), 12.Dept (CS), 13.Course (Java)}.

3.2 Stable Ontology Measurement and Preprocessing

An ontology can be regarded as a set of triples of the form (s,p,o). The structural descriptionof an ontology O is the set of explicitly represented triples in O. The semanticdescription of O is the set that contains not only the structurally described triples, butalso all implicit triples obtained by reasoning O. Communication that an ontology with the similar semantic explanation possibly has multiple structural descriptions (including O).

Definition 1. Let Sem(O) be the semantic account of an ontology O. Sem(O) has the manifold structural imagery, denote Stru(O)=fO, O1, ¢ ¢ ¢, Ong. A stable ontology measurement M is mapping, M : Stru(O) ! R such that M(O) =M(O1) = ¢ ¢ ¢ =M(On), where R is a nonempty locate of actual figures. We summarize the preprocessing for stable ontology measurement from [5].

1) Naming all anonymous classes and all anonymous individuals. We can automatically detect the related labels and name anonymous classes. Anonymous individuals can be detected and named by class membership. The set of named concepts of Ontology O is denoted CO = fC1; ¢ ¢ ¢ ;Cng, where each Ci is unique, and is either an atomic concept or a named anonymous concept.

2) Eliminating cycles of concept subsumption such as A v A1, ¢ ¢ ¢, An v A, where A, Ai(1 · i · n) are concepts. Previously we identify such a cycle view of sub asumption an ontology, we replace all cyclic concept subsumption axioms with B v Ai (1 · i · n), where B is a new concept name for each cycle.

Definition 2. 8C;D 2 CO, C is directly subsumed by D, i.e., directly-subsumed by (C;D), iff 8C;D 2 CO(C v D ^ :9C0 2 CO(C0 v D ^ C v C0)).

Definition 3. 8C 2 CO, the axiom fanouts of C are denoted AFC = fD1; ¢ ¢ ¢ ;Dmg, where for each Di(1 · i · m · jCOj), directlysubsumed-by(Di;C) holds, and jCOj represents the cardinality of CO.In the following, we simply analyze the correction of the preprocessing. On one hand, as mention over, for an ontology O, its semantic description Sem(O) containsnot only the structural description of O, but also the implicitly expressed knowledge derivative from O. This resources that, for any saw or allegation ® in O, O implies ® iff Sem(O) implies ®. On the other hand, the preprocessing for stable ontology measurementis terminable because stride 1,2,3 will be finished if thereis no multifaceted notion, cycle of awareness subsumption, and unenriched concept in O.

3.3 Graph Derivation Representation

Graphs were initially defined to represent conceptual schemas used in database systems but after that they had a wide range of applications in artificial aptitude, mainframe knowledge, and cognitive science. A basic conceptual graph is composed of two kinds of nodes, i.e., concept nodes representing entities and relation nodes representing relationships between these entities. In [3], some specific graphical methods based on conceptual graphs are defined and described, such as the basic conceptual graphs and the simple conceptual graphs methods. Multilayered extended semantic networks Multilayered Extended Semantic Networks is defined as a formalism for the semantic representation of natural language expressions which can be used as a universal knowledge representation paradigm in human sciences [4].

Definition 1the set of inference labels: {→In/n ∈ Z} ∪ {→Em/m ∈ Z}, • F-Labels is the set of formula labels: {→i /i ∈ N} and the propositional letters {p,q,r,...}, • E-Labels is the set of edge labels: {l (left), r (right), conc (final conclusion), hyp (hypothesis)} ∪ {pj (premise)/ j ∈ Z} ∪ {mj (minor premise)/ j ∈ Z} ∪ {Mj (major premise)/ j ∈ Z} ∪ {cj (conclusion)/ j ∈ Z} ∪ {discj (discharge)/ j ∈ Z}, • D-Labels is the set of delimiter labels: {Hk/k ∈ Z} ∪ {C}.

Definition 2. A graph G is a directed graph hV, E, L, lV , lEi where: V is a set of nodes, E is a set of edges, L is a set of labels, hv ∈ V, t ∈ L, v0 ∈ Vi, where v is the source and v0 the target, lV is a labeling function from V to R∪F-Labels, lE is a labeling function from E to E-Labels.

