NSSA: A Holistic Perspective of Network Security

Pardeep Bhandari[1], Dr.Manpreet Singh[2]
Doaba College, Jalandhar, Punjab(India)[1], Punjabi University, Patiala, Punjab, India[2]

Abstract- ***Traditionally network security deals with maintaining the confidentiality of information, authenticating the user and making the resources available reliably to the intended user, but now apart from these concerns which are at the stake in public networks other important factors are availability and survivability of services which are available on the computer networks. The current generation network security means like intrusion detection system, firewalls, virus detection system etc. present only one of the dimensions of a multidimensional problem of overall network security status. These tools provide detailed information about one aspect of the network security. The task of correlating the events happening in the network and being reported by these tools is left to network administrator. The number of services being made available through these networks is increasing exponentially and so is the number of users of these networks. This paper explores a new concept Network Security Situational Awareness (NSSA). Network Security Situational Awareness is a discipline which focuses on perception, evaluation, projection and resolution of the security risk to computer networks. In this paper the term situational Awareness is explained in context of computer network security. So the root of the term NSSA is explored. Various techniques employed to achieve NSSA have been explored in this survey paper. The conceptual model for NSSA and its functional requirements are also discussed.***

Keywords: *Situational Awareness, NSSA, Multi sensor data.*

I. Introduction

The Computer networks are being widely used in sensitive domains, so Network Security has become very sensitive issue. Traditionally network security deals with maintaining the confidentiality of information, authenticating the user and making the resources available reliably to the intended user, but now apart from these concerns which are at the stake in public networks other important factors are availability and survivability of services which are available on the computer networks. The current generation network security means like intrusion detection system, firewalls, virus detection system etc. present only one of the dimensions of a multidimensional problem of overall network security status. The perception of security situation of the network involves fusion of data from heterogeneous sources. The task of correlating the events happening in the network and being reported by these tools is left to network administrator. The number of services being made available through these networks is increasing exponentially and so is the number of users of these networks. The real-time ID systems are not technically advanced enough to detect sophisticated cyber attacks by trained professionals. For example, during the Langley cyber attack the ID systems failed to detect substantial volumes of email bombs that crashed critical email servers (Bass, T., Freyre, A., Gruber, D. and Watt, G.,1998). Coordinated efforts from various international locations were observed as hackers worked to understand the rules-based filter used in counter information operations against massive email bomb attacks. In computer networks, cyber attacks are numerous and evolving, such as code-driven attacks, deliberate malicious software attacks, espionage, distributed denial of service attacks, phising and insider attacks. Although individual and independent controls exist to protect computer networks from each of these attacks, unfortunately, each control is directed towards addressing a specific attack. Hence, detection of widespread or enterprise-wide attacks is challenging (C. Onwubiko,2008); more so, the way existing controls are deployed makes it extremely difficult to detect a variety of attacks, make broader attacks classifications, assess situations perceived in the enterprise, or even quantify associated risks accurately and swiftly. A recommended approach is to use existing controls in the organisation but to combine their set of evidence to provide better situational awareness of network states, and interdependent risks that may exist in networks. To cater to this problem new concept of NSSA has been explored in this paper.

In this paper section II gives brief discussion about evolution of network security technologies; section III discusses the application of concept of situational awareness in the field of network security; Section IV discusses the efforts to use various implementation schemes to achieve holistic view of situational awareness and section V discusses the current research directions in this field.

II. Evolution of Network Security

Various approaches and techniques for network security have evolved over a period of time as shown in Fig.1.

Packet Filtering: Initially the method of packet filtering was proposed. It involved scanning each packet going into and out of the network. Packet filtering determines whether a packet is allowed to enter or exit the network by comparing some basic pieces of information located in the packet's header. Filtering the income packet is called ingress filtering, and filtering the outgoing packet is call Egress filtering. Most suitable device to implement packet filtering is Entry and exit point of your network, and most probably that device is Border Router. In the initial days packet filtering was restricted to layer 3 of OSI model i.e. Network layer, it means traffic was filtered based upon source and destination IP address only, for example Standard access list in Cisco routers(Chapman, 1992; El-Atawy, Al-Shaer, Tran, & Boutaba, 2009). With the development of new rule sets packet filtering upgraded to layer 4 of OSI

