Ontological Engineering Approach Towards Network Security Situational Awareness

Pardeep Bhandari
Doaba College, Jalandhar, Punjab — 144001, India
bhandaridcj@gmail.com

Abstract

This paper proposes an ontological engineering based approach for network security situational awareness which provides formal representation and functional prototype of National Social Security Authority (NSSA). Ontology based approach and Resource Description Format (RDF) is used for implementation of the formal model. Besides this a novel capability to adapt the proposed system according to dynamically changing network structure has been proposed. Secondly the ability to perceive a particular situation in a specific manner by network administrator is to be incorporated in the system. This capability empowers the administrator to devise context specific security policy instead of using a generalized security policy. A number of experiments have been conducted to measure the performance of our proposed framework on a software simulated environment. The performance overheads of proposed framework have been quantified to ascertain the scalability and effectiveness of the proposed system. This approach provides a non-database semantic approach which can be used to semantically correlate information, thus providing an affective mental model to deal with complex network situations.

Keywords: ***Network Security Situational Awareness (NSSA), Ontology, Semantic Web, Semantic Web Rule Language (SWRL)***

1. Introduction

Computer networks now a days are not just means of data transfer. These are also providing various sensitive services to the users. Securing data and maintaining availability of services has become a big challenge. New entities in form of services, hardware, network protocols etc. are being added to the network, which is leading to new ways to attack the network. Network Security Administrators are totally dependent on the automated tools to monitor, detect and control the security of the resources of the network. The agents in action in a network and their mutual interaction make it extremely difficult for a network administrator to maintain appropriate level of situation awareness. Various approaches and techniques for network security have evolved over a period of time like packet filtering, intrusion detection system, intrusion prevention system, biometrics[1](Kumar A, Jayaram R., 2016) etc. The common problems of above approaches are:

a. These mechanisms are not aware of the resources they are protecting.
b. These mechanisms are independent of the context of their application. Their working is similar in every kind of environment.
c. These approaches do not adapt according to the changing environment (configuration of the network and changing scenarios) on the run.
d. Continuous patches and updates are required to maintain their top condition and relevance.
e. These approaches do not take the holistic view of security situation.

To handle these problems a relatively new concept NSSA i.e. Network Security Situational Awareness is

proposed. Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority" [2]. The idea of situation awareness was introduced in Network Security domain by Tim Bass. In his seminal article titled "a glimpse into the future of intrusion detection [3]", he gave an idea about the future intrusion detection systems. But he just proposed a framework; the detailed implementation details have not been provided. Other researchers and group in this area include Stephen Lau (Lawrence Berkeley National Labs), NetSA (The CERT Network Situational Awareness Group) of Carnegie Mellon University, National Center for Advanced Secure Systems Research (NCASSR). The realization of NSSA is divided into three layers as shown in Figure 1.

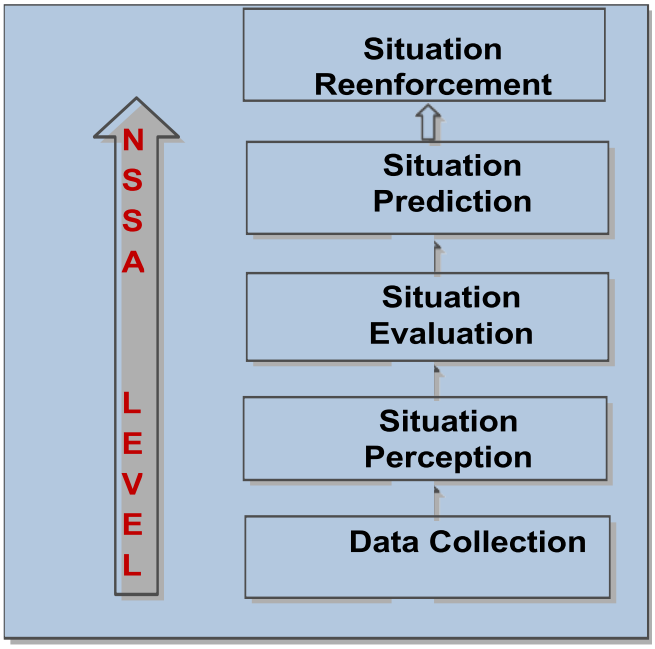


Figure 1. Conceptual model of NSSA

First is perception of Situational Factors i.e. Situation Perception. Second is evaluation of Situation Factors (SF) which involves comprehension, combination, explanation and storage of SFs. The third and most important layer is projection or situation prediction which deals with forecast of network security situations [4] in near future. Another layer i.e. Situation reinforcement has been proposed which deals with incorporating necessary measures to maintain desired security situation of the network. Two detailed theoretical models[5][6] have been proposed. The concept of NSSA has been studied in relation to space base support being provided to defence forces, termed as Space Situational Awareness(SSA) in report of Strategic Studies Institute and US Army war college press[7]. Various techniques have been used to implement these models leading to a limiting success. Following section highlights challenges of NSSA, which still need to be addressed to provide effective situation awareness.