3.4 Ontology Representation

In the most common sense of the term, a graph is an orderedpair G = (V, E)comprisinga set V of vertices or nodes to gether with a set E of edges or lines, which are 2-element subsets of V (i.e., an edge is related with two vertices, and the qualified is symbolize as an unordered pair of the vertices with respect to the particular edge). A vertex may exist in a graph and not belong to an edge.V and E are usually taken to be restricted, and most of the eminent results are not true (or are rather different) for infinite graphs because many of the arguments fail in the infinite case. The order of a graph is $|V|$ (the number of vertices). A graph's size is $|E|$, the number of edges.

4.GENERATING GDR'S OVERVIEW

4.1 Node

A Node is a drop of knowledge (term, entity) different from any other knowledge in the model. All concepts which have their own meaning are in nodes. Thus nodes can represent particular named citizens, equipment, trial, procedures, thoughts, but also concepts on a higher level of abstraction, such as a person, a table, a sporting event, learning, a feeling, activities etc. A node is the smallest unit of knowledge which cannot be further divided. Larger units of knowledge are represented by a group of connected nodes. Also, nodes are not groups (relations, tables, classes) of similar entities.

4.2 Links

The second basic concept is link, which has the role of connecting a maximum of two nodes in the network. Links do not have link names, but can have role names. Role name (as described below) is the information belonging to the node, and this name questions the role of the connection between that node and one more node. A link is represented by a procession, with or devoid of an arrow. A link cannot connect three or more nodes. Only binary links are allowed. If there is a need to connect three or more nodes then "process nodes", which connect several nodes by dual links, can be introduce. The cardinality of a link is always (1,1): (1,1) [12].

4.3. Example for Generating GDR of Ontology

According to the procedure described , we can traverse each of axioms and assertions in the example ontology, and generate its corresponding description of structural semantics with GDR. Then, they are included for behavior, and form a complete and semantically constant GDR.The other measures consider the excavation of implicit semantic information reside in ontologies, and the absolute semantic in sequence of ontologies.

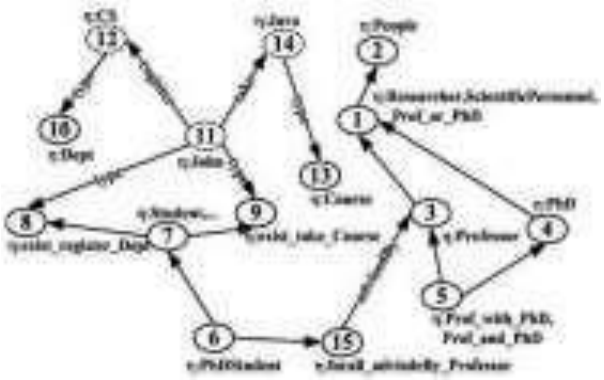


Fig 1.GDR of Example 1

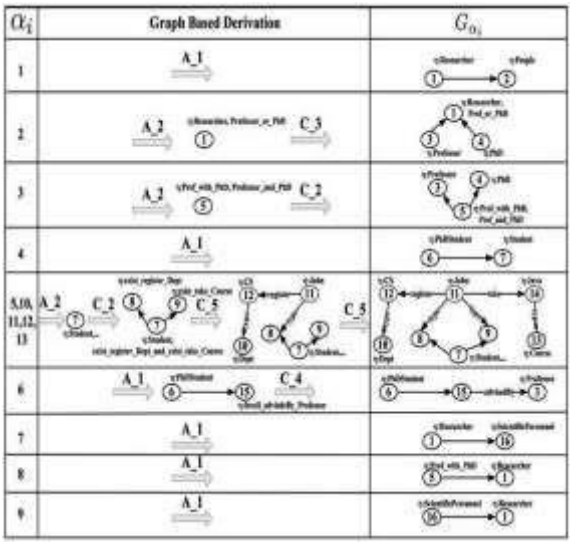


Fig. 2. Generating GDRs for each axiom/assertion in Example 1

5.STRUCTURAL SEMANTICS OF ONTOLOGY

5.1 Structural Semantics of Axioms in GDR

OWL DL has some differences from standard Description Logics. These differences provide a bridge between the formal Description Logic world and the Semantic Web world. OWL uses URI references as names, and constructs these URI references in the same manner as that used by RDF. It is thus common in OWL to use qualified names as shorthand's for URI references, using, for example, the qualified name owl:Thing for the URI reference http://www.w3.org/2002/07/owl#Thing.OWL gathers information into ontologies, which are generally stored as Web documents written in RDF/XML. Ontologies can import other ontologies, adding the information from the imported ontology to the current ontology.OWL allows RDF annotation properties to be used to attach information to classes, properties, and ontologies, such as owl:DeprecatedClass.