ISSN: 2229-6913 (Print), ISSN: 2320-0332 (Online) - www.ijoes.org

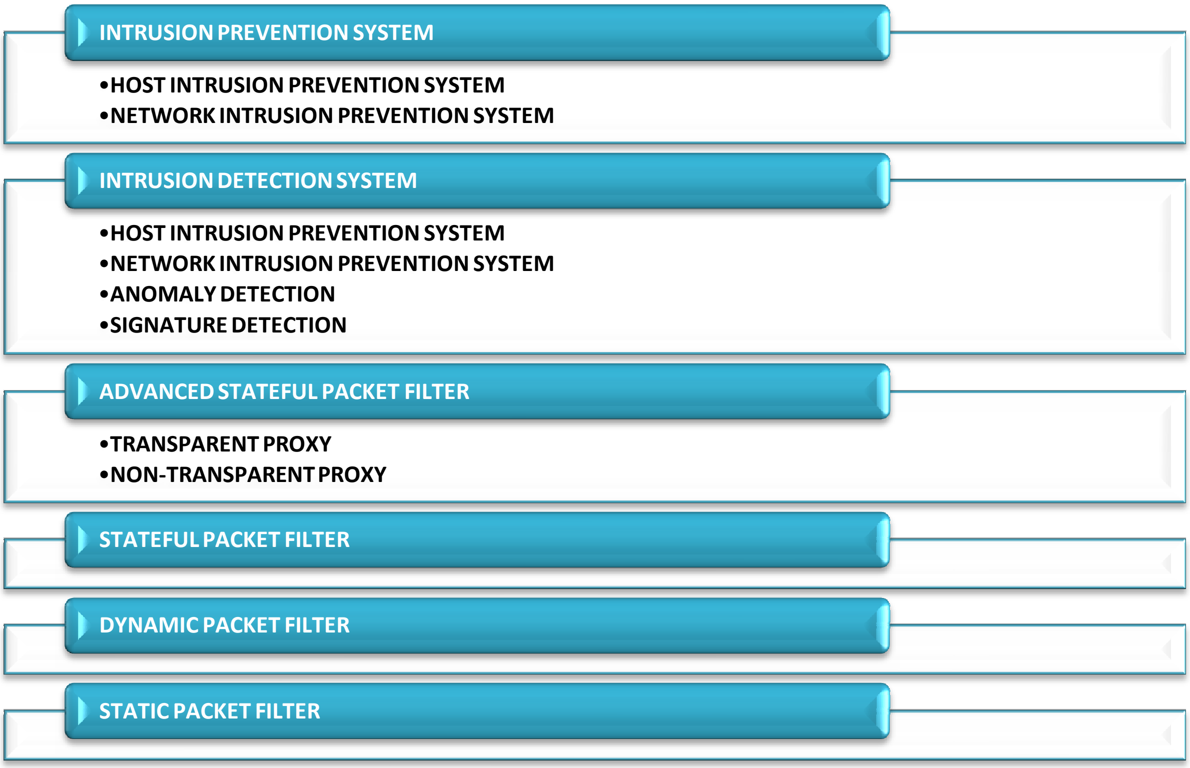
INTRUSION PREVENTION SYSTEM
•HOST INTRUSION PREVENTION SYSTEM
•NETWORK INTRUSION PREVENTION SYSTEM
INTRUSION DETECTION SYSTEM
•HOST INTRUSION PREVENTION SYSTEM
•NETWORK INTRUSION PREVENTION SYSTEM
•ANOMALY DETECTION
•SIGNATURE DETECTION
ADVANCED STATEFUL PACKET FILTER
•TRANSPARENT PROXY
•NON-TRANSPARENT PROXY
STATEFUL PACKET FILTER
DYNAMIC PACKET FILTER
STATIC PACKET FILTER

Figure 1 Evolution of Network Security Techniques

model i.e. Transport layer. It means packet filtering can be done based upon Source, Destination IP addresses and port numbers as well, for example extended access list in Cisco router. But at that moment packet filtering was still missing the capability of application behavior detection, application comes into action at layer 7 of OSI model i.e. Application layer. With the course of the time advanced packet filtering mechanisms developed and Packet filtering armed with traffic filtering capabilities at layer 7 in OSI model i.e. Application layer, for example Stateful packet filtering emerged.

Packet Filtering can be categorized as Static Packet Filtering, Dynamic packet filtering, Stateful filtering. Filtering the traffic based upon pre-defined rules of accept and deny rule set is called packet filtering. Static packet filtering was one of the first Network security mechanisms. Static packet filtering can be implemented using Standard and Extended Access Control List in Cisco router and IP Tables and IP chains in Linux based systems. The standard access list is used to specifically allow or disallow traffic from a given source IP address only. It cannot filter the packets based on destination or port number. Because of these limitations, the standard access list is fast and is preferred when the source address is the only criteria on which we need to filter. Despite many positive uses of packet filters, problems exist due to inherent limitations in the way packet filters work. Spoofed and fragmented traffic can bypass the packet filter if protections aren't properly implemented. In addition, because of the always-open nature of a "permit" static packet filter, issues exist with opening such a "hole." The concept of Dynamic packet filtering is that filters are built on-the-fly as needed and torn down after connections are broken. Reflexive access lists are examples of dynamic packet-filtering technology. A criterion is set up on the outbound interface that watches defined connection types to the outside world. When the traffic returns, it is compared to an access list that was dynamically created as the outgoing traffic left the network. The stateful filtering device spends most of its cycles examining packet information in Layer 4 (transport) and lower.