2. Challenges of Network Security Situational Awareness

Despite serious efforts in field of SA in cyber operations, wide gap still exists between the SA being provided by the current system and requirement of cyber operators. There are various challenges to be handled for development of the required system [8]. The biggest challenge in having appropriate SA of the cyber operations is large size and ever changing configuration of the network. Configuration change may be due to addition, deletion of new nodes, installation of new services, addition of new hardware in the network, updation of installed softwares, technology updates and more recently mobile devices. Developing and maintaining an accurate picture of a network has become an insurmountable challenge. Similarly, software systems have become very large and complex. High noise to signal ratio is another serious problem. Anomalous events are quite common in working with computer networks. Users are quite used to systems not working properly and thus may miss early signals of anomalous behaviour of the system and may ignore it as a normal system problem [9]. This abnormal behaviour in the network may act to mask the features of an actual cyberattack. With new technology, potential attack vectors have increased

enormously. According to [10] by 2025 there will be 200 million new malware signatures per year. Speed of events in a computer network provides another challenge. To overcome the challenges of network complexity, change and speed of cyber operations, various types of automated tools have been developed for automatic detection of cyberattacks. While such tools are necessary for supporting SA, keeping in view the limits of human cognition and speed of reaction, high level of automation have been found to actually reduce SA by putting operator out-of-loop making it difficult for them to detect and understand system operations [11][12].

3. Proposed model for NSSA

Keeping in view the challenges highlighted in previous section, we have proposed a framework on the premise that complexity of network situation awareness should be dealt in a layered manner in a fully automated manner. The proposed NSSA framework Fig.2, conforms to the Endsley's three-layer model namely Situation Perception, Situation Evaluation and Situation Prediction. The lowest layer of the proposed framework deals with data from heterogeneous sensors deployed in the network such network monitors, service performance monitors, automated vulnerability scanner, malware detectors, vulnerability databases etc. The individual components of network are represented in network setup layer of the framework. The parameters of interest of each of these components, which are of concern to network administrator are considered as situational factors (SFs). SFs are the most basic unit for NSSA.

The characteristics and relationships among them form the whole network security situation. Network setup layer involves modeling of individual components and inter-component relationships. This layer is responsible for providing situation perception in the network. After modeling of network components and formal representation of inter-component relationship, in network security view layer we propose to handle the concepts related to network security. Networks are mainly used to provide services and share resources in form of services. Therefore, in this layer Service concept is modeled along with its properties. Security issues in the network are result of vulnerabilities in its constituent components. The automated classification of vulnerabilities is essential so has been modeled separately. The result of vulnerabilities, probable attacks and their properties like attack impact, actor, actor location decides the current security situation, so has to be modeled separately.

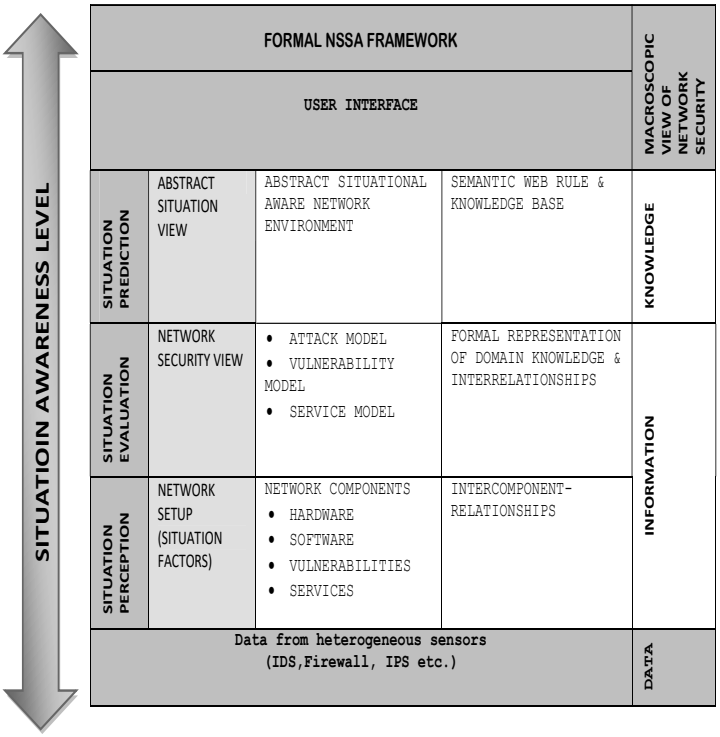


Figure 2 Proposed NSSA Framework

The ability to project the future actions of the elements in the environment in very near term forms the highest level of SA. This is achieved through knowledge of current status and dynamics of the situational factors and comprehension of situation i.e. both the lower level contributes to this layer. To achieve this

level of SA, current security situation is first to be assessed.