5.2 Structural Semantics Concept of Ontology

A formal semantics, very similar to the semantics provided for Description Logics (see Section ??), is provided for this style of with OWL. Full particulars on this representation theory can be create in the OWL Semantics and Abstract Syntax [Patel-Schneider et al., 2004.Because OWL includes datatypes, the semantics for OWL is very similar to that of Description Logics that also incorporate datatypes, in particular SHOQ(D). However, the meticulous datatypes worn in OWL are full from RDF and XML Schema Datatypes [Biron and Malhotra, 2001]. Data values such as xsd:integer thus mean what they would mean as XML Schema data values.

In DL, a complex concept can be con-structed by the following ways, e.g, $C * D$, $C \sqcup D$, $\forall R.C$ $\exists R.C$, $\exists R.\{a\}$, $\{a1, a2, \ldots, an\}$, $\geq nR.C$ and $\leq nR.C$. lists the structural semantics of GDRs of different type of complex concepts in DL. Obviously, mapping a complex concept onto a vertex of GDR is a recursive process.It is worth noting that in Table 2 we need to normalize the naming of vertices when complex concepts are mapped onto vertices because complex concepts have no specific names unlike atomic concepts. An atomic concept X can be mapped onto a vertex i with the literal name X. We assign the literal names of complex concepts in terms of the semantic meanings based on which they are defined. For examples, the vertex name of the complex concept $\forall R.C$ is named as forall_R_C. The vertex of the complex concept $C1 * C2$ has the name C1 _and_C2 .

5.3 Syntax and Semantics of Ontologies

The description of ontologies and knowledge in description logics uses constructs that have semantics given in predicate sense. However, due to chronological reasons, poles apart memo is used, that is closer to semantic networks and frame-based systems. Let us have a look at theAL (attribute language) logic that is a minimal logic with a practically usable vocabulary. In the table below there is the syntax and semantics of the AL logic including a short comment. In the table as well as in the following description A and B are atomic concepts, Cand D are concept descriptions, and R is atomic role. The semantics is defined using interpretation I that consists of non-empty set Δ^I (the domain of interpretation) and an interpretation function, which assigns a set $A^I \subseteq \Delta^I$ to every atomic concept A and that assigns a binary relation $R^I \subseteq \Delta^I \times \Delta^I$ to every atomic role R. The interpretation function is then extended by inductive definitions summarized in the table below. Two concepts C and D are equivalent, written $C \equiv D$, if $C^I = D^I$ for all interpretations I.

TABLE 1
AL(attributive language)logic syntax and semantics

Syntax	Semantics	Comment
A	$A^{\mathcal{I}} \subseteq \Delta^{\mathcal{I}}$	atomic concept
R	$R^{\mathcal{I}} \subseteq \Delta^{\mathcal{I}} \times \Delta^{\mathcal{I}}$	atomic role
$\top$	$\Delta^{\mathcal{I}}$	top (most general) concept
$\bot$	$\emptyset$	bottom (most specific) concept
$\neg A$	$\Delta^{\mathcal{I}} \setminus A^{\mathcal{I}}$	atomic negation
$C \sqcap D$	$C^{\mathcal{I}} \cap D^{\mathcal{I}}$	intersection
$\forall R.C$	$\{a \in \Delta^{\mathcal{I}} \mid \forall b.(a,b) \in R^{\mathcal{I}} \Rightarrow b \in C^{\mathcal{I}}\}$	value restriction
$\exists R.\top$	$\{a \in \Delta^{\mathcal{I}} \mid \exists b.(a,b) \in R^{\mathcal{I}}\}$	limited existential quantification

The AL logic can be further extended by adding new constructs, see table above for examples. The name of the logic is then formed from the string AL[U][E][N][C], so for example the logic ALEN is the attributive language logic extended with full existential quantification and number restrictions.