Another approach for protecting the network from unsafe environment is proxy firewall. It acts as a *route* for every network to network conversation. Connections do not flow through a proxy. Instead, computers communicating through a proxy establish a connection to the proxy instead of their ultimate destination. The proxy then initiates a new network-connection on behalf of the request. This provides significant security benefits because it prevents any direct connections between systems on either side of the firewall.

Proxy firewalls are often implemented as a set of small, trusted programs such that each supports a particular application protocol. Each proxy agent has in-depth knowledge of the protocol it is proxying, allowing it to perform complete security analysis for the supported protocol. This provides better security control than is possible with a standard stateful firewall. However, we receive this benefit only for the protocols included with the proxy firewall. If we allow the use of a protocol that the proxy firewall does not specifically support, this is equivalent to using a generic proxy. Generic proxies do not have any in-depth knowledge of the protocols they proxy, so they can only provide basic security checks based on the information contained within the headers of the packets (IP address, port, and so on). Above mentioned approaches were initial efforts to control the flow of incoming and outgoing traffic as per security requirements of the user. These approaches allowed or prevented the communication as per predefined rules. Then more advanced systems have been proposed and implemented which helped the network administrator not only to restrict the network traffic but to comprehend the meaning of traffic and detect the possible intrusion, and were termed as Intrusion Detection Systems(Journal, 2012).

Intrusion Detection System: Intrusion detection systems are designed to sniff network traffic and analyze it to identify threats in the forms of reconnaissance activities and attacks. By detecting malicious activity, network intrusion detection tries to identify and react to threats against the network. IDS are of two types: Network Intrusion detection systems (NIDS), and Host Intrusion detection systems (HIDS). Properly configured and robust IDS can play more than one role in identifying typical attacks. IDS can detect reconnaissance activity that may indicate future targets of particular interest. It also generates alerts for the subsequent attempts to breach host security. Alerts are usually generated through one of two methods. The first method, **anomaly detection**, relies on statistical analysis to identify traffic that falls outside the range normally seen in this environment, or it relies on protocol analysis to identify traffic that violates protocol standards or typical behavior. The second method **signature detection**, identifies known attack signatures observed in traffic(Scarfone & Mell, 2007).

IDS suffer from problems of False Positive and False Negative alarms. Signature development is always a balancing act. A specific signature might be extremely accurate in identifying a particular attack, yet it might take many resources to do so. If an attacker slightly modifies the attack, the signature might not be able to identify it at all. On the other hand, a general signature might be much faster and require far fewer resources, and it might be better at finding new attacks and variants on existing ones. The downside of a general signature is that it also might cause many false positives when a sensor classifies benign activity as an attack.

The more recent approach for network security is Intrusion Prevention System (IPS). Intrusion prevention technology adds an active layer of defensive technology. Intrusion prevention technology attempts to stop the attacks before they are successful. IPS is of two types: Network Intrusion Prevention System (NIPS) and Host Intrusion Prevention System (HIPS). An IPS must be a fast, maintain the state, know the application protocol or behavior, be accurate and up to date, and be able to nullify an attack. This is done by maintaining list of signatures of the known attacks. The exhaustive list of attack signatures or patterns cannot be maintained(Scarfone & Mell, 2007).

These approaches are deployed in computer networks as generic systems with little or no customization. The customization, if any, is general or ad-hoc in nature and with little attention to the resources being secured. Various network environments are significantly diverse in nature w.r.t. end-host characteristics, threat perception, services deployed and traffic behavior – a collection of features, which constitute the security context of a network. The scale and diversity in security context of production networks make manual or ad hoc customization of security systems difficult (Sinha, 2009).

The common problems of all the 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 common to every kind of environment.
c. These approaches do not adapt 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 solve these problems a formal model of network security is required to represent entities of a network. The model should have the extensibility to accommodate new entities, to represent the relationships among the entities and also adapt to configuration changes in the network. Another issue is to handle heterogeneous data to get a holistic view of the network security. Data produced whether net flow or produced by various sensors in the network is heterogeneous in nature. The model should be able to handle such heterogeneity in data and should provide mechanism for automated fusion and processing of the network data. These are the prime requirements for perception and comprehension of the network security(Bass, 1999)(Zhang & Geng, 2008).