4. Use of Ontology for network security

According to [13] Ontology is used for formal representation of knowledge in a domain to make it machine processable. Ontology was initially used for various practical applications by Gruber T.R.[14][15](Guarino N., 1998) (Gruber TR, 1993) proposed to write definitions of the concepts of a domain in predicate calculus, which are then translated by a system called Ontolingua in to specialized representation like frame based system and relational languages. Ontology was used for definition of detection and reaction process of security incident by [16]. They proposed an ontology based methodology for instantiation of security policy in a particular attack context. Ontology has also been used in intrusion detection by [17]. They have proposed ontology specifying a model of computer attack using DARPA- Agent mark-up language and ontology inference layer, which is an extension to Description Logic Language[18] used ontology for situation awareness. In this landmark paper author represented situation theory of Barwise in terms of Web Ontology Language (OWL). [19][20]built ontology for vulnerability and proposed an ontological approach to computer system security. Ontology has been used for automated classification of attacks, vulnerabilities, alerts, for specifying of security policies, intrusion detection and reasoning about situation awareness too [21] have proposed ontology based attack model, which is utilized for security assessment of network and computer system [22] has used layered approach for ontology matching.[23] has used ontology for hierarchical extraction of web data. So use of ontology in different perspectives has been quite pervasive and ontology are at the core of semantic web. Semantic web is defined and linked in a way that it can be used by machines not just for display purpose, but for automation, integration and reuse of data across various applications[24]. There are various studies about implementation of semantic web using ontologies [25] [26]. Focus of these studies has been to provide formal representation of a domain to make it suitable for machine processing. This automated processing may then be used for automated classification and detection.

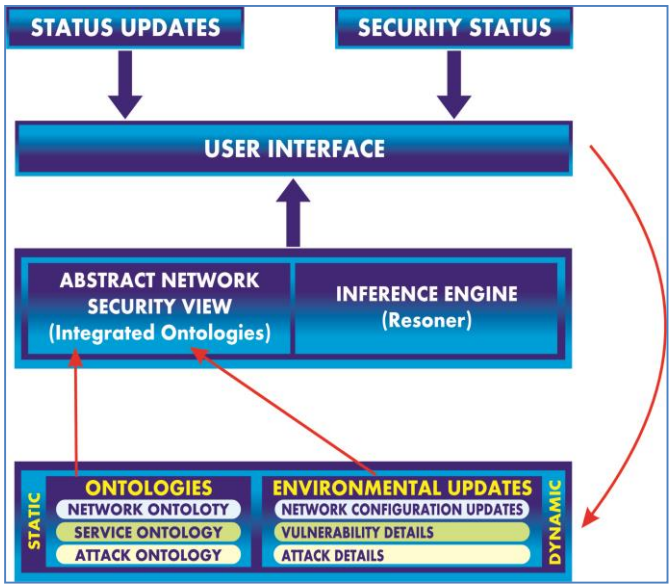


Figure 3. General Architecture of proposed NSSA implementation

5. Ontological Engineering Approach

The present study uses ontological engineering approach towards implementation of framework of network security situational awareness discussed in section 3. Figure 3 shows the general architecture of the proposed NSSA implementation. This architecture consists of a static and a dynamic part at the bottom. Static part consists of Network, Service and Attack ontologies. Dynamic part consists of Network configuration updates, information about new published vulnerabilities and information about new types of probable attacks which may be enabled by new vulnerabilities. The network setup is represented by modeling its components (hardware and software) and their relationships as ontology. Two separate ontologies have been developed to model Vulnerabity and Attack concepts. Hardware, software, vulnerability, attack ontologies together with the network setup represent the network security view of the

network. The Ontology Web Language, recommended by W3C, is used to implement the ontologies [27]. SWRL is used on the top of these ontologies to represent domain specific rules to infer the state of components of the network [28]. This inference is then used to predict the status of higher level concepts and ultimately the network security situation of the network. The concepts, properties and restriction, individuals of network ontology are described as follows. Other ontologies namely *attack ontology, vulnerability ontology, and service ontology* are modeled in similar fashion. Protégé tool is used for the development of ontologies.

5.1 The Network Ontology

The network ontology focuses on building blocks of a computer network and their interrelationships. There is need of network ontology that captures the dynamic interaction among various components of the network components, which is responsible for changing security status of the network. With the increasing number and type of components and multiple values of the properties of the individuals the combinations of situational factors to be handled to perceive and comprehend current situation are enormous. This ontology along with the specified web rules makes the skeleton of the system, which is capable of handling these enormous combinations and hence the dynamic nature of the network security. The knowledge base along with the above edifice enables the network administrator to not only comprehend but take necessary corrective action.

5.1.1 The Concepts

Classes are the focus of most ontology. A subclass of a class represents a concept that has "is a kind of" relationship with the concept represented by the super class. The words concept(s) and class(es) are synonyms for this study, so can be used inter- changeably in the text. The main class hierarchy, consisting of concepts involved in the said ontology is explained below. Thing is abstract super class for all classes. The concepts in the ontology with their brief descriptions are as shown in Table 2.

Network Concept

The *Network* has been considered as a single holistic entity as considered by network administrator. The components are Network_Hardware, Network_Software, Network_Service and Network_Packet_Drop_Rate. The compositional structure is as shown in Figure 4.

Hardware Concept

The *Hardware concept* represents various type of hardware that may be deployed in a network. This covers storage devices, processing devices, gateways, routers, switches etc. The vulnerability information about various hardware devices as per specific make, model and firmware version has been made available by Mitre.org in form of Common Vulnerability Enumeration (CVE) and Common Weakness Enumeration (CWE), which is considered as standard for safety compliance of these devices. The information about the make, model, firmware version of the hardware deployed in the network, are to be represented in form of properties of individuals of *Hardware concept* in the ontology. *Hardware concept* has two sub- classes which represent two types of hardware namely vulnerable hardware and safe hardware. Any hardware deployed in the network is inferred as vulnerable or safe hardware depending upon its object properties explained in the next section.