6.MODULES OF GDR

6.1 SET Protocol

In this module, Secure and Efficient data Transmission (SET) protocol for ontologies. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with elevated efficiency. The projected SET-IBOOS operate equally to the preceding SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then portray the key administration of the protocol by using the IBOOS scheme, and the protocol operation afterwards. Secure communication in SET-IBS relies on the ID based cryptography, in which, user public keys are their ID in sequence.

6.1.1. Initialization of SET-IBS Protocol.

Setup phase: In the code of behavior initialization the Base Station generates a master key msk and public parameter param for the generation of private key and sends them all to the sensor nodes.

Extraction process: Node j first obtains its private key as from msk and where is its IDj , and is the time stamp of node j's time interval in the current round that is generated by its CH i from the TDMA control. Signature signing: The sensor node j picks a random number and computes. The sensor node further computes

$$cj = h(Cj \mid tj \mid \theta j$$
$$\sigma j = cj\ sekj + \alpha j$$

Where the digital signature of node j on the encrypted messageCj. The broadcast message is now concatenated in the form.

Verification: Upon in receipt of the communication, every sensor node verifies the authenticity in the following way. It check the time stamp of present time interval tj and determines whether the received communication is bright. Then, if the time stamp is correct, the sensor node further computes θj , $= e\ \sigma j, P\ e(H(IDj \mid tj\ , -Ppub\ )\ cj$ using the time stamp of current time interval .

6.1.2. Initialization of SET-IBOOS Protocol.

Setup phase: In the etiquette initialization the Base Station generates a master key msk and public parameter param for the generation of private key and sends them all to the sensor nodes.

Extraction process: Before the autograph process, node j first extract the classified key from the msk τ and its identity ID, as

where

$$Rj = grj$$
$$sj = rj + H\ Rj\ ,\ IDj\ \tau mod\ q.$$

Offline signing: At the offline stage, node j generates the offline value $< \sigma\ j >$ with the time stamp of its time slot tj for program, and store the acquaintance for sign online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, for example, the CH sensor node. Let then

$$gsj = grj\ gH\ Rj\ ,IDj\ \tau mod\ q = Rj\ XH\ Rj\ ,IDj\ mod\ q$$
$$\sigma\ j = g - tj$$

Online signing: At this stage, node j computes the online signature based on the encrypted data Cj and the offline signature$\sigma\ j\ .hj = H(Cj\ ,\ IDj\ )$

$$zj = \sigma\ j + hj\ sj\ mod\ q \quad \sigma j = g\sigma\ j$$

Then, node j send the memorandum to its target withtj ,Rj and the online signature, in the form ofIDj , tj , R, σj , zj , cj .

Verification process:. Then, if the time crush is acceptable the sensor node further computes the values of gzj and $\sigma j\ Rj\ hj\ Xhj$

$H\ Rj\ ,IDj\ mod\ q$,. If the values of and $\sigma j\ Rj\ hj\ Xhj\ H\ Rj\ ,IDj\ mod\ q$, are equal from the customary meaning, the node i considers the received message authentic, accepts it, and propagates the message to the next hop or user.

6.1.3 Enhanced Secure Data transmission Protsocol:

In the proposed system, an innovative technique in introduced which is called Enhanced Secure Data Transmission protocol (ESDT) which is used to improve the SET-IBS and SETIBOOS protocol. In the improved SETIBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity.

6.1.4. Protocol Features

The protocol characteristics and hierarchical clustering solutions are presented in this section. We first summarize the features of the proposed SET-IBS and SET-IBOOS protocols as follows: Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete IDbased settings, which use ID information and digital signature for authentication... Comparing the SET-IBS, SET-IBOOS requires less energy for totaling and luggage compartment. Moreover, the SET-IBOOS is more apposite for node-to-node communications in CWSNs, since the computation is lighter to be executed. In SET-IBOOS, the offline signature is executed by the CH sensor nodes; thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing.

6.2 Key Management For Security

Security is based on the DLP in the multiplicative assembly. The equivalent private coupling parameter are preloaded in the sensor nodes through the protocol initialization. The IBOOS method in the projected SET-IBOOS consists of following four operation, taking out, offline sign, online signing and verifications.