II. Situational Awareness

The term Situational Awareness is the perception of elements in environment with a volume of time and space, their interpretation and projection of their states in the near future. In other words, Situational Awareness is taking into consideration various environmental factors of a particular domain in totality.(Baclawski & Matheus, 2003; Endsley, 1996)

Mica Endsley(Endsley, 2000) has given a model for situational awareness. Her model has two main parts: the core Situation Awareness portion and the various factors affecting Situation Awareness. The situation awareness portion of the model shows that the process of situation awareness involves perception of elements of the situation as its innermost component. These elements are termed as situational factors. Situational factors are the parameters of utmost importance in a particular context. The perception of these situational factors involves getting their status, attributes and dynamics of these elements in the environment. It also involves the classification of values of situation factors into understandable and preferably machine processable representation. These representations provide the basic building blocks for Level 2 and Level 3. After identification of situational factors, inter-component relationships are to be established to comprehend the current situation i.e. Situation Comprehension. This level requires the domain knowledge and contextual relationship among the situational factors. It includes the integration of multiple pieces of information and a determination of their relevance to the underlying goals. Comprehension provides an organized picture of the current situation by determining the significance of objects and events. Level 3 i.e. situation projection involves, projection of situation of the system in near future. This level is a dynamic process, as it combines new information with the information provided by level 2. Level 3 is the highest level of awareness.

The model shows that situational awareness is governed by the goals and objectives of the systems. These goals and objectives define the context for situation awareness, which in turns decides the situational factors. Other portions of the model show how the human manager is able to make decisions based upon the output of core portion of the model. The decision and the quality of actions based upon those decisions depends on long term memory, information processing mechanism and automation of the system. The abilities, experience and training also affects the decision making capabilities of the decision maker. Apart from these interface of the system, complexity of the domain and stress and workload influences the situational awareness of the administrator.

III Application of Situation Awareness for Network Security

The situational awareness described above has been extensively used in Air Traffic Control, Military Command and control, missile defense etc. There is a striking similarity between the transit of a datagram on the Internet and an airplane through airspace and between future network management and air traffic control (ATC). At a very high abstract level, the concepts used to monitor objects in airspace apply to monitoring objects in networks. The DGCA divides airspace management into two distinct entities. On the one hand, local controllers guide aircraft into and out of the airspace surrounding an airport. Their job is to maintain awareness of the location of all aircraft in their vicinity, ensure proper separation, identify threats to aircraft, and manage the overall safety of passengers. Functionally, this is similar to the role of network controllers, who must control the environment within their administrative domains.(Endsley, 1996)(Bass, Tim, 1999) The network administrator must ensure that the proper ports are open and that the information is not delayed, that collisions are kept to a minimum, and that the integrity of the delivery systems is not compromised. The DGCA maintains situational awareness of whole air traffic. For proper management of our ever expanding computer networks there is dire need of Network Security Situational Awareness. So, Network security situational awareness (NSSA), a terminology recently used to describe situation awareness in computer network defence (CND), relies on the knowledge and ability of the analyst to perceive and analyse situations, make sound decisions on how to protect organisations' valued assets and offer accurate predictions of future states in a dynamic and complex environment(Bass, Tim, 1999).

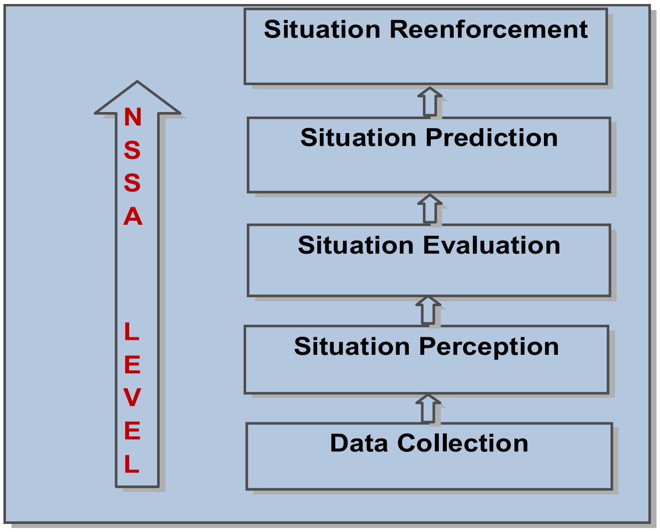

Figure 2 Conceptual Model of NSSA(Yong et al., 2007)

According to Zhang Yong et. al.(Yong, Xiaobin, & Hongsheng, 2007),modeling is the basis of NSSA. According to Tim's idea, it's to construct the network security situation infrastructure with the application of multisensors data fusion. Tim Bass gave a primary framework which provides conceptual analysis of NetSA. It is the basis of other models. But it can't solve the actual security problems and has many shortages. As networks evolve in complexity, the number of objects, threats, sensors and data streams dramatically increase (Bass T. et. al., 1998). (Yong et al., 2007) has given a general conceptual model (Fig. 2) for NSSA, which is a generalization of various models. Data collection module observes information in cyberspace and captures metadata by multi-sensors. The output of this module is raw data from various sensors. Situation perception module analyzes the original data, classifies and converts the data in machine processable form. Situation evaluation module analyzes the input of security incidents with precise mathematics model, gives a comprehensive and quantitative description of current situation. It is the core of situation awareness. Situation prediction module comprehends all historical situation values this module plots situation map. It forecasts the future situation using time series model. Security Reinforcement Scheme module gives a practical security reinforcement scheme to guide managers to improve network security.

