International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

A Survey on Cyber Security Analytics

Nerella Sameera[1*], M. Shashi[2]

[1,2] Department of CS&SE, AU College of Engineering (A), Andhra University, Visakhapatnam, INDIA

[*]*Corresponding Author: sameerascholar@gmail.com, Tel.: +91-7989006859*

Available online at: www.ijcseonline.org

Accepted: 24/Nov/2018, Published: 30/Nov/2018

Abstract— Increase in internet dependency in all walks of life, digital nature of data in huge amounts getting accumulated through online transactions and decentralization of data repositories, has led to the development of effective security mechanisms. While discussing the challenges of combating cybercrime, this paper provides a comprehensive overview of cyber security mechanisms, recent attack prediction techniques to create attack prediction models. This paper also explores recent trends in cyber-security like graph data analytics and security in wireless sensor networks. Emerging trends in security system design leveraging social behavioral biometrics, network security analytics, and contextual information to identify known as well as unknown cyber- attacks are also discussed. A framework for contextual information fusion to detect cyber-attacks is presented.

Keywords- Contextual information, Attack similarity, Zero-day attack, vulnerability

I. INTRODUCTION

The process of digitalization of all aspects of human life, like healthcare, education, business, etc., has gradually led to the storage of all sorts of information, including sensitive data. We can define security, as the process of protecting the digitized information from theft or from physical damage while maintaining the confidentiality and availability of information [1]. But as technology is growing rapidly, the cybercrime rate also increases both in number and complexity. The reason behind this tremendous growth in cyber-crime is the usage of inadequate software, expired security tools, design flaws, programming errors, easily available online hacking tools, lack of awareness in public, high rates of financial returns, etc. In order to explore the vulnerabilities in the target and thereby to attack the victim, more powerful attack tools are developed by the technical attackers. With this, new attacks in different variations are coming which are difficult to detect.

Increase in internet dependency in all walks of life, digital nature of data in huge amounts getting accumulated through online transactions and decentralization of data repositories, has led to the development of effective security algorithms. The continuously changing nature of cybercrime also leads to the difficulty of handling and avoiding emerging threats. The task of securing cyber-space is the most difficult and challenging task as advanced threats play a very active role. Therefore it is necessary to get insights into the concepts of security defense mechanisms, different techniques and trending topics in the area of information security.

Rest of the paper is organized as follows; Section II describes about Graph data analytics, Section III explains the concept of Security in wireless sensor networks, Section IV presents the trends in Social behavioural biometrics, Section V explains the concept of Intrusion detection analytics, Section VI discusses the techniques of attack prediction and Section VII concludes the research work with future direction.

II. GRAPH DATA ANALYTICS

Cyber-attacks may alter the structure, behavior and internal functionality of the network. In-order to handle this, one has to understand and learn about the nature of network topologies and communication patterns.

'Graph data analytics' provides the basics of how network structures are modeled measured and compared [2]. Networks are represented in-terms of graph like structures where each vertices of a graph represents a node in the network and each edge of graph reflects the communication between the corresponding nodes as can be observed from the Fig 1.

Two kinds of measures are taken from the graph: Node level measures, Graph level measures. Node level measures are node centrality, degree centrality, between-ness centrality, Eigen vector centrality, page rank centrality. Graph level measures are density and diameter. A technique called "change detection" is applied on these measures periodically. One needs to apply micro level change detection and macro level change detection. Changes in the measures are recorded and observed which indicates the shifts in corresponding network structure and behavior over time. If this change is an outlier like an abnormal activity, it indicates an attack.

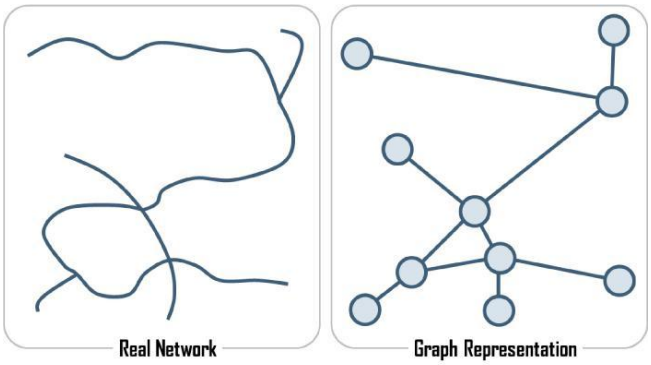

Fig. 1: Graphical representation of a network

III. SECURITY IN WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) refers to the group of sensors which can be able to sense the sensitive information and can be operated even in unattended environments [3]. The environment itself will be saturated with computing and communication capabilities, yet gracefully integrated with human users. WSNs can assess the environmental conditions like temperature, radiation, noise, sound, humidity, climate, vibrations and so on [4]. They can be applicable for monitoring space, things and interactions. The major components of sensor node are: sensor, processor, memory, RF transceiver, and camera. In order to understand the data captured by the nodes, sometimes, it is necessary to consider physical characteristics of the node like nodes location, proximity because depends up on the context, sometimes data needs to be analysed by considering these characteristics. Fig. 2 shows the communication structure of WSNs.