6.2.1. Key Management

The solution cryptographies used in the etiquette to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

6.2.2. Neighborhood Authentication

This module used for secure access and data transmission to nearby sensor nodes via authenticating with every extra. Here, “limited” means the chance of neighborhood confirmation, where only the nodes with the common pairwise key can validate each other

6.2.3. Storage Cost

In this module, represent the obligation of the security keys stored in sensor node’s memory.

6.2.4. Network Scalability

It indicates whether a security protocol is able to scale without compromising the security necessities. Here, “comparative low” means that, compare with Ontologies and Gdr, in the secure data transmission with a symmetric key supervision, the better network scale augments the supplementary orphan nodes emerge in the network.

6.2.5. Communication Overhead

The security will be overhead in the data packets during communication. two classes of GDR treatments to poly-morphism of ontology representation for automatic and reliable measurement and comparison of the structural semantics of ontologies.

6.2.6. Ontologis Resilience

The types of attacks that security protocol can protect against. A distributed attack requires that the adversary bring in code, such as a Trojan horse or reverse-door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution.

6.2.7. Protocol Characteristics

- **Key management**: the enter cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric keybased security.
- **Neighborhood authentication**: used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, “limited” means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.
- **Storage cost:** represent the requirement of the security keys stored in sensor node’s memory.
- **Network scalability**. indicates whether a security protocol is able to scale without compromising the security requirements. Here, “comparatively low” means that, compare with SET-IBS and SET-IBOOS, in the secure data

transmission with a symmetric key management, the better net scale increase the more orphan nodes emerge in the system and vice versa**.**

- **Communication overhead:** the security overhead in the data packets during communication. » Computational overhead. the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.
- **Attack resilience**: the type of attack that security protocol can protect against.

7. ALGORITHM OF GDR

7.1 Clustering Algorithm

Clustering can be considered the most important unsupervised knowledge difficulty so, as every other problem of this sort, it deals with finding a structure in a collection of unlabeled data.A slack definition of clustering could be "the procedure of organize objects into groups whose members are similar in a number of way".A cluster is therefore a compilation of substance which are "similar" between them and are "dissimilar" to the objects belonging to other clusters.

The algorithm is collected of the following steps:

Begin with the displace clustering having level L(0) = 0 and sequence number m = 0.

- Find the least dissimilar pair of clusters in the current clustering, say pair (r), (s), according to d[(r),(s)]=mind[(i),(j)] where the smallest amount is over all pair of clusters in the current clustering.
- Increment the sequence number: m = m +1. Merge clusters (r) and (s) into a single cluster to form the next cluster m. Set the stage of this clustering to

$$L(m) = d[(r),(s)]$$

- Update the proximity matrix, D, by deleting the rows and column equivalent to clusters (r) and (s) and adding a row and column corresponding to the newly shaped cluster. The nearness amid the new cluster, denoted (r,s) and old cluster (k) is defined in thisway:

$$d[(k), (r,s)] = \min d[(k),(r)], d[(k),(s)]$$

- If all substance are in one cluster, stop. Else, go to step 2.

However, semantic measurement neglects the polymorphism of ontology representation, which inevitably cause the trouble, i.e., multiple graphs perhaps live for representing the same ontologies. Reliable ontology measurement is the precondition on which the meaningful and useful ontology comparison and evaluation can be made .

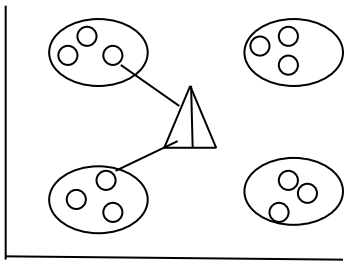


Fig 3. Form group fo cluster

8.ONTOLOGY MEASUREMENT

8.1Classification of Measurement Entities

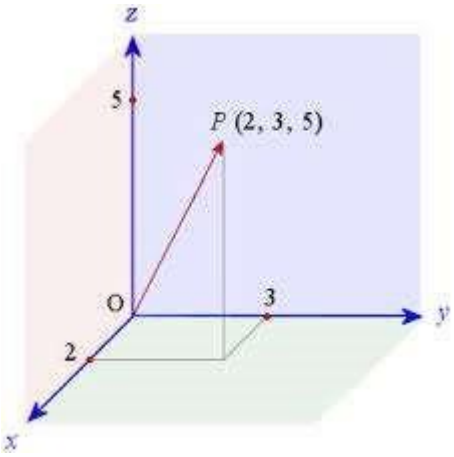
Although various ontology measures have been proposed in the previous decade, the types of dimension entity can be generally classified into two classes of entity types in terms of granularity: Fine-grained measurement thing types and coarse-grained measurement entity types. We dispute that most of the accessible ontology trial should be uti- lized to measure the semantic structures of ontologies in the form of their GDRs.