Table 2. Concepts in the network ontology

S.No.	Concepts	Description
1.	Network	High level concept in the ontology, which is the abstract representation of real world network.
2.	Network_ Hardware	Represents the hardware of all types deployed in the network (network devices in particular and storage and processing devices in general
3.	Network_ Software	Represents the softwares of all types in the network namely, Network Operating System, Protocols, Services and other application softwares.
4.	Network_ Packet_ Drop_Rate	Represents packet drop rate at the gateway of the network. Important characteristic to depict traffic in the network.
5.	Network_ Service	Represents services provided by the network like web server, file server, print server, authentication server etc.

Software Concept

The *Software* is very important component of the network structure, as most of the security concerns emanate from software components of the network. It has two subclasses Network_operating_system and Network_protocol. *Network_operating_system concept* represents the current operating system installed in the network. *Network_protocol concept* represents the current communication protocol and other protocols being used in the network.

Packet Drop Rate Concept

Network_packet_drop_rate concept represents the packet drop rate of the gateway system in the network. This is the vital information about the traffic status of the net- work. The increase in packet drop rate at the gateway represents the first sign of excessive traffic in the network. DDoS attack which accounts for more than 25% of the cyber-attacks initiates by generating excessive traffic at host network[29], so this parameter has been specifically represented in the network. The packet_drop_rate concept has qualitative values like nominal, high and very high packet drop rate. These qualitative values provide the network administrator, the freedom to consider any specific range of quantitative packet drop values as nominal, high or very high.

In case of the network, which caters to a large number of users, the acceptable range of packet drop rate i.e. the range which is considered as nominal must be on the higher side as compared to other network which caters to lesser number of users, where marginally big value must be considered as an alert. On the similar lines Service Concept has been specified. The Service concept represents all the services being provided through the network. The actual services in the network are represented as the individuals of Service concept. This includes all kind of communication services, authentication services, file management services, printing services, account management services and web services. The security status of the network is composition of status of the components identified in this ontology. Based upon the values of the properties of the component concepts of the network, the network may fall in four states namely Safe State, Vulnerable State, Highly Vulnerable State, Congested State, and Under Attack State.

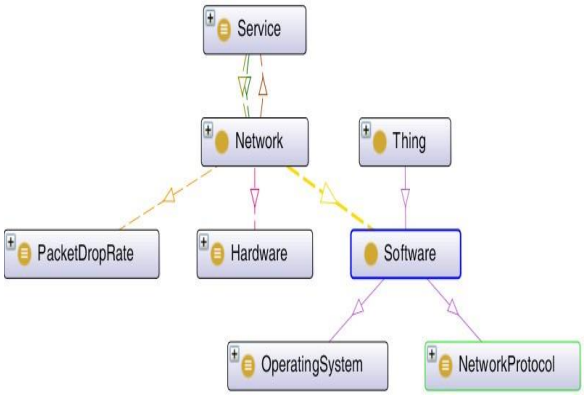


Figure 4. Components of network concept

5.1.2 The Properties

OWL properties represent relationships. These relationships are form of mathematical relation with domain and range. The domain and range are individually set of values of some concept defined in the ontology. These relationships are binary in nature. At the detailed level, object properties link an individual to an individual. Datatype properties link an individual to an XML schema datatype value or an rdf literal. In other words, they describe relationships between an individual and data values.

Object Properties

To represent a network and its real world behavior some properties must be defined in the ontology. There are two types of properties in ontology. These are object properties and data properties. As a convention the name of property starts with lower case letter but may consist of upper case letters in the word, whereas name of concept starts with upper case letter. The graphical visualization to illustrate the linkage between the concepts via properties has been shown in Figure 5 by dotted arrows. Between some of the concepts there is more than one arrow, but each arrow shows the different property or characteristic.

For instance between *Service concept* and *Network concept*, the arrow from *Service to Network concept* represents the object property *"provideBy"* and arrow from *Network to Service concept* represents inverse property *"provides"*.The object property *networkConsistOfHardware* has subproperties. The purpose of *networkConsistOfHard-ware_ProcessingDevice* subproperty is to link network with its hardware components responsible for processing of data. The next object subproperty *networkConsistOf- Hardware_NetworkDevice* links network with hardware components responsible for establishing the network i.e. routers, switches etc.

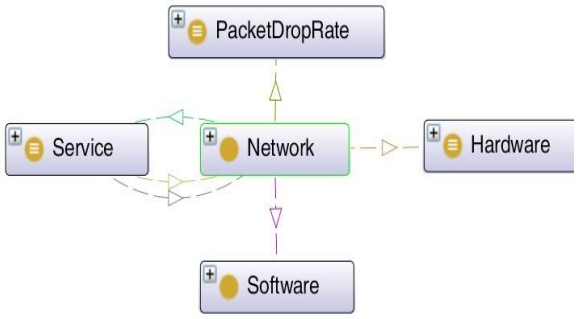


Figure 5. Object properties between the concepts

5.1.3 Individuals

Individual instances are most specific concepts repre- sented in the knowledge base. In case of network ontology the individuals for *Network concept* are generated at run time, whenever network administrator intends to model the network system in form of ontology by creating individuals of component concepts of network i.e. hardware component and software component. In our model we have created a unique ID for network at any instance of time by concatenating current system date, time and a predefined prefix. Services are assumed to be instantiated directly from the log of real network by extracting currently running services in the network. The individuals of *PacketDropRate concept* are qualitative *Nominal, High, and Very High.* Though the packet drop rate is a quantified measure but its value is assessed by the administrator as per the context of the network and mapped to the mentioned individuals as nominal, high or very high. On the similar pattern attack concept and service concept has been implemented.