IV APPROACHES USED FOR NSSA

The field of NSSA is still in its infancy. The reference architecture of situational awareness system for dynamic environment is given by George P. Tadda et.al(Tadda & Salerno, 2010) is shown in Fig. 3. It is a combination of Endsley's model and JDL data fusion model. In this model the levels 0,1,2,3,4 of JDL model of data fusion are mapped on to the levels proposed by Endsley's model viz. situation perception, situation comprehension and situation prediction. Situation perception covers level 0 and level1. Level 0 involves gathering real time data from sensors and other data sources, which have been termed as situational factors in Endsley's model. Level1 involves identification of object (physical and abstract), concepts, events and group of entities and their relationship. So level1 termed as "object recognition and tracking level" also maps to situation perception level. For recognition of objects, concepts, events etc. models and a priori knowledge of the domain is required. Level3 i.e. impact and threat assessment deals with prediction of future events on the system. This level maps to the situation prediction level of Endsley's model. Level 4 i.e. process refinement deals with improvement in the prediction process of the system. This level is actually about the feedback process in the situation awareness system. Situation prediction at one particular instance of time assists the analyst to predict future situation more accurately, incrementally. Most important observation is that, human is an inevitable part of this awareness system as the system alone is not capable of making prediction in case of patterns, which has never been encountered before. It is important that the human use these tools as input and verify/validate the results. Various techniques are being applied in four core modules of NSSA. The following table, Table1 tabulates the main contributions in field of NSSA.

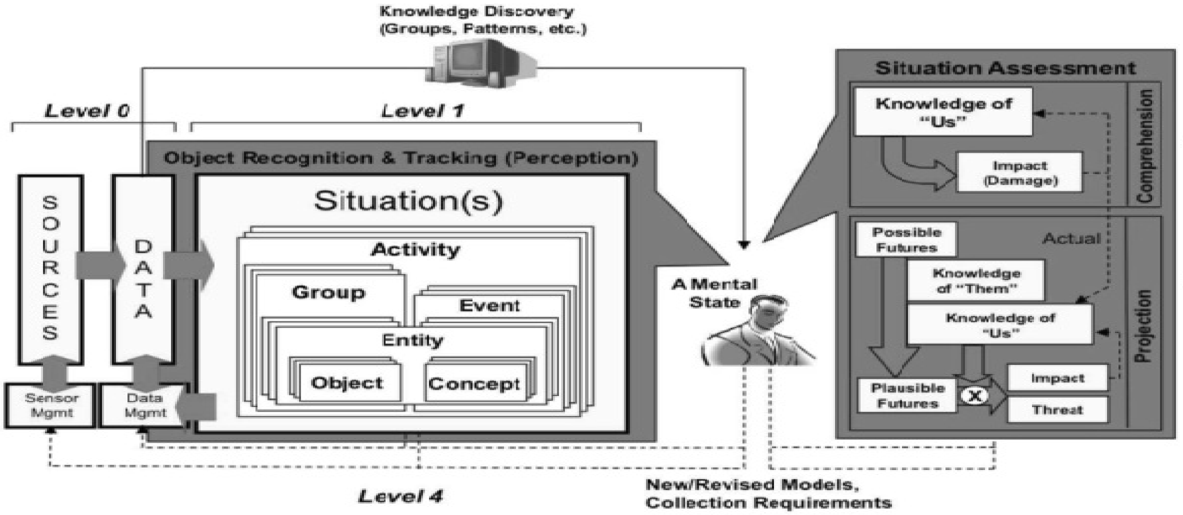

Figure 3 Situational Awareness Reference Model(Tadda & Salerno, 2010)

Table 1 Application of various techniques for NSSA

AUTHOR	YEAR OF PUBLICATION	Paper	CONTRIBUTION	Research Gap
(Bass, Tim, 1999)	1999	Proposed the road map for future generation IDS	One of the earliest researchers to highlight the application of situation awareness concept being used in aviation field, in the field of cyber security by modifying the current generation IDS.	Didn't provide a prototype system or model for its implementation.
(Bass, 2000)	2000	Intrusion Detection System & Multi sensor data fusion: Creating cyberspace situational awareness	Highlighted that for better cyberspace situational awareness, IDS must be supplemented with multi sensor data fusion.	Introductory paper without formal model for implementation