9.Distance Metrices of Ontology

A common approach to measuring similarity between two graphs is to solve the problem of graph isomorphism, subgraph isomorphism and maximal widespread sub- graphs [48]–[50]. In this paper, we employ the graph isomorphism of GDRs described in Definition 8 to measure the similarity between two ontologies by computing the distance between their GDRs using a distance based met- ric, such as the one in [48]. Let mcs(GO1 , GO2) denote the maximal common subgraph of the two GDRs, GO1 and GO2 .Let |GO | denote sthe number of vertices of a graph GO (i.e.,|VO |). The distance metric between GO1 and GO2 , denoted by d(GO1 ,
GO2).The experimental evaluations for ontology comparison are made based on the following considerations.

- If the distance similarity between two ontologies is zero (i.e., 0.000), then they represent the same semantic knowledge in the identical domain. For exam- ple, the GDRs of example 1 and 2 have the pairwise distance resemblance of value 0.000, which indicate that they symbolize the same semantic knowledge in the same domain.

9.1. Graphs and Result



A three-dimensional graph is the graph of a function f(x, y) of two variables, or the graph of a association g(x,y, z) amongst three variables provide that x, y, and z or f(x, y) are real numbers, the graph can be represent as a planar or curvedsurface in a threedimensional Cartesian coordinate system. A three-dimensional graph is classically strained on a two-dimensional page or screen using perspective methods, so that one of the dimensions.when compared to existing system we are going to enhance that and add length of the message or security key combine to the range of message and length of message.

9.2Applications of UML for Ontology Representation

A variety of different research projects and commercial initiatives have been applying UML for ontology representation. This section briefly describes these efforts. The approaches taken in these efforts vary in a number of different ways including:

- UML has been used directly as an ontology representation and as a graphical front-end for another ontology representation language (e.g., DAML+OIL12 - referred to as DAML in the rest of this paper).
- UML has been used with a variety of agent infrastructures and knowledge base implementations (e.g.,Java objects and the Open Knowledge Base Connectivity13 (OKBC) API).

10. Conclusion

Theoretical anal- ysis of the property of GDR, we illustrate that the GDR of an ontology is semantic-preserving and "unique" in stipulations of labels, linking organization and isomorphism, which guar- antees stable semantic ontology measurement. We scrutinize and appraise the utility of our GDR

approach and com- pare our GDR with conventional graph models (GM). We draw two important conclusions. Successful data transmission and security can be achieved by using CWSN's. The inadequacy symmetric key management for secure data transmission has been addressed. In previous method, consist of two efficient protocol called SET-IBS and SET-IBOOS protocol.

REFERENCES

[1].Yinglong Ma, Ling Liu, *Senior Member, IEEE,*Ke Lu, Beihong Jin, and Xiangjie Liu **“** A Graph Derivation based approach for and comparing structural semantics of ontologies” VOL. 26, NO. 5, MAY 2014

[2].M. d’Aquin and N. F. Noy, “Where to publish and find ontologies? A survey of ontology libraries,” *J. Web Semant.*, vol. 11, no. 8,pp. 96–111, 2012.

[3].Z. Khan and M. Keet, “ONSET: Automated foundational ontology selection and explanation,” in *Proc. 18th Int. Conf. EKAW*, Galway City, Ireland, 2012, pp. 237–251.

[4].A. M. Khattak, Z. Pervez, K. Latif, and S. Lee, “Time efficient reconciliation of mappings in dynamic web ontologies,” *Knowl. Based Syst.*, vol35,. no. 11, pp. 369–374, 2012.