6. Implementation of the Framework

A prototype system has been developed using OWL API 3.4.2, Java and Pallet & Hermit reasoners to validate the proposed framework and demonstrate its practical applicability. The implemented framework presents the basic elements of the network, vulnerabilities, protocols, services and attacks using web ontology language[27] extended with semantic web rule language [30] for identifying and reasoning about relevant security parameters and corresponding security policies. OWL has been used for modeling the concepts. In order to support the process of specifying network security policies, a set of reasoning rules need to be defined that are associated with the concepts defined in the ontology. To support such needs, Semantic Web Rule Language (SWRL) based rules have been used for specifying network security policies. An example SWRL rule specifying condition for Vulnerable Service is shown below.

NominalVulnerability(?v)∧Service(?s)∧ hasAvgResponseTime(?s, HighResponseTime)∧ hasAvgTurnAroundTime(?s,HighTurnAroundTime)∧ hasServiceImportanceLevel(?s, NominalPriority) ∧ hasUsageFrequency(?s, Normal) ∧ hasVulnerability(?s,?v) ->VulnerableService(?s)

This rule states that if s is a service, the service s is having high response time, high turnaround time, nominal priority, normal usage frequency and service s is having v, a nominal vulnerability then service is to be interpreted as a vulnerable service. Using exhaustive rules asserted in the system along with the axioms and hierarchy of concepts, the prototype system is able to detect vulnerabilities, attacks and hence status of services, hardware and software of the network. This in turn predicts the current status of the network security.

7. Performance Evaluation, Results and Analysis

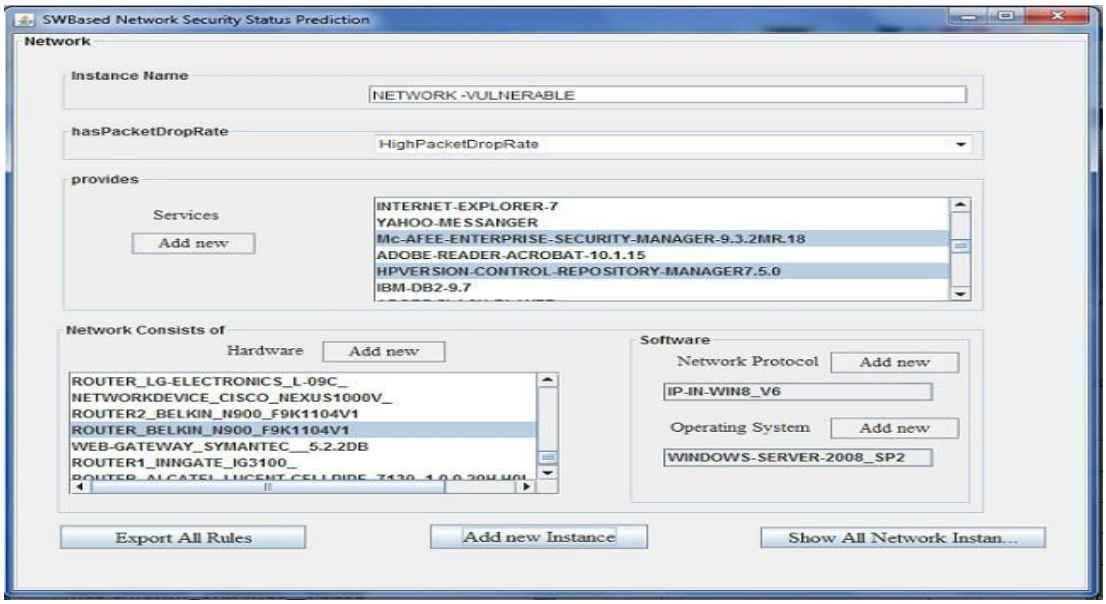


Figure 6. Instantiating a network instance into the system.

To demonstrate the feasibility of the proposed framework, a number of experiments have been conducted on a software simulated environment[31] [32]. The performance overheads of the proposed framework have been quantified for measuring the inference time w.r.t. increase in number of instances, rate of increase of inference time w.r.t. increase in number of policies etc. We have conducted a set of experiments on a system loaded with Windows 7 operating system running on Intel CPU T2250@1.77GHz with 3GB RAM. Case-based approach has been used to analyze the feasibility and scalability of the approach.

5.1 Use Case-I

In this case a network with following specifications has been instantiated into the system as shown in Figure 6. Linux operating system running on kernel 4.1.2, employing Cisco device NX with device OS Nexus 9000 11.1(1C) & Huawei Honor wireless router W5860s, IPV6 protocol, network having high packet drop rate at the border router, network providing services Mc-Afee Enterprise Security Manager 9.3.2 MR.18, HP version control repository manager 7.5.0, Adobe Flash Player.