Since these devises are placed in far places and due to the broadcast nature of transition medium, wireless sensor networks are vulnerable to attacks. Some security measures like maintaining the confidentiality, integrity, availability of

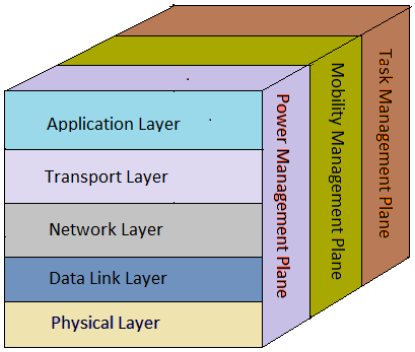

Fig. 2: Communication structure of WSN

the data and node-authentication has to be achieved. All these measures can be achieved by encrypting the sensor network. Along with these measures some other security goals like data freshness, self-organization, time-synchronization, and secure localization should be complete.

Security protocols in WSN like TinySec, SPINS, LISP, IEEE 802.15.4, LSec,, LISA, MiniSec, LLSP, etc may be helpful to protect WSNs from attacks like jamming, tampering, collision, spoofing, sinkhole and sniffing, …etc.

IV. SOCIAL BEHAVIORAL BIOMETRICS

As another step towards providing higher security, existing biometrics are integrated with social behavioral information so that a secure system is designed with the combination of social behavioural biometrics [5]. Basic information like persons style of conversation, gestures, emotions, voice, way of interaction, facial expressions and gait recognition,…etc., can be collected from the social on-line and off-line networks, by considering or observing users online presence patterns (time ,day, month,...etc.), nature of interaction with others (tweets, blogs, chats,…etc.), contents of interaction (topics, likes, opinions,…etc.), online game playing strategies, communication patterns, uploaded videos in you-tube. For example by analyzing you-tube videos, persons facial expressions can be captured as most of the videos covers persons face very closely.

By applying this social behavioral biometrics on issues like Person authentication, Access control, Security & Forensic, Customer profiling, Behaviour analysis and Risk analysis. Most robust secured system can be built.

V. INTRUSION DETECTION ANALYTICS

Intrusion Detection Systems (IDSs) are the software application or the hardware systems that monitors the system for detecting malicious activity. If any intrusion is detected

by an IDS, that should be typically reported either to an administrator or collected centrally using a Security Information and Event Management (SIEM) system. IDS detecting process is done by two methods one is signature based detection and the other is anomaly based detection [6]. In former approach, each packet's signature is compared with some predefined intrusion patterns which are collected from historical transactional data. This mechanism is good enough to identify only known attacks but the attack strategies are keep on changing to compete with the security patches. In later approach, IDS monitors the system activity, behaviors of all incoming transactions are observed. Finally deviations from normal behavior are captured and marked as anomalies. In this way by using anomaly based intrusion detection both known and unknown zero-day attacks are captured.

VI. ATTACK PREDICTION TECHNIQUES

In spite of the increasing efforts in designing preventive system measures, new attack types arise on a regular basis. To combat this, new mechanisms should be adopted by the existing attack prediction techniques. Attack prediction techniques include "Implementation of contextual information to identify cyber-attacks", "Framework for contextual information fusion to detect cyber-attacks" and "Detecting unknown attacks using context similarity".

A. Implementation of contextual information to identify cyber- attacks

Attack prediction leads to knowledge based IDS which gives knowledge about cyber-attacks and possible vulnerabilities. The prediction is a good prediction when-ever context is also considered along with the knowledge based IDS [7]. Contextual information includes relevant preconditions of the attack, semantic relationships between attacks etc. There are 5 aspects of contextual information to improve detection rate of cyber-attacks. Activity- set of events that occur during system execution time, location- reveals location of attackers or victims, Time- reveals time of events that target an entity, Individuality- gives environmental characteristics of entity and Relations- gives relationship between activities that target the entity.

B. Framework for contextual information fusion to detect cyber-attacks

It discovers known and zero-day attacks by examining known software vulnerabilities [8]. There are two phases under this framework; Static phase and Runtime phase. In static phase, training data from network connection repository is taken for data preprocessing step where preprocessing is done by discretization and feature selection [9]. From this preprocessed data, Contextual information is extracted by performing attack-normal probability extraction, attack similarity calculation, host information extraction and attack conditional entropy calculation. Later this contextual information extracted is sent to modeling step by using Bayesian network based profiles and Semantic networks. In runtime phase, testing data is applied on the model which is built in the static phase. Predictions are drawn and finally system evaluation is performed. Similarly this frame work also directs the process of detecting zero-day attacks.