[5].D. Sanchez, M. Batet, D. Isern, and A. Valls, “Ontology-based semantic similarity: A new feature-based approach,” *Expert Syst. Applicat.*, vol. 39, no. 9, pp. 7718–7728, 2012.

[6].F. Ensan and W. Du. “A semantic metrics suite for evaluating modular ontologies,” *Inform. Syst.*, vol. 38, no. 5, pp. 745–770, 2013

[7].L. Razmerita, “An ontology-based framework for modeling userbehavior-A case study in knowledge management,” *IEEE Trans.Syst., Man, Cybern. A, Syst., Humans*, vol. 41, no. 4, pp. 772–783, Jul. 2011.

[8].J. Park, S. Oh, and J. Ahn, “Ontology selection ranking model for knowledge reuse,” *Expert Syst. Applicat.*, vol. 38, no. 10, pp. 5133–5144, 2011.

[9].H. Zhang, Y.-F. Li, and H. B. K. Tan, “Measuring design complexity of semantic web ontologies,” *J. Syst. Softw.*, vol. 83, no. 5, pp. 803–814, 2010.

[10]. R. Kontchakov, F. Wolter, and M. Zakharyaschev, "Logicbased ontology comparison and module extraction, with an application to DL-Lite," *Artif. Intell.*, vol. 174, no. 15, pp. 1093– 1141, 2010.
[11]. Y. Ma, B. Jin, and Y. Feng. "Semantic oriented ontology cohesion metrics for ontology-based systems," *J. Syst. Softw.*, vol. 83, no. 1,pp. 143–152, 2010.
[12]. Y. Ma, "Towards stable semantic ontology measurement," in *Proc. ISWC*, 2010, pp. 21–24
[13]. Z. Zou, J. Li, H. Gao, and S. Zhang, "Mining frequent subgraph patterns from uncertain graph data," *IEEE Trans. Knowl. Data Eng.*,vol. 22, no. 9, pp. 1203–1218, Sept. 2010.
[14]. M. Mao, Y. Peng, and M. Spring, "An adaptive ontology mappingapproach with neural network based constraint satisfaction,"*J. Web Semantics*, vol. 8, no. 1, pp. 14–25, 2010.
[15]. J. Li, J. Tang, Y. Li, and Q. Luo, "RiMOM: A dynamic multistrategy ontology alignment framework," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 8, pp. 1218–1232, Aug. 2009.
[16]. H. Zhuge, "Communities and emerging semantics in semanticlink network: Discovery and learning," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 6, pp. 785–799, Jun. 2009.
[17]. B. Motik, B. C. Grau, I. Horrocks, and U. Sattler, "Representing ontologies using description logics, description graphs, and rules," *Artif. Intell.*, vol. 173, no. 14, pp. 1275–1309, 2009.
[18]. S. Rudolph, M. Krotzsch, and P. Hitzler, "Description logic reasoning with decision diagrams: Compiling SHIQ to disjunctive datalog," in *Proc. ISWC*, 2008, pp. 435–450
[19]. A. Burton-Jones, V. C. Storey, V. Sugumaran, and P. Ahluwalia,"A semiotic metrics suite for assessing the quality of ontologies,"*Data Knowl. Eng.*, vol. 55, no. 1, pp. 84–102, 2009.
[20]. H. Stuckenschmidt, "A semantic similarity measure for ontologybased information," in *Proc. 8th Int. Conf. FQAS*, Roskilde,Denmark, 2009, pp. 406–417.
[21]. M. Popescu, J. M. Keller, and J. A. Mitchell, "Fuzzy measures on the gene ontology for gene product similarity," *IEEE/ACM Trans. Comput. Bio. and Bioinfo.*, vol. 3, no. 3, pp. 263–274, Jul./Sept. 2009.
[22]. H. Al-Mubaid and H. Nguyen, "Measuring semantic similarity between biomedical concepts within multiple ontologies," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 39, no. 4, pp. 389–398Jul. 2009.
[23]. D. Fensel, "Ontology-based knowledge management," *IEEE Comput.*, vol. 35, no. 11, pp. 56–59, Nov. 2008.
[24]. L. Chen, N. R. Shadbolt, and C. A. Goble, "A semantic webbased approach to knowledge management for grid applications," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 2, pp. 283–296, Feb. 2008.

SNAPSHOTS