(Jibao, L., Huiqiang, W., & Liang, 2006)	2006	Used additive weight and grey theory for NSSA	Model of current security situation evaluation is established using simple additive weight of threat degree of attacked services and grey theory is used to predict future network situation.	Scalability and application in various types of networks is not established.
(Hu, Li, & Shi, 2006)	2006	Proposed a hierarchical model for network security situation, which works by weighted evaluation of vulnerabilities in each node of the network.	Proposed model based upon statistical computations about the damage degree which the network may suffer	No provision to justify the result and assist network administrator to find possible problem areas.
(Jibao, Huiqiang, Xiaowu, & Ying, 2007)	2007	Proposed a quantitative prediction method for network security situation based on wavelet neural network	Proposed an improvement over the method based on back propagation neural network on same architecture.	Though the improvement in convergence speed and training effect is there, but the provision to incorporate the dynamic structure of the network components is missing
(Yong et al., 2007)	2007	Proposed a multi perspective model for NSSA based upon evaluation of attacks, vulnerabilities and security services.	Quantified the network security situation awareness and used time series analysis to predict future situation.	Model not implemented on real world network
(Liu, Wang, Lai, Liang, & Yang, 2007)	2007	Proposed NSSA based on heterogeneous multi sensor data fusion. Used support vector machine as fusion engine and used feature reduction technique to minimize computation cost.	According to the authors multi sensor data fusion along with feature reduction has resulted in better NSSA. Proposed a situation generation method and a novel situation process mode that makes the automatic response possible.	No method to reduce invalid data and for feature reduction. Also visualization which is an important part of SA is not covered in the model.
(H. Wang, Lai, Liu, & Liang, 2007)	2007	Proposed a method to forecast the network security situation based on the Back Propagation Neural Network with Genetic Algorithm (GABPN).	The proposed quantitative forecast method of network security situation based on GABPN has combined the self-learning and self-adaptation advantages of the BP neural network and fast global searching capacity of a genetic algorithm	Although the proposed approach apparently exceeds the SF_BPN in the convergence speed, functional approximation and forecast accuracy, the scalability of approach to handle large amount of runtime data is not proved. Adaptability of approach for different topologies of networks has not been considered.

(Liang, Wang, & Lai, 2007)	2007	Proposed a quantitative method of network security situational awareness using a combination of evolutionary strategy and neural network. Evolutionary strategy is used to optimize the parameters of neural network, and the evolutionary neural network model is established to extract the network security situational factors.	A layered NSSA model is proposed in which lowest layer consists of situational factors and provides situation perception. Combination of situation factors provides situation comprehension and the top most layer uses neural network to provide situation projection.	Model is not capable of handling all types of known attacks and depends on the subjective assessment of different experts.
(Liang, Y., Wang, H. Q., Cai, H. B., & He, 2008)	2008	Used Hidden Morkov Model to model Network Security SA.	HMM is of the characteristic of dual stochastic process, and similarly the state of both the attacker and services in networked system together constitutes the real network security status, a stochastic mathematical modeling for NSA is finally established in this paper	Not validated on various types of networked systems.
(J. Wang, Qin, & Ye, 2008)	2008	Proposed an improved model for NSSA.	Introduced privacy preserving module, enriched the data source for better situation perception and integrated GIS technique for better visualization	The paper suggests the improved model but detail workability of the model has not been discussed.
(Hui-qiang, Ji-bao, Ying, & Xiao-wu, 2008)	2008	Proposed a classification method of security sensors, design a general architecture of security sensor and mentioned some key technologies related to implementing security sensors.	Extraction of situation factors and their precise reporting and measurement provided by security sensors is fundamental to effective network situational awareness. This paper provided insight about sensor classification, placement and management in the network.	Contributed in situation perception for NSSA
(Lin, Chen, Guo, & Liu, 2008)	2008	Proposed a method for situation prediction based on particle swarm optimization for optimizing back propagation neural network.	Main contribution of this paper is to optimize the back propagation neural network for network situation prediction based on particle swarm optimization.	Contributed for security state prediction