C. Detecting unknown attacks using context similarity

Along with the context, relationship between the attacks in terms of attack similarity is also needs to be considered for the effective detection of attacks and to avoid false predictions [10]. In general, there could be several types of contextual relationships between the attacks. In Fig.3, sim1 indicates the similarity between C2 and Attack1. Sim2 indicates the similarity between C2 and Attack2. Such that sim2 is greater than sim1. Attack2 profile contains some subset of features of Attack1 profile. Since it is be observed that C2 and Attack1 profiles are less similar, one may think that C2 is a being activity which is actually a wrong prediction. As C2 and Attack2 profile are more similar, we think that C2 is an unknown attack which is a proper prediction. So, one has to identify relation between attacks based on the strength of the contextual relationship between two attacks, these features can be selected so that one profile complements the other or at a minimum, both profiles have same similarity. Attack profiles are utilized to identify unknown attacks as a variation of known attacks.

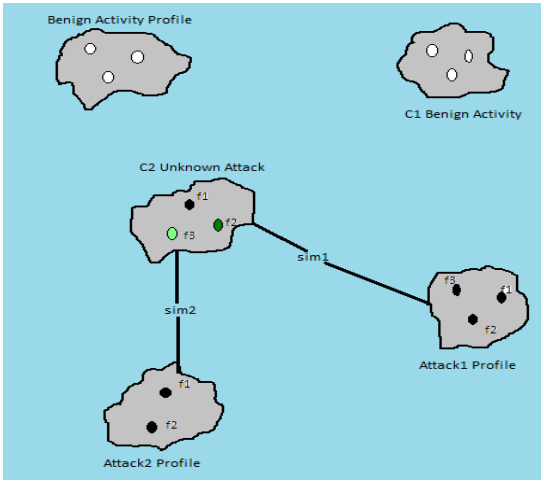

Fig. 3: Importance of considering attack similarities in attack detection

VII. CONCLUSION

Rapid growth in adaption of technology in all walks of life, unfortunately, leads to increased cyber-crime rate. Available data regarding cyber-crime is little and unreliable, unwillingness of organizations to report the crimes and lack of international collaboration makes it difficult to combat cyber-crimes. Day-by-day new attacks are being evolved with complex patterns and tough signatures making them more difficult to detect. Therefore synergizing the concepts of Cyber security and data analytics is essential to learn about different security mechanisms. This paper briefly discusses about the recent research efforts (like graph data analytics, security in WSNs, social behavioural biometrics, attack prediction techniques etc.) that can create attack prediction models with new trends in cyber-security. Our future research focuses on the issues in the Intrusion Detection Systems.

REFERENCES

[1] Oreku, George S., and Fredrick J. Mtenzi. "Cybercrime: Concerns, Challenges and Opportunities." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp. 129-153, 2017.

[2] Namayanja, Josephine M., and Vandana P. Janeja. "Characterization of Evolving Networks for Cybersecurity." Information Fusion for Cyber-Security Analytics. Springer, Cham,. pp.111-127, 2017.

[3] Chakraborty, I, Das, P., "Data Fusion in Wireless Sensor Network-A Survey", International Journal of Scientific Research in Network Security and Communication, 5(6), pp.9-15, 2017.

[4] Anchugam, C. V., and K. Thangadurai. "Security in Wireless Sensor Networks (WSNs) and Their Applications." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp.195-228, 2017.

[5] Gavrilova, M. L., et al. "Emerging trends in security system design using the concept of social behavioural biometrics." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp.229-251, 2017.

[6] Grahn, Kaj, Magnus Westerlund, and Göran Pulkkis. "Analytics for network security: A survey and taxonomy." Information fusion for cyber-security analytics. Springer, Cham, pp.175-193, 2017.

[7] AlEroud, Ahmed, and George Karabatis. "Using contextual information to identify cyber-attacks." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp.1-16, 2017.

[8] Singh, U.K., Joshi, C, Singh, S.K., "Zero day Attacks Defense Technique for Protecting System against Unknown Vulnerabilities", International Journal of Scientific Research in Computer Science and Engineering, 5, pp.13-18.,2017.

[9] AlEroud, Ahmed, and George Karabatis. "A Framework for Contextual Information Fusion to Detect Cyber-Attacks." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp.17-51, 2017.

[10] AlEroud, Ahmed, and George Karabatis. "Detecting Unknown Attacks Using Context Similarity." Information Fusion for Cyber-Security Analytics. Springer, Cham, pp.53-75, 2017.

Authors Profile

Mrs.Nerella Sameera has received Bachelor of Technology from Chirala Engineering College, Affliated to JNTU Kakinada in the year 2011 and Master of Technology from Andhra University in year 2013. She is currently pursuing Ph.D in the Department of Computer Science and Systems Engineering, Andhra University,Visakhapatnam since 2017. Her main research work focuses on Data Analytics for Cyber Security and Intrusion Detection Systems. She has 3 years of teaching experience.

Prof. M Shashi pursed B.E in Electrical and Electronics Engineering and M.E in Computer Science Engineering, and Ph.D. in Artificial Intelligence and Knowledge Engineering. She is currently working as a Professor in the Department of Computer Science and Systems Engineering. Her areas of interest are Data Analytics, Data Warehousing & Mining, AI, and Data Structures.