The status of all the components of the network is inferred based on the rules asserted into the system at that particular instance. The system may be adapted to modification in configuration in the network w.r.t. hardware, software, protocols and services. Status of new systems is then incrementally inferred based on the status of each individual component. By incremental we mean that, an individual of any component is first classified by the reasoner based upon the data properties of the individual. After individual classification, the upper level concepts are classified incrementally based upon object properties i.e. relationship among the concepts and asserted rules. Finally, the network is classified into the categories of Vulnerable Network, Highly Vulnerable Network, Under Attack Network and Safe Network. We have evaluated the total inference time over no. of different network instances modeled in the system (Figure 7). It can be observed from the graph that there is linear increase in inference time w.r.t. increase in number of network instances modeled in the system. In order to measure the inference time, we have increased the number of network instances from 5 to 20. The inference time includes the time taken for classification of concepts, consistency checking and extraction of new implications from the asserted axioms or

rules. The trend of increase of inference time is linear and hence acceptable. This proves that system is adaptable to modification in configuration.

5.2 Use Case II

This use case describes the capability of adding new knowledge in form of new semantic web rules to the prototype system on run time. This feature enables the system to be incrementally intelligent to face future complex situations. The new rules are asserted into the knowledgebase by network administrator. The network administrator is assisted by the prototype system by dividing a single complex situation into many smaller complex situations. These multiple situations are presented to the network administrator one by one.

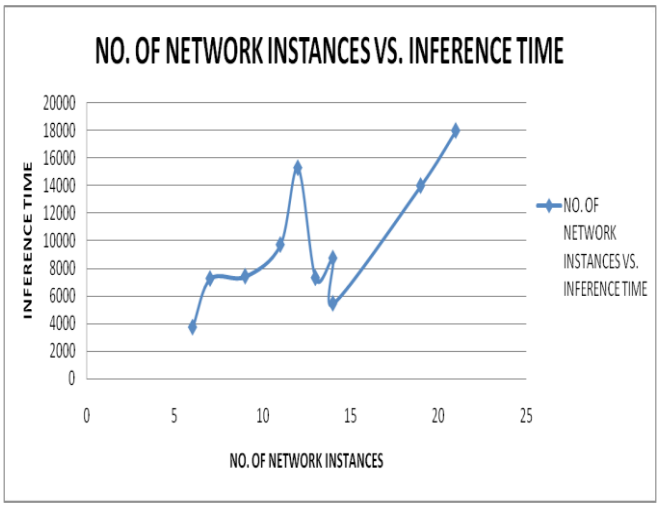
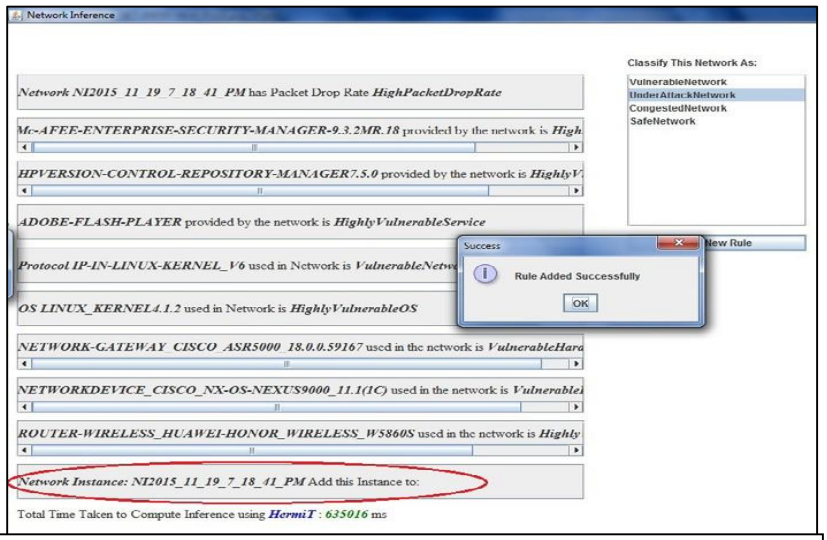


Figure 7. Network instances vs inference time

In this use case the prototype system is confronted with an instance of higher level concept. The higher level concept like Network has been defined in terms of Hardware, Software, Service and Protocol. The classification of new instance of higher level concept like network is governed by the classification of instances of next lower level concept. When no appropriate rule exists in the prototype system to infer a lower level concept, the situation is presented to the network administrator, who then decides the appropriate classification. The decision taken is then converted in form of rule and asserted in the knowledgebase automatically (Figure 8).



All the future inferences are made by the reasoner by using newly included rule. The decision to handle new situation by human operator is as per findings of Mica Endsley in

```
HighlyVulnerableHardware(?h)∧HighlyVulnerableOS(?os) ∧HighlyVulnerableService(?s)∧
Network(?n) ∧Vulnerability(?v) ∧VulnerableNetworkProtocol(?pr)∧
NetworkConsistOfHardware(?n, ?h)∧NetworkConsistOfOS(?n, ?os)∧
NetworkConsistOfProtocol(?n, ?pr) ∧hasPacketDropRate(?n, HighPacketDropRate)∧
hasVulnerability(?s, ?v)∧provides(?n, ?s)--> UnderAttackNetwork(?n)
```

Figure 9. New Rule asserted at run time in the Ontology.

[33]which recommends active participation of human monitor in situation management. Figure represents a situation in which a new network instance has been fed into the system by instantiating its components i.e. Linux as OS, McAfee enterprise security manager, HP version control repository manager, Adobe Flash Player as services, IPv6 Protocol, Cisco ASR 5000 as network gateway, Cisco NX9000 device and Huawei wireless router. All the mentioned instances are classified by reasoner to their suitable classes as per asserted rules and axioms. But this particular combination of various types of instances in the network instance is not classifiable by current set of axioms and rule in the ontology. In such case, the possible classification options are shown to the network administrator who may decide the appropriate classification. This decision is then added in form of rule to the knowledgebase. The new rule (Figure 9), in addition to existing rules makes a bigger knowledgebase, which is then used for classification by the reasoner.

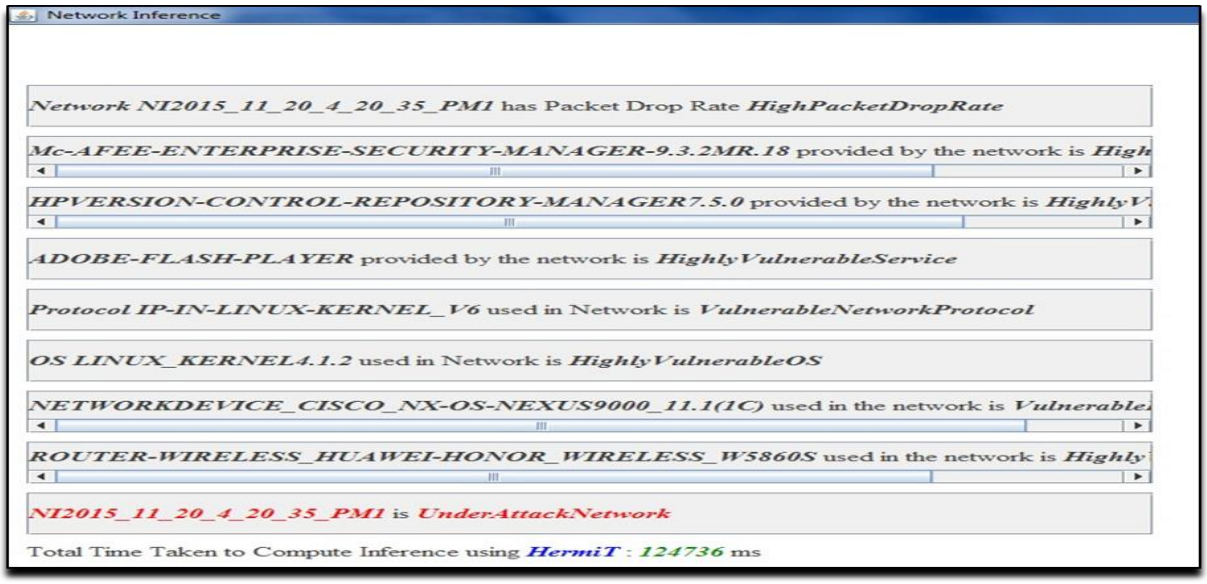


Figure 10. Network inference after addition of new rule

The system is able to check for any kind of consistency issue introduced in the system because of addition of new security policy. If such is the case the issue is reported to the network administrator for one-time corrective action. Figure 10 shows that the new rule has been successfully asserted into the ontology and is being used for the inference. Because of newly asserted rule the network instance with identical components have now been inferred as instance of "Under Attack Network" concept.

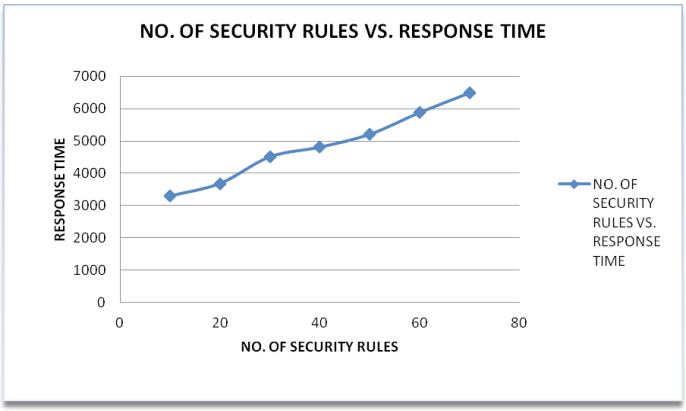


Figure 11. Response time vs no. of SWRL rules

we measured the response time of our prototype system in light of increasing number of security rules. First, we have selected 10 security rules and measured response time, then; we varied the number of security

rules up to 50 and measured the response time. For each of the set- ting, the average value of 10 executions is used for the analysis as shown in the Figure 11.

8. Conclusion

We have validated our proposed network security situational framework and demonstrated its practical implementation by using scenario based approach. Various scenarios have demonstrated the adaptability, scalability, incremental knowledgebase and suitable user interface of the prototype system. We have conducted a number of experiments to measure the performance of our proposed framework on a software simulated environment. We have quantified the performance overheads of our proposed framework for measuring the inference time and response time. All the experimental results have shown that our framework has satisfactory response as far as the performance is concerned and for the better performance, more powerful machines can be used. This approach provides a non-database semantic approach which can be used to semantically correlate information, thus providing an affective mental model to deal with complex network situations.

9. Acknowledgement

This work is supported by University Grants Commission, New Delhi under Minor Research Project grant.

10. References

1. Kumar Ankit, Jayaram Rekha,"Biometrics as a Cryptographic Method for Network Security. *Indian Journal of Science and Technology*. 2016 Jun; 9(22). DOI: 10.17485/ijst /2016/v9i22/95288
2. Tadda GP, Salerno JS. Overview of Cyber Situation Awareness. *Cyber Situational Awareness*. 2010 Apr; 46(1):p.15-35.
3. Bass T. A glimpse into the future of ID, login Special Issue Intrusion Detection, USENIX Assoc Mag. 1999.
4. Yong Z, Xiaobin T, Hongsheng X. A novel approach to network security situation awareness based on multi-perspective analysis. In: *Proceedings of IEEE International Conference on Computational Intelligence and Security*, Harbin, China, 2007 Dec, p. 768-72.
5. Bass, T. Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems. *Irish National Symposium*, 1999, p. 1-6.
6. Lambert, DA. Situations for Situation Awareness. In:*Proceedings of International Conference Fusion*, 2001, p. 1-7.
7. Jeffrey Caton L., Evolving Army needs for space-based support, Strategic Studies Institute, US Army War college, April 2015
8. Endsley MR, Connors ES Foundation and Challenges, In: Cyber Defense and Situational Awareness,Springer, Advances in Information Security 62,2014 .ISBN 978-3-319-11390-6
9. Endsley MR, Jones DG, Disruptions, Interruptions, and Information Attack: Impact on Situation Awareness and Decision Making. In: Proceedings of the Human Factors and Ergonomics Society 45th Annual Meeting, Santa Monica, CA.2001, p 63-68
10. Cyber Vision 2025, United States Air Force,2012, Washington, DC.
11. Endsley MR, Kiris EO. The out-of-the-loop performance problem and level of control in automation. Human factors. 1995 Jun;37(2),p.381-94.
12. Lee, JD, See, KA, Trust in automation: Designing for appropriate reliance. Human Factors,2004, 46(1),p.50-80
13. Robert Arp et. al., Building Ontologies with basic formal ontology, MIT Press, Cambridge, 2015.
14. Guarino, N. Formal Ontology in Information Systems. *Proceedings of International Conference FOIS'98*, 1998, 46, p. 3-15.
15. Gruber TR. A Translation Approach to Portable Ontology Specifications. *Technical Report Knowledge Acquisition*. 1993; 5(2), p.199-220.
16. Vergara JE, Vázquez E, Martin A, Dubus S, Lepareux MN. Use of Ontologies for the Definition of Alerts and

Policies in a Network Security Platform. *Journal of Networks*. 2009; 4(8), p.720-33.

17. Undercoffer J, Joshi A, Pinkston J. Modeling computer attacks: An ontology for intrusion detection. *Springer LNCS Recent Advances in Intrusion Detection*, 2003, p. 113-35.
18. Kokar MM, Matheus CJ, Baclawski K.Ontology-based Situation Awareness. *Springer International Journal on Information Fusion.* 2009; 10(1), p.83-98.
19. Wang J, Guo MM, Camargo J. An Ontological Approach to Computer System Security. *Information Security Journal: A Global Perspective*. 2010; 19(2), p.61-73.
20. Bhandari P, Singh M. Semantic Web Based Technique for Network Security Situation Awareness Status Prediction. 2014, 14, p. 1-7.
21. Gao JB, Zhang BW, Chen XH, Luo Z. Ontology-Based Model of Network and Computer Attacks for Security Assessment. *Journal of Shanghai Jiaotong University Science.* 2013; 18, p.554-62.
22. Viniba V. A Hybrid Layered Approach for Ontology Matching. *Indian Journal of Science and Technology.* 2015 Aug; 8(17). DOI: 10.17485/ijst/2015/v8i17/62219
23. Karthikeyan K, Karthikeyani V. Ontology Based Concept Hierarchy Extraction of Web Data. *Indian Journal of Science and Technology.* 2015 Mar; 8(6). DOI: 10.17485/ijst/2015/ v8i6/61070
24. W3C Semantic Web Activity, 1994-2006, http://www.w3.org/2001/sw/
25. John Hebeler et.al., Semantic web programming, Wiley Publishing,2009
26. Naveen Ashish, Amit P. Sheth Eds., Geospatial Semantics and semantic web, Springer, 2011
27. Smith MK, McGuinness D, Volz R, Welty C. Web ontology language (OWL), Guide version 1.0. *W3C Working Draft*. 2002.
28. Zhang W, Hansen KM. An OWL/SWRL Based Diagnosis Approach in a Pervasive Middleware. In: *SEKE*, 2008 Jul, p. 893-98.
29. Internet Stats. Website: Internet World Stats- www.internetworldstats.com. Downloaded in August 2018.
30. Elenius D, Riehemann S. SWRL-IQ User Manual, 2012, p. 1-33.
31. Salahi A, Ansarinia M. Predicting Network Attacks Using Ontology-Driven Inference. *International Journal of Information and Communication Technology*. 2013; 4(1):1- 9.
32. Lu A, Li J, Yang L. A New Method of Data Preprocessing for Network Security Situational Awareness. In: *2nd International Workshop on Database Technology and Applications (DBTA)*, Wuhan, 2010, p. 1-4
33. Jones DG, Endsley MR. Sources of situation awareness errors in aviation. Aviation, space, and environmental medicine. 1996 Jun.