(H. Wang, Liang, & Ye, 2008)	2008	Proposed a method to extract situation factors for NSSA using evolutionary strategy and evolutionary neural network	Established the fact that effective extraction of situational factors may be achieved by evolutionary strategy based neural network as compared to genetic algorithm based neural network.	Contributed in situation perception for NSSA
(Liu, Yu, & Wang, 2009)	2009	Proposed NSSA based on heterogeneous multi sensor data fusion. Employed Multi layer feed forward neural network and feature approach to improve real time nature of fusion engine and hence SA computation cost.	Multilayer feed forward neural network in combination with feature reduction approach has been used as real time fusion method. Security situation generation method for automatic response is also proposed.	Fusion method for heterogeneous data needs to be refined and method must be tested for complex network topologies.
(Sun & Xu, 2009)	2009	Proposed a novel antibody concentration based method for NSSA inspired from biological immune system.	Proposed principles and framework of system termed as ACnssa based on concepts and mathematical model of antibodies, antigens and lifecycle of mature and memory lymphocyte in the biological immunity systems. The antibody concentration has been used as a measure of damage done to the system as a result of an attack.	The proposed framework is focused only on network attack frequency and intensity. Other security factors like network flow, vulnerabilities in the services, softwares, hardwares etc. have not been considered.
(Nian, Diangang, Xuemei, Sunjun, & Kui, 2009)	2009	Proposed application of artificial immune technology in NSSA.	Proposed a proactive defense technique to move towards self defending networks which provide grounds for reasonable and accurate response to ensure the availability of the system.	Provides the theoretical foundation for the application of artificial immune technology for NSSA, formal framework has not been developed.
(Onwubiko, 2009)	2009	Proposed a conceptual model for NSSA based on (Endsley, 1995)	Highlighted ten fundamental attributes of situational awareness, which should be considered in designing and implementing SA in network security.	Laid the theoretical foundation of required functional characteristics of NSSA.
(Li & Wang, 2009)	2009	Proposed a method to quantify the network security situation of the network using conditional random fields.	Attempted to apply the segmenting and tagging capabilities of CRF model to NSSA. Diverse set of effective features have been used as network security factors.	Contributed for quantification of network security.

(Xiaobin, Guihong, Yong, & Ping, 2009)	2009	Applied exponential and logarithmic analysis to compute network security situation of the network	Proposed multi-level quantization model to quantify security situation of the network, which is better poised than previous methods of summing up value of security situations of individual assets of the network.	Not flexible to incorporate dynamic nature of the components and network configuration as whole.

Above table tabulates the main theme of the paper, its contribution and research gap identified from the paper. The tabulation shows that though the efforts are on to formalize and optimize different levels of NSSA, but holistic practically implementable model is not proposed. The systematic flow of information from lower to higher level of NSSA is utmost requirement.

VIII. Conclusions and Future Scope

As discussed above various diverse techniques have been used for comprehensive NSSA, and results have been encouraging. Some techniques are related to representation of states of a network, extraction of situational factors, quantification of security state of a network etc. But still there is gap between actual situation of network security and availability of monitoring and response system for security of sensitive computer networks. There hasn’t been development of any concrete theory in this field. Because of dynamism and stakes involved in this field, there is a lot of scope of research in this field. The formulation of formal model for Network Security Situation Awareness, which possesses the desirable properties of dynamism, adaptability, comprehensive and practically implementable will be our future direction of research.

References

- Mica R. Endsley. “Theoretical underpinnings of Situation Awareness: A Critical Review.”, In *Situation Awareness Analysis and Measurement* (pp. 3-32). Mahwah, NJ: Lawrence Erlbaum Associates Inc.
- Baclawski, K., & Matheus, C. J. (2003). Formalization of Situation Awareness. *Practical Foundations of Business System Specifications. Springer Netherlands*, 25–39.
- Bass, T., Freyre, A., Gruber, D. and Watt, G.(1998) “E-Mail bombs and countermeasures: Cyber attacks on availability and brand integrity”. *IEEE Netw. 12,* 2 (Mar./Apr.), 10–17.
- Bass, T. (1999). Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems. *Irish National Symposium*, 24–27. doi:10.1.1.51.1753
- Bass, T. (2000). Intrusion Detection Systems & Multisensor Data Fusion : Creating Cyberspace Situational Awareness. *Communications of the ACM*, *4*, 99–105.
- Bass, Tim, and D. G. (1999). a glimpse into the future of id. *Login: Special Issue Intrusion Detection, The USENIX Association Magazine*.
- C. Onwubiko,(2008) “Security Framework for Attack Detection in Computer Networks”, VDM Verlag Publisher, ISBN: 978-3-639-08934-9.
- Chapman, D. B. (1992). Network (In)Security through IP Packet Filtering. *Proceedings of the UNIX Security Symposium III*.
- El-Atawy, A., Al-Shaer, E., Tran, T., & Boutaba, R. (2009). Adaptive Early Packet Filtering for Defending Firewalls Against DoS Attacks. *Infocom 2009, Ieee*, 2437–2445. doi:10.1109/INFCOM.2009.5062171
- Endsley, M. R. (1995). Towards a theory of situational awareness in dynamic systems. *Human Factors Journal*.
- Endsley, M. R. (2000). THEORETICAL UNDERPINNINGS OF SITUATION AWARENESS : A CRITICAL REVIEW Process More Data ≠ More Information.
- Hu, W., Li, J., & Shi, J. (2006). A Novel Approach to Cyberspace Security Situation Based on the Vulnerabilities Analysis. *2006 6th World Congress on Intelligent Control and Automation*, 4747–4751. doi:10.1109/WCICA.2006.1713284
- Hui-qiang, W., Ji-bao, L., Ying, L., & Xiao-wu, L. (2008). The Classification, Design and Placement of Security Sensor for Network Security Situational Awareness System. *2008 International Conference on Internet Computing in Science and Engineering*, 321–324. doi:10.1109/ICICSE.2008.62
- Jibao, L., Huiqiang, W., Xiaowu, L., & Ying, L. (2007). A Quantitative Prediction Method of Network Security Situation Based on Wavelet Neural Network. *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*, 197–202. doi:10.1109/ISDPE.2007.36
- Jibao, L., Huiqiang, W., & Liang, Z. (2006). Additive Weight and Grey Theory. *International Conference on Computational Intelligence and Security, Chicago*, *Vol. 2*, 1548–1554.
- Journal, A. (2012). Intrusion Detection and Prevention System : Classification and Quick Review, *2*(7), 661–675.

- Li, J., & Wang, H. (2009). A Quantification Method for Network Security Situational Awareness Based on Conditional Random Fields. *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, 993–998. doi:10.1109/ICCIT.2009.155
- Liang, Y., Wang, H., & Lai, J. (2007). QUANTIFICATION OF NETWORK SECURITY SITUATIONAL AWARENESS BASED ON EVOLUTIONARY NEURAL NETWORK, (August), 19–22.
- Liang, Y., Wang, H. Q., Cai, H. B., & He, Y. J. (2008). A Novel Stochastic Modeling Method for Network Security Situational Awareness. In *The 3rd IEEE Conference on Industrial Electronics and Applications* (pp. 2422–2426). NanGang, China.
- Lin, Z., Chen, G., Guo, W., & Liu, Y. (2008). PSO-BPNN-Based Prediction of Network Security Situation. *2008 3rd International Conference on Innovative Computing Information and Control*, 37–37. doi:10.1109/ICICIC.2008.436
- Liu, X., Wang, H., Lai, J., Liang, Y., & Yang, C. (2007). Multiclass Support Vector Machines Theory and Its Data Fusion Application in Network Security Situation Awareness. *2007 International Conference on Wireless Communications, Networking and Mobile Computing*, 6343–6346. doi:10.1109/WICOM.2007.1557
- Liu, X., Yu, J., & Wang, M. (2009). Network Security Situation Generation and Evaluation Based on Heterogeneous Sensor Fusion. *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, 1–4. doi:10.1109/WICOM.2009.5302714
- Nian, L., Diangang, W., Xuemei, H., Sunjun, L., & Kui, Z. (2009). Research on Network Security Situation Awareness Technology Based on Artificial Immunity System. *2009 International Forum on Information Technology and Applications*, 472–475. doi:10.1109/IFITA.2009.487
- Onwubiko, C. (2009). Functional requirements of situational awareness in computer network security. *2009 IEEE International Conference on Intelligence and Security Informatics*, 209–213. doi:10.1109/ISI.2009.5137305
- Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, *800*, 94. Retrieved from http://www.reference.com/go/http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
- Sinha, S. (2009). Context-Aware Network Security.
- Sun, F., & Xu, F. (2009). Antibody Concentration Based Method for Network Security Situation Awareness. *2009 3rd International Conference on Bioinformatics and Biomedical Engineering*, (1), 1–4. doi:10.1109/ICBBE.2009.5162372
- Tadda, G. P., & Salerno, J. S. (2010). Cyber Situational Awareness, *46*, 15–36. doi:10.1007/978-1-4419-0140-8
- Wang, H., Lai, J., Liu, X., & Liang, Y. (2007). A Quantitative Forecast Method of Network Security Situation Basedon BP Neural Network with Genetic Algorithm. *Second International Multi-Symposiums on Computer and Computational Sciences (IMSCCS 2007)*, 374–380. doi:10.1109/IMSCCS.2007.65
- Wang, H., Liang, Y., & Ye, H. (2008). An Extraction Method of Situational Factors for Network Security Situational Awareness. *2008 International Conference on Internet Computing in Science and Engineering*, 317–320. doi:10.1109/ICICSE.2008.53
- Wang, J., Qin, Z., & Ye, L. (2008). Modeling of Network Situation Awareness. In *International Conference on Communications, Circuits and Systems,IEEE 2008.* (pp. 461–465).
- Xiaobin, T., Guihong, Q., Yong, Z., & Ping, L. (2009). Network Security Situation Awareness Using Exponential and Logarithmic Analysis. *2009 Fifth International Conference on Information Assurance and Security*, 149–152. doi:10.1109/IAS.2009.38
- Yong, Z., Xiaobin, T., & Hongsheng, X. (2007). A Novel Approach to Network Security Situation Awareness Based on Multi-Perspective Analysis. *2007 International Conference on Computational Intelligence and Security (CIS 2007)*, 768–772. doi:10.1109/CIS.2007.160
- Zhang, F., & Geng, I. (2008). Using data fusion for awareness of intrusion in large-scale network. *2008 International Conference on Communications, Circuits and Systems*, 519–523. doi:10.1109/ICCCAS.2008.4